Sensors & Transducers, Vol. 175, Issue 7, July 2014, pp. 226-233

Sensors & Transducers

Application of the Information Encryption Technology in the Industrial Control Network Based on FPGA

Guo Yao-Hua
The Department of Information and Engineering, Tangshan College, Hebei, Tangshan, 063008, China
Tel.: 18232590419
E-mail: tdgyh@sina.com

Received: 18 December 2013 /Accepted: 30 May 2014 /Published: 31 July 2014

Abstract: With the rapid development of information technology industry, Information encryption is an effective means of information security. Data encryption system based on FPGA in the field of industry is elaborated in this paper, and the data acquisition module, the basic principle of 3DES algorithm, its implementation in FPGA and PMC bus interface module are introduced. Based on the function simulation, test and analysis of the design results, this scheme has the characteristics of high reliability, fast algorithm and less hardware resources, and it can be widely used in industrial networks. *Copyright © 2014 IFSA Publishing, S. L.*

Keywords: FPGA, 3DES algorithm, Data transmission.

1. Introduction

Along with the gradual popularization of computer application in all walks of life and the rapid development of network communication technology, networked data acquisition and transmission system are used in all kinds of data monitoring in the industrial enterprises. In order to make the management and monitoring of data acquired from the field convenient for the managers, the RS232/RS485 and various industrial buses to form the industrial control network are used and all data acquired from the field are transmitted remotely to the monitoring center. Although the widespread use of network monitoring system has realized the automation of industrial production level, the network monitoring bring a lot of conveniences to the enterprise, the emergence of network virus and network hacker causes the hidden danger of network data security. How to protect a great deal of data stored and transmitted in the network, especially some important data resources of enterprises, is becoming more and more important, so the data encryption technology is playing a more and more important role in industrial network.

Nowadays, the data encryption technology is mainly used in the field of software, but software encryption can only be treated as software plug-in, and it takes up a lot of CPU time and resources during the runtime, so the demands of speed of system encryption and data transmission were not met, and using the hardware system to realize data encryption work is very necessary [1]. A kind of embedded encryption/decryption system is designed in this paper, and the encryption technology is applied into the industrial network, using the high processing ability of FPGA to realize the 3DES algorithm, and making the data transmitted in the network processed by the 3DES encryption, the safety of data transmission is realized on the basis of not affecting the transmission efficiency.

2. System Design Scheme

The whole system design scheme is shown in Fig. 1, designed information encryption and decryption system are implemented by hardware interface boards. One is the field encryption board, the other one is the host decryption board. The field encryption board is responsible for the data acquisition and encryption of measured signal in the field. Sensor and control circuit convert measured signal to 0~5 V (4~20 mA) voltage (current) signal, and transmit it into A/D (ADC0809) converter to realize the analog-to-digital conversion, data converted by A/D is transmitted into FPGA for 3DES encryption under the control of the FPGA, at last, encrypted cryptograph carry out the long-range data transmission through a serial communication interface and coaxial cable. The host decryption board receives the cryptograph through serial interface, cryptograph is implemented 3DES decryption in the FPGA, finally transmitted to the host computer through the industry PMC bus. This process not only guarantees the security of important field data during network transmission, at the same time, it also will not affect the efficiency of data transmission. Instead the host site encryption and decryption card and board functions, via the serial interface receiving the cryptograph, the acceptance and 3DES decryption of the cryptograph are implemented in the FPGA, decrypted cryptograph will be transmitted to the host computer via the industry PMC bus eventually.

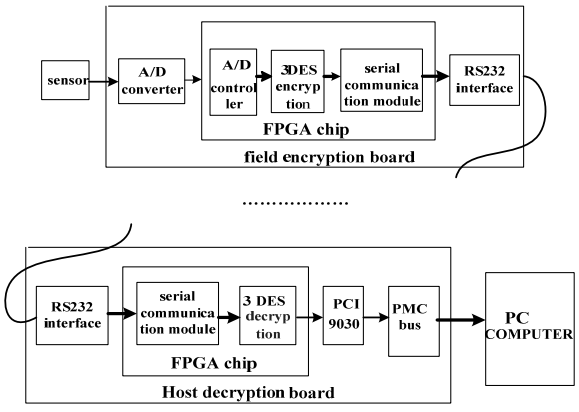

Fig. 1. Diagram of the overall system design.

