中和市建八路 123 號 2F
電話：886-2-66202225
傳真：886-2-22234362
www.ZEROPLUS.com.tw
2F., No.123,Jian Ba Rd,
Chung Ho City, Taipei Hsien, R.O.C.
Tel: 886-2-66202225
Fax: 886-2-22234362

Measurement and Analysis Introduction of ISO7816 (Smart Card)

ISO 7816 is an international standard related to electronic identification cards with contacts, especially smart cards, managed jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

It is edited by the Joint technical committee (JTC) 1 / Sub-Committee (SC) 17, Cards and personal identification.

- **ISO7816-1 (Physical characteristics):**

It defines the specifications of the Physical Layer, which includes tolerable working temperature, static tolerance or tolerable bending and weight, etc, of the Smart Card. This part of ISO7816 is very important for card manufacturers. It is helpful for manufacturers to choose the producing materials.

- **ISO7816-2 (Dimensions and location of the contacts):**

It defines the dimensions and the connector including the location of the contacts on the card and the dimensions of the Smart Card.

- **ISO7816-3 (Electrical interface and transmission protocols):**

It defines the electrical signals and the communication transmission protocols.

中和市建八路 123 號 2F
電話：886-2-66202225
傳真：886-2-22234362
www.ZEROPLUS.com.tw
2F., No.123,Jian Ba Rd,
Chung Ho City, Taipei Hsien, R.O.C.
Tel: 886-2-66202225
Fax: 886-2-22234362

- **ISO7816-4 (Organization, security and commands for interchange):**

From Abstract of www.iso.org, it defines how to use the application identifier in the card to check whether there is an application retrieval of the or/and status.
Functions are as below:
·Connect the command-response pairs exchanged at the interface.
·Indicate the retrieval of data elements and the data objects in the card.
·Indicate the structures for applications and data in the card.
·Indicate the means and mechanisms for identifying and addressing applications in the card.
·Describe the structures and contents of historical bytes of the operating characteristics of the card.
·Describe the access methods to files and data in the card.
·Describe the access methods to the algorithms processed by the card.
·Describe the security architecture defining access rights to files and data in the card.
·Describe the methods for secure messaging.
Link from
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=36134

- **ISO/IEC 7816-5:** shows how to grant the uniqueness of application identifiers through the international registration of a part of this identifier, and defines

the registration procedure,
the authorities in charge thereof,
the availability of the register which links the registered parts of the identifiers and the relevant application providers.
Link from
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=34259

- **ISO7816-6(Inter-industry data elements for interchange):**

From Abstract of www.iso.org, it specifies the Data Elements (DEs) used for inter-industry interchange based on integrated circuit cards (ICCs) both with contacts and without contacts. It gives the identifier, name, description, format, coding and layout of each DE and defines the means of retrieval of DEs from the card
Link from
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38780

中和市建八路 123 號 2F
電話：886-2-66202225
傳真：886-2-22234362
www.ZEROPLUS.com.tw
2F., No.123,Jian Ba Rd,
Chung Ho City, Taipei Hsien, R.O.C.
Tel: 886-2-66202225
Fax: 886-2-22234362

- **ISO1816-7(Inter-industry commands for Structured Card Query Language):**

Structured Card Query Language(SCQL) Inter-industry commands
It describes the specification of the inter-industry commands for the Structured Card Query Language(SCQL).

- **ISO7816-8(commands for security operations):**

From Abstract of www.iso.org, the inter-industry commands(with contacts and without contacts) of the Smart Card is to be defined in 2004, which is applied in the cryptographic operations. The definitions of the commands are based on the Commands listed in the ISO/IEC 7816-4. certificates and the import 及 export of asymmetric keys.
The Annexes provides the examples of digital signatures, certificates and the import and the export of asymmetric keys.
The choice and the condition of use of the cryptographic mechanism may effect the card exportability, and the algorithms and the contents of Protocol Analyzer are outside the range of the ISO/IEC 7816-8.
Link from
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=37989

- **ISO7816-9(Commands for card management):**

From Abstract of www.iso.org, it defines the file management of the inter-industry commands(both with contacts and without contact) of the Smart Card, such as file creation or file deletion and so on. These commands include the entire life cycle of the Card and other commands may be used which is issued.

The Annex provides that shows how to control and read (secrecy transmission) the data of the Card, by means of transmitting and verifying the data under the secrecy condition, such as code, keys and applets.
Link from
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=37990

- **ISO7816-10(Electronic signals and answer to reset for synchronous cards):**

From Abstract of www.iso.org, this part defines the Power Supply, Signal Structure and Reset Structure when the Smart Card is transmitted from the interface to the synchronous transmission of device.
Link from
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=30558

中和市建八路 123 號 2F
電話：886-2-66202225
傳真：886-2-22234362
www.ZEROPLUS.com.tw
2F., No.123,Jian Ba Rd,
Chung Ho City, Taipei Hsien, R.O.C.
Tel: 886-2-66202225
Fax: 886-2-22234362

- **ISO7816-11(Personal verification through biometric methods):**

  From Abstract of www.iso.org, this part defines the usage of the inter-industry commands and data objects related to personal verification through biometric methods in the Smart Card.

Inter-industry commands ISO/IEC 7816-4. data objects ISO/IEC 19785-1。

Please refer to the ISO/IEC 7816-4 about the definition of the inter-industry commands. The data objects are partially defined in this International Standard, partially imported from ISO/IEC 19785-1.

ISO/IEC 7816-11 also presents examples for enrollment and verification and addresses security issues.

Link from

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=31419

- **ISO7816-12(USB electrical interface and operating procedures):**

  From Abstract of www.iso.org, this part defines the operating conditions of the Smart Card in the USB Interface, and a Smart Card with USB Interface is named USB-ICC.

  ISO/IEC 7816-12:2005

The ISO/IEC 7816-12:2005 defines the below content:

· Define the Electrical Characteristics Condition when the USB-ICC is operated by the way of the Interface Mode.

·· The Descriptions of the USB Standard and the USB-ICC Class.

· It is about the specification of Bulk Transmission and Control Transmission when the transmitting data is between HOST and USB-ICC.

· It can accept two different Protocol Analyzer Versions when srtarting the Control Transmission.

· It indicates the status of the interrupt transmission and the error conditions under the Asynchronous Status.

- **ISO/IEC 7816-12:** It has provided two protocol versions for the Control Transmission in 2005; one is to support the protocol T=0 (version A) and the other is to use the transfer on APDU level (version B).

  This part provides the instruction sheets of the different transmissions(Bulk Transmission, Control Transmission, version A and version B) for the USB-ICC. The USB-ICC can deal with the possible and sequential examples in the informative annex.

中和市建八路 123 號 2F
電話：886-2-66202225
傳真：886-2-22234362
www.ZEROPLUS.com.tw
2F., No.123,Jian Ba Rd,
Chung Ho City, Taipei Hsien, R.O.C.
Tel: 886-2-66202225
Fax: 886-2-22234362

- **ISO/IEC 7816-12:** It has provided two protocols for the Control Transmission in 2005. In order that it can support the protocol T=0(version A) or use the transfer on APDU level(version B).

The Annex provides the examples of the USB-ICC.
Link from
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40604

- **ISO7816-13(Commands for application management in multi-application environment):**

  This part introduces the relative items when developing the Global Platform Standard, such as the Secure Channel Protocols.

- **ISO7816-15(Cryptographic information application):**

From Abstract of www.iso.org, it defines the Applications of the Smart Card and the Cryptographic Function. It has defined the common syntax(in the ASN.1) and format in 2004, which contrapose to the Cryptographic Information and the Sharing Machanism.