With this encryption and decryption system in the field of industrial control, the data transmitted in the network are all cryptographs out of the encryption system after encrypted, even if some illegal intruders intercepts data link by some means, they will be unable to obtain the plaintext data for no decryption key, so as to achieve the purposes of transmission security and protection of confidential data. The normal users establish a secret shared communication channel with the negotiated encryption/decryption key at the time to ensure the security of data. The whole system processing of encryption and decryption is independent of the host, so no delay in ensuring high-speed data transmission at the same time, thus it not only improve the security of data transmission, and also not take up the host CPU's processing time.

3. System Hardware Design

The hardware circuit includes four parts: the A/D converter, the FPGA core chip, serial interface, the host interface hardware module.

3.1. FPGA Core Chip

As the core of the system, all the data encryption and decryption algorithm are implemented in the FPGA chip, we select the Cyclone III series EP3C25Q240 chips as the FPGA chip. Cyclone series is currently the highest cost-effective FPGA on the market, the chip is based on the process of whole copper 1.5 V SRAM after the cost optimization, with 20060 logical units and as many as 294912 bits embedded RAM, supporting a variety of single-ended I/O standards, such as LVTTL, LVCMOS. There are double data rate (DDR) SDRAM and the interface FCRAM dedicated circuit in the Cyclone chip, and also two phase-locked loops (PLLs), providing the hierarchical structure and complex design of clock circuit clock management [2].

The hardware interface card provides the download interface and debugging interface of the FPGA chip design, the download interface is the download hardware description file interface in FPGA; the debugging interface which is implemented in embedded system is the interface of embedded processors connections, and this interface is typically existed in the high-performance embedded processor.

3.2. Host Interface Module

The host decryption board designed by system is based on VME bus of industrial PC as the motherboard, integrated to the PC control system through the PMC bus, so the decryption board should follow the PMC (PCI Mezzanine Cards) card design specifications. PMC bus is according to the CMC card of PCI bus defined from two standard forms of IEEE1386 and IEEE1386.1, is one daughterboard structure of the connection between VME64x board and CompactPCI board.

PCI9030 is a high-performance target interface chip developed by PLX company, it can simplify the complex PCI bus control logic into relatively simple local bus control logic, so that the design of the PCI bus interface function can be simplified to the realization of the local bus control logic, and make

high-performance PCI bus interface used conveniently. The diagram of PCI9030 with PMC bus and FPGA chip connection is shown in Fig. 2. The corresponding pins on the PCI side of PCI9030 chip are connected to the corresponding pins of PMC bus, the local bus side is connected with FPGA, PMC bus operations (including reading and writing, etc.) can be converted into the operation of local address space by setting the 9030 internal register values, to realize data transmission between the FPGA chip and PMC bus.

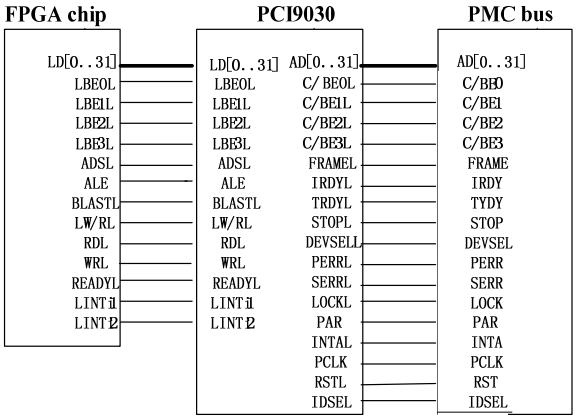

Fig. 2. The diagram of PCI9030 with PMC bus and FPGA chip connection.

4. Software Module Design of FPGA Chip

The core functions of encryption/decryption system are all implemented in the FPGA chip, internal implementation of function module mainly includes data acquisition and transmission module, the DES encryption/decryption module, 3DES encryption/decryption module and local bus interface module, each function module is introduced respectively in detail as the following.

4.1. Control of Data Acquisition and Transmission

The A/D converter of data acquisition in the field encryption board is ADC0809. It is an 8-bit A/D converter with 8 channels, the conversion time is 100 us. The state machine is selected to design the controller of A/D conversion in FPGA, according to the work sequence of ACD0809, the state machine is set into 7 state to controlling the startup, A/D conversion and data reading respectively. Fig. 3 is ADC state transition diagram of state machine controller, seven states are respectively: st0: ADC0809 initialization state, it comes into st1 state when the next pulse is coming; st1: channel address latch state, if the ALE = 1, it comes into the st2 state when the next pulse is coming; st2 state: A/D conversion START state, START the A/D conversion when falling edge of START is coming; st3 state: the state of determining is the conversion start, the signal of ADC0809 working state (EOC), if the EOC = '1', the conversion don't start yet, continue to wait; if the EOC = '0', the conversion start, it comes into the st4 state when the next pulse is coming; st4 state: the state of determining the conversion if completed, if the EOC = '0', it means the conversion is still in progress, continue to wait; if EOC = '1', the end of the conversion is over, it comes into the st5 state when the next pulse is coming; st5 status: the state of allowing data to output, if the OE = '1', it comes into the st6 state when the next pulse is coming; st6 status: data latch state, if the LOCK = '1', the converted data latch. The converted 8-bit data form 64-bit plaintext after processing, and then transmit to the 3DES module for encryption.

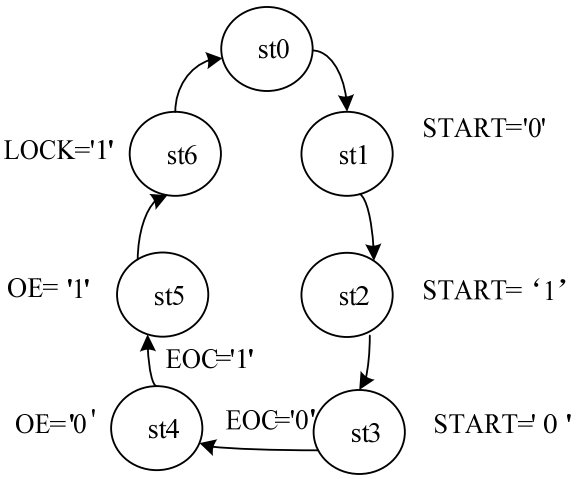

Fig. 3. ADC state transition diagram of state machine controller.

UART is a kind of universal serial data bus, used for asynchronous communication. The cryptograph data are transmitted through serial communication module in the network, and implementing the communication between the field encryption board and the host decryption board. Due to the transmitted cryptograph is 64-bit, according to the RS232 serial communication standard, the custom communication protocol is used in this process, the format of basic data frame is a 1-bit start bit, a 64-bit data bit, a 1-bit stop bit, gathering a total data of 66-bit, receiving module is carried out in accordance with the definition of a 66-bit data frame information.

UART serial communication in the design is mainly divided into three modules: data sending module, data receiving module and the baud rate generator module. Sending module is for data delivery, converts data from parallel input to serial output; receiving module is for data reception, converts data from serial input to parallel output; UART baud rate generator module controls and generates the clock frequency. In order to enhance

the anti-interference of data, improve the reliability of data transmission, and also avoid the edge distortion at the ends of the data bits, a "from 1 to 0 jump detector" is designed in the receiving module, when the jump detector receives eight consecutive low electricity at ordinary times, RXD detector will regard that there is a start bit on the RXD, the module comes into the state of receiving data.

A 9600 b/s baud rate is selected in this design, in order to get a precise sampling at the receiving end, sampling clock frequency is 16 times of the baud rate clock frequency at the receiving end. In the receiving state, receiving controller will sample for 7, 8, 9 three pulse of data bit, and adhere to the principle of choosing two from three to determine the final receiving value.

Data sending and receiving modules are realized by using the design of state machine, the state flow-line is shown in Fig. 4, in accordance with the design requirements, the state machine is divided into five state, respectively are: f_ree idle: when resett = '0' (reset), the state machine into f_ree state, when xmit_cmd_p = '1' to enter s_tart state; s_tart start bit state: UART sends data to the TXD, it comes into w_ait state when the next clock pulse is coming; W_ait shift wait state: in this state, every 16 clock pulses sent one data, sending the data bits in the state of the shift in turn into sending register, until the eight data bits are sent, comes into s_top state; S_hift shift state: in this state, parallel/serial conversion of the ready-to-send data is completed, and it comes back to w_ait state after the conversion; S_top stop bit state: in this state, there are 16 BCLKT cycle logic 1 signals, namely, 1 stop bit, after state machine sending the stop bit, it comes back to f_ree state, waiting to send another data frames.