- **ISO/IEC 7816-15:**

It supported the below functions in 2004:
· It can store multiple instances of cryptographic information in the Smart Card.
· Use of the Cryptographic Information.
· Retrieval of the Cryptographic Information.
· The DOs defines the most suitable Cross-referencing of the Cryptographic Information in the ISO/IEC 7816.
· Different Authentication Mechanisms.
· Multiple cryptographic algorithms.
· Cross-referencing of the cryptographic information with DOs defined in ISO/IEC 7816 when appropriating.

The ISO7816-1～ISO7816-13 and the ISO7816-15 define the different specifications of the Smart Card, the following will introduce the Smart Card and how to start the measurement.

中和市建八路 123 號 2F
電話：886-2-66202225
傳真：886-2-22234362
www.ZEROPLUS.com.tw
2F., No.123,Jian Ba Rd,
Chung Ho City, Taipei Hsien, R.O.C.
Tel: 886-2-66202225
Fax: 886-2-22234362

Introduction of Smart Card

A smart card, chip card, or integrated circuit card (ICC), is any pocket-sized card with embedded integrated circuits which can process data. This implies that it can receive input which is processed — by way of the ICC applications — and delivered as an output. There are two broad categories of ICCs. Memory cards contain only non-volatile memory storage components, and perhaps some specific security logic. Microprocessor cards contain volatile memory and microprocessor components. The card is made of plastic, generally PVC, but sometimes ABS. The card may embed a hologram to avoid counterfeiting. Using smartcards is also a form of strong security authentication for single sign-on within large companies and organizations

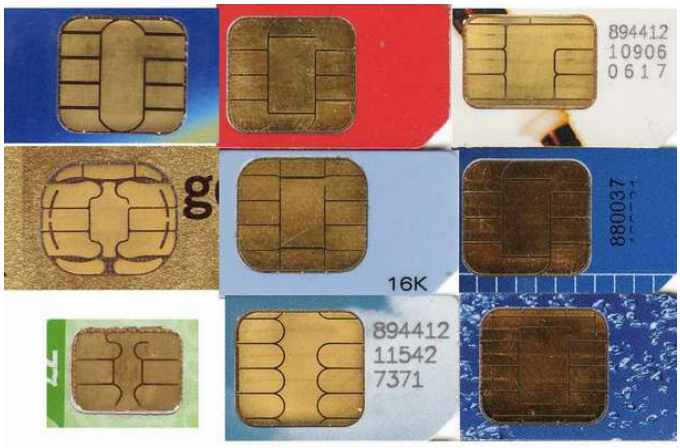


Figure1: Types of Common Smart Card on the Market

中和市建八路 123 號 2F
電話：886-2-66202225
傳真：886-2-22234362
www.ZEROPLUS.com.tw
2F., No.123,Jian Ba Rd,
Chung Ho City, Taipei Hsien, R.O.C.
Tel: 886-2-66202225
Fax: 886-2-22234362

Table1 is about the description of contacts of Smart Card, and Figure2 is about the slot diagram of the Smart Card Reader which is sold on the market. Users can clearly understand the position of each contact according to the entity picture marking.

Contact	Designation	Use
C1	**Vcc**	Power connection through which operating power is supplied to the microprocessor chip in the card.
C2	**RST**	Reset line through which the IFD can signal to the smart card's microprocessor chip to initiate its reset sequence of instructions.
C3	**CLK**	Clock signal line through which a clock signal can be provided to the microprocessor chip. This line controls the operation speed and provides a common framework for data communication between the IFD and the ICC.
C4	**RFU**	Reserved for future use.
C5	**GND**	Ground line providing common electrical ground between the IFD and the ICC.
C6	**Vpp**	Programming power connection used to program EEPROM of first generation ICCs.
C7	**I/O**	Input/output line that provides a half-duplex communication channel between the reader and the smart card.
C8	**RFU**	Reserved for future use.

Table1: Description of Contacts of Smart Card

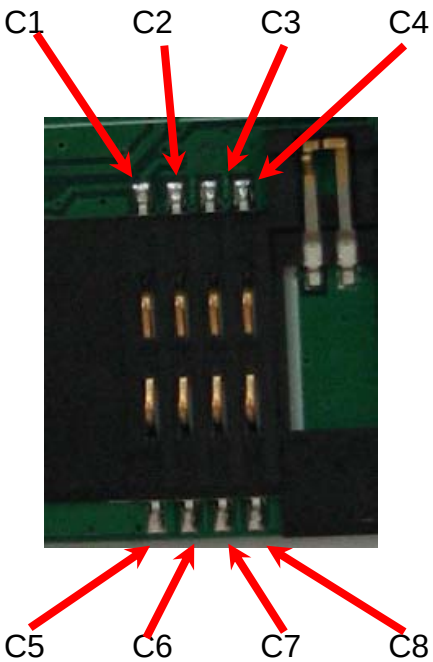


Figure 2: Contact Diagram of the Smart Card Reader

中和市建八路 123 號 2F
電話：886-2-66202225
傳真：886-2-22234362
www.ZEROPLUS.com.tw
2F., No.123,Jian Ba Rd,
Chung Ho City, Taipei Hsien, R.O.C.
Tel: 886-2-66202225
Fax: 886-2-22234362

Measurement of Actual Signals of ISO7816 with ZEROPLUS Logic Analyzer

There are eight contacts on the Smart Card in total. It only needs connecting C3, C5, C7 to ZEROPLUS Logic Analyzer when measures signals.

C3	**CLK**	Clock signal line
C5	**GND**	Ground line
C7	**I/O**	Input/output line

The test point can be connected to the Logic Analyzer by ZEROPLUS test probe .
Connect C3 to A0 channel of Logic Analyzer ; connect C7 to A1 channel and C5 to the GND of Logic Analyzer,

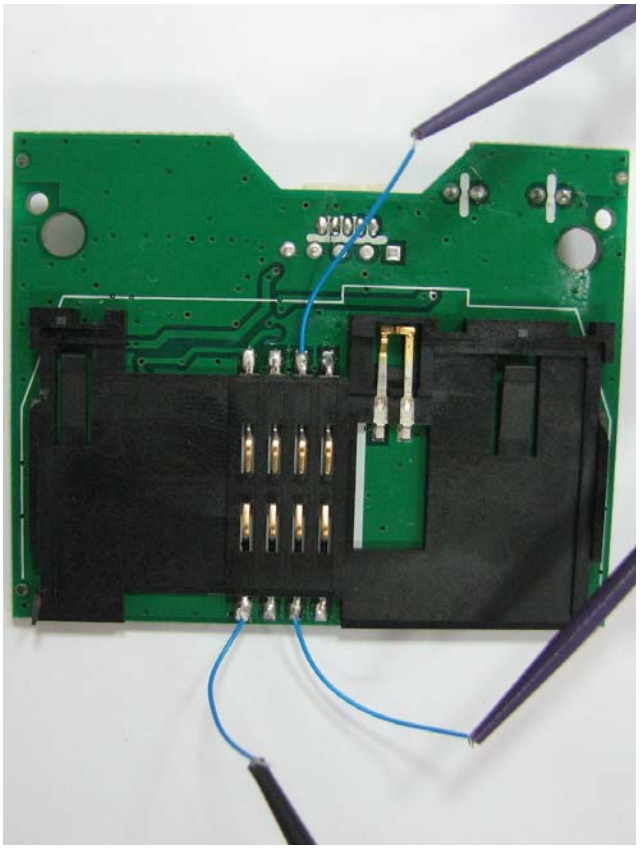


Figure 3: Measure the Smart Card Reader.