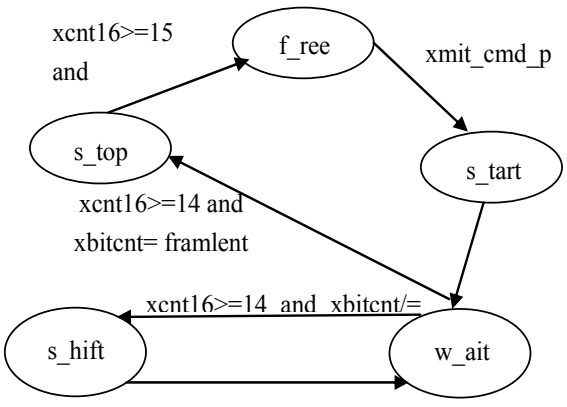

Fig. 4. The state transition diagram of accept communication module.

4.2. DES Algorithm Principle and FPGA Software Implementation

Data Encryption Standard (DES) which is belonged to grouping algorithm of symmetric algorithm is a commonly used symmetric encryption technology [5]. Because of the high encryption strength, this standard is widely used in many occasions of requiring encryption. In the DES algorithm, by combining the technology of confusion and diffusion, that is the substitution first and the replace later, the 64-bit key plays a role in the plaintext and the 64-bit cryptograph is generated after 16 rounds of iterations. It uses the same key during the encryption and decryption process, decryption is the inverse process of encryption. The Fig. 5 that is the process of DES encryption algorithm shows the whole process includes three stages: Firstly, transform the plaintext, take the given 64-bit initial plaintext *X* as the object, and rearrange the *X* through a replacement *IP* list to construct 64-bit *X0*, *XO=IP(X)=L0R0*, *L0*represents the first 32-bit of X0, *R0*represents the other 32-bit of *X0*.

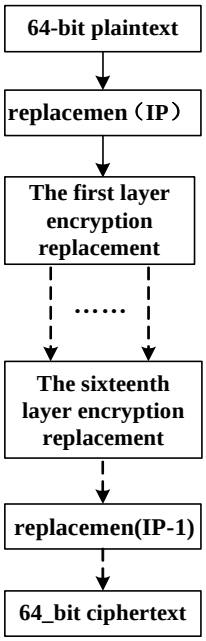

Fig. 5. The process of DES encryption algorithm.

Secondly, according to the rules of 16 rounds of iterations to realize the alternation encryption, there are replacements and substitutions during each round and the diagram of each iteration and alternation are shown in Fig. 6. The output of each layer alternation acts as the input of the next iteration and the alternation formula of each layer is:

$$Li = R_{i-1}$$

$$Ri = L_{i-1} \oplus f(R_{i-1}K_i)$$

$$i = (1,2,3...16)$$

Symbol $\oplus$ represents the XOR mathematics operation, f is operation function replaced by *S* box, K_i is some sub-keys produced by key scheduling function. After 16 rounds of iterations, make *L16R16* replaced inversely by using *IP-1*, then get the cryptograph. There are four key points during the process of DES encryption: *IP* replacement, *f* function, sub-key *Ki* and S box.

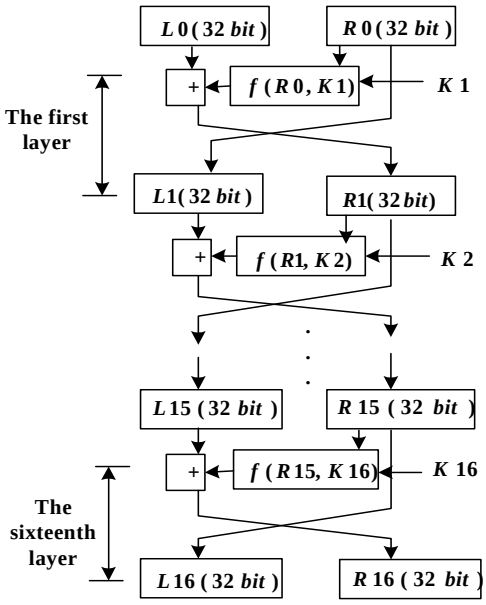

Fig. 6. The diagram of 16 rounds of iterations and alternations.

DES encryption and decryption functions are realized in the FPGA chip, and how to implement 16 rounds of iteration, the maximum efficiency of encryption/decryption, guarantee the speed of algorithm of implementation and to reduce the consumption of the chip resources, is the problem need to be solved in the design. The method of multiple data block assembly line processing is used in this design, after the plaintext transmitted into FPGA processing unit, first, according to the DES grouping method to group the plaintext data, in the first clock cycle, the first block of data after processed in the first round is saved into the register 1; In the second clock cycles, the data after processed in the register 1 is saved into the register 2, at the same time, the second block of data is processed, and the processed data is saved into register 1; In the third clock cycle, the data in register 2 after the third round processing is saved into the register 3, the data in the register 1 is saved into register 2 through the second round of processing, at the same time, a new data after the first round processing is saved into the register 1. So multiple data block assembly line processing can be realized, and making the encryption/decryption efficiency improved dramatically [6].

4.2.1. *IP* Replacement

The function of *IP* replacement is to recombine the input 64-bit plaintext data according to the *IP* list, and to make the output divided into *L0* and *R0* whose length is 32-bit. *L0* and *R0* are the latter part of rearrangement output, *L0* is the left 32-bit of output, *R0* is the right 32-bit. *L16*and *R16* can achieved after 16 rounds of iterative computations, take these results as input for inverse replacement, that is, the result of cryptograph output has gotten. *IP* inverse replacement is the inverse operation of the initial replacement.

4.2.2. The Generation of Sub-key K_i

The length of key *K* is 64-bit, and the 8-bit, 16-bit, 24-bit, 32-bit, 40-bit, 48-bit and the 64-bit is parity bits, so, in fact, the real length of key is 56-bit. The values range of the subscript of *K* is 1 to 16, constructed by 16 rounds of iterations, In each round, it applies the bit alteration to choose bit for sub-key, the result of the selected is 56-bit, the first 28-bit of that is part C and the latter 28-bit of that is part D. Starting from the first cycle in the FPGA, part C and D shift one or two-bit to left during each clock cycle, as the input of next round after latching, after merging by a compression processing, the shifted part C and D produce 48-bit sub-keys *K1, K2, K3 … K16.* Using the CASE statement of VHDL language can realize bit-alteration and compression algorithm during the FPGA implementation.

DES iterative transformation is with 16 rounds, the transformation are selected and shift in each round, after 16 rounds after transformation, a corresponding secret key will be generated in each round. In the hardware implementation of FPGA chip, the design of displacement and compression algorithm is function form, the transformation will call this function in each round, resulting in a corresponding secret key.

4.2.3. *f* Function

The *f* function has two inputs 32-bit R_{i-1} and 48-bit K_i, the 32 bit right parts of R_i is extended to 48 bits through E extend and displacement algorithm. By using the case statement in E algorithm, the 32_bit and some bit from it is made 48-bit data. Finally, the 48 bit output is made through exclusive or operation of the 48-bit input data and K_i. The 48 bit output is divided into 8 groups, each group is six and the eight boxes is the input of the *S* box.

4.2.4. *S* Box Replacement

S box that is a complex nonlinear function is a key part of DES algorithm, the design of the box directly affects the whole performance of the algorithm, its main function is to realize the function of the output data of 48 to 32 bits of data conversion. DES encryption has eight boxes, each box has six inputs and four output. The conversion from the 48 bit output data to the 32-bit data is achieved through *S* box.

In FPGA design of S box, the look-up table (LUT) is used to configuration ROM, the input of the six as ROM address, the ROM corresponding address space store the output of four, thus the six input/output 4 lookup table (LUT) are realized.

4.3. 3DES Encryption and Decryption

Due to the 64-bit length of the key used by DES, the encryption intensity is difficult to meet the requirements. 3DES encryption algorithm is a process of data encryption-decryption-encryption, in which the plaintext is encrypted 3 times, the different keys are used in each time, and the valid keys are increased to 168 bits. By using 3DES, the encryption intensity is greatly enhanced, the risk of exhaustion attack in the DES algorithm can be effectively overcome, and at the same time, the resistance of linear analysis and the ability of checking are both increased [7]. The diagram of 3DES encryption/decryption implementation is shown in Fig. 7, the encryption key K1 is used for DES encryption of the plaintext, the key K2 is used for the decryption, the key K3 is also for the encryption, and finally, the cryptograph is outputted. Triple keys can be same during the process of 3DES encryption, and also can be different, if the keys are same, it is the simple DES algorithm, otherwise, the 3DES achieves the same strength as 168-bit key, and the process of 3DES decryption is the inverse process of the encryption. In the FPGA hardware implementation of 3DES, it uses the design thought of the top-down, and calls DES encryption and decryption module for several times, and finally the 3DES algorithm realized [10].