Users can activate the software of ZEROPLUS Logic Analyzer to measure the signal after completing the connection (Please visit the website (www.ZEROPLUS.com.tw) of ZEROPLUS Logic Analyzer). The captured waveform is displayed as below (Refer to *Figure 4*).

中和市建八路 123 號 2F
電話：886-2-66202225
傳真：886-2-22234362
www.ZEROPLUS.com.tw
2F., No.123,Jian Ba Rd,
Chung Ho City, Taipei Hsien, R.O.C.
Tel: 886-2-66202225
Fax: 886-2-22234362

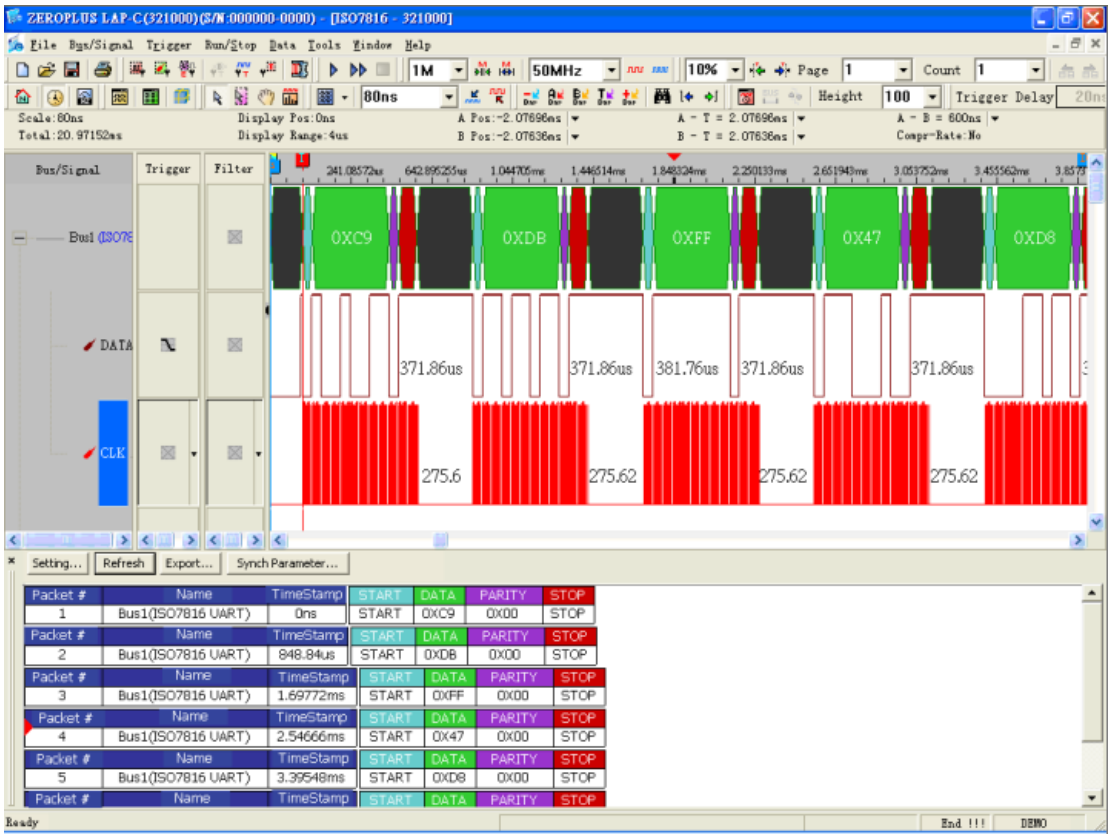


Figure 4: Waveform Display by ZEROPLUS logic analyzer

The signal structure of the ISO7816 is similar to that of the RS-232C, and the difference is that the ISO7816 needs relying on the CLOCK to judge the data; the RS-232C uses the baud rate in its signal to judge the data. The ISO7816 takes the 16bits of CLOCK as one unit to start sampling data; see the following Figure 5.

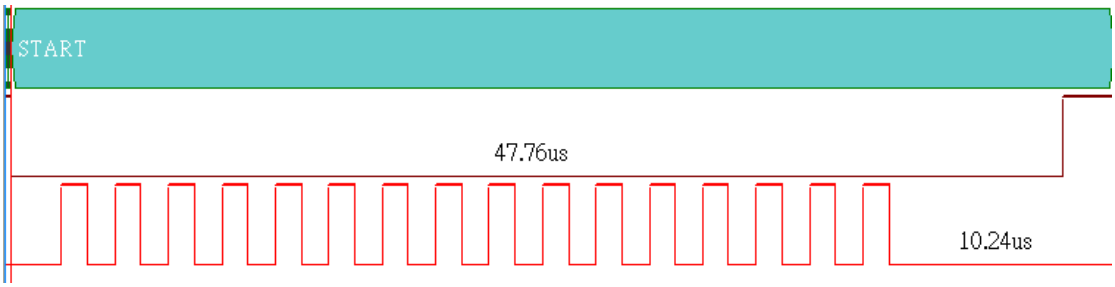


Figure 5: ISO7816 START Packet

中和市建八路 123 號 2F
電話：886-2-66202225
傳真：886-2-22234362
www.ZEROPLUS.com.tw
2F., No.123,Jian Ba Rd,
Chung Ho City, Taipei Hsien, R.O.C.
Tel: 886-2-66202225
Fax: 886-2-22234362

According to the Figure 5, after the CLOCK under the START bit generates 16 periods (1 ETU) clock, it is time to do the judgment; users can analyze the DATA Packet with the same way.

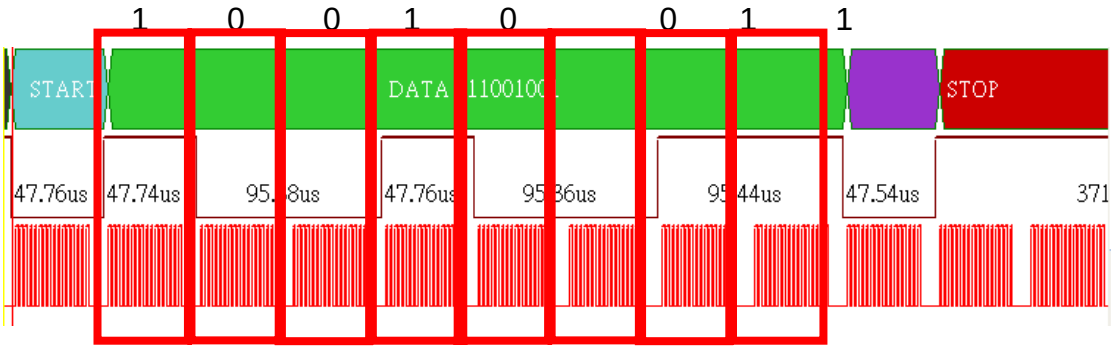
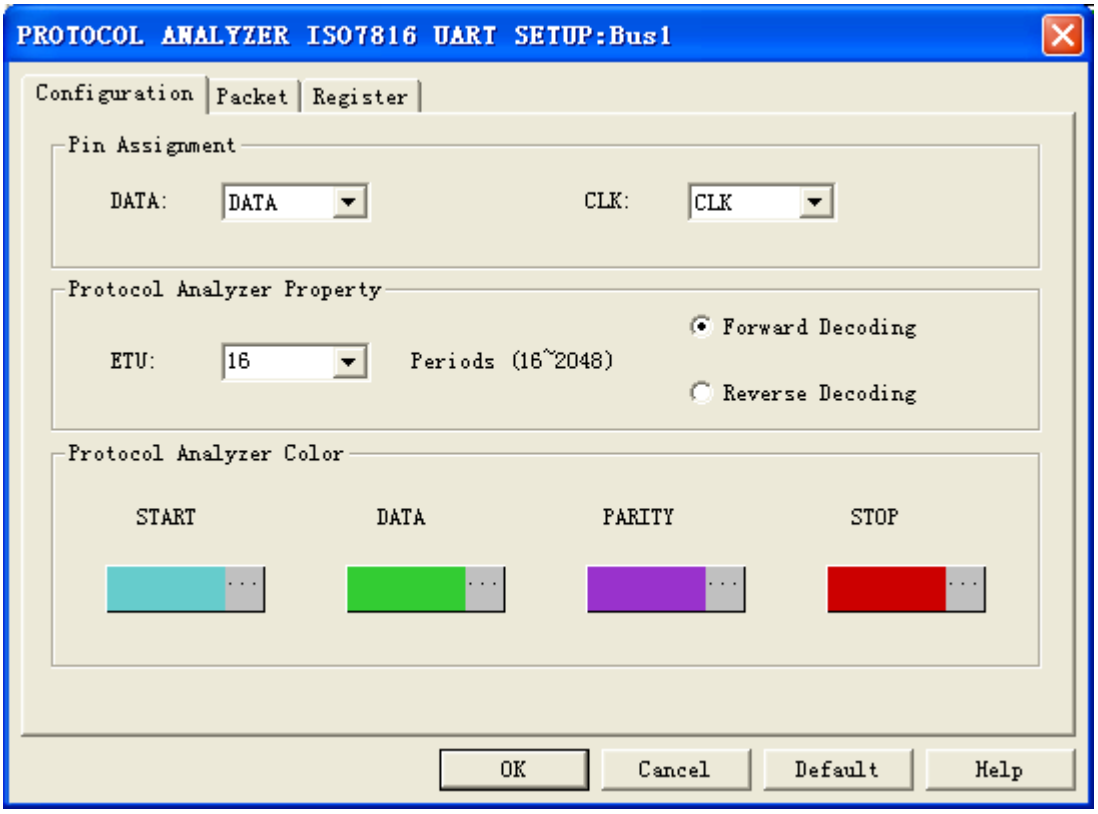


Figure 6: The Whole ISO7816 Signal Packet

The format of the Signal Packet consists of the START (1bit), DATA (8bits), PARITY CHECK (1bit) and STOP (2bits). Each bit on the DATA Line needs appearing 16 periods (1 ETU) clock on the CLOCK Line, and the Transmission Direction of DATA is fixed, which is LSB to MSB.

Interface of the Protocol Analyzer ISO7816 UART of ZEROPLUS Logic Analyzer



Pin Assignment: Setting channel DATA and CLK

Protocol Analyzer Property: Set the periods of clock as 1bit in the signal of ISO7816. The default is 16 Periods, and the Max. can be set as 2048 Periods.

中和市建八路 123 號 2F
電話：886-2-66202225
傳真：886-2-22234362
www.ZEROPLUS.com.tw
2F., No.123,Jian Ba Rd,
Chung Ho City, Taipei Hsien, R.O.C.
Tel: 886-2-66202225
Fax: 886-2-22234362

Conclusion

Today, Digital Signal and Protocols are widely use in different electronic products and technical area. From mobile phone, PC, multimedia, automotive to RF and so on, all the use trends are testing the analysis ability of engineers who have to deal with the Digital Signal for developing or testing and debugging. It is very hard to analyze the Digital Signal when engineers only use the oscilloscope. However, matching with ZEROPLUS Logic Analyzer can improve the efficiency of development greatly. ZEROPLUS Logic Analyzer has launched over 55 Protocol Analyzer Modules and Patent Technologies for different technical areas. For more detailed introduction about ZEROPLUS Logic Analyzer, please visit our website: www.ZEROPLUS.com.tw.

Reference:

CardWerk from http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816.aspx
Wikipedia ISO/IEC 7816 from http://en.wikipedia.org/wiki/ISO_7816