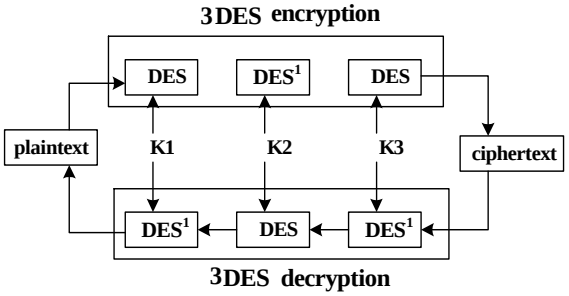

Fig. 7. The diagram of 3DES encryption/decryption implementation.

4.4. Local Bus Interface Module

Local bus interface module is a module of achieving the data exchange between the 3DES module in FPGA and local bus interface module. Its basic function is to realize the operation of data reading, to read the plaintext of the latch decrypted by the 3DES into the PCI9030 local bus side, so as to realize the data exchange between the module and PMC bus (host computer).

PCI9030 is PLX company launched a PCI - Local Bus interface chip of bridge, it converts the PCI signal to a Local Bus. Developers don't need to take care too much PCI Bus details, only need to operate through the Local Bus, and it can conveniently design module based on PCI Bus. There are many configuration registers in the PCI9030 internal, through operating these registers, the local bus configuration can be carried out, mainly including local address space scope, local space base address registers, the description registers of the local address space. The address space in the design of size, type, parameters such as the number of address space, can be configured, and different access width and speed can also set for each address space.

According to the reading, writing and interrupt control sequence of PCI9030 chip, the local read/write operation of interface module is implemented by a state machine. The state transition diagram of local bus is shown in Fig. 8 and shake hands communication of the local bus is finished. One time of read (write) operation contains four bus operating state: idle state(idle), address state (address), data/wait state (data/wait) and recovery state (recovery), among them, the data/wait state is divided into write data state and read data state. Local bus adopts the model of reuse, address/data bus for the LAD, address output line address, accept R_sign data line, line including ADSL, LW_RL, RDL, WRL, BLASTL. Due to the read and write operations using only a single cycle, so in the process of read and write operations omitted some control signal, read and write cycle did not join the wait state.

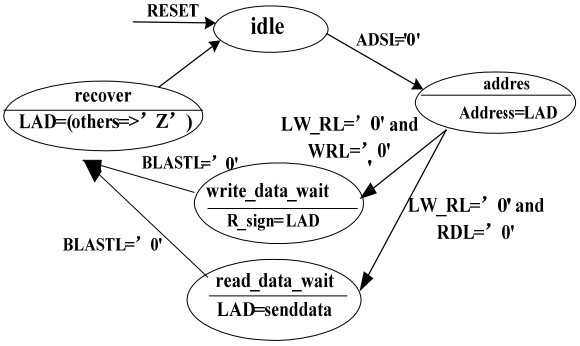

Fig. 8. The state transition diagram of local bus.

5. System Test

Choosing ALTERA corporation Cyclone □ series EP3C25Q240 chip as the FPGA chip in the design, using VHDL language to design A/D controller, serial module and 3DES encryption and decryption module, and function and timing simulation are implemented in the Quartus [9].

Both chips used in this design are EP3C25Q240C8 chip of Cyclone III series of ALTERA company, and the whole design is simulated with function and timing in the Quartus.

The test results show that the encryption system used 2024 LEs, accounts for 8 % of the total 26254 LEs, the decryption system used 5446 LEs, accounts for 20 % of the total Les. It means the hardware resource used by system is relatively few. Fig. 9 is the simulation diagram of encryption system, the Key1_in is the input of key 1, the Key2_in is the input of Key2, and so on. Function_select is the choosing key of encryption and de4- cryption, its high level means encryption and low level means decryption; Data_in that is the 6bit data after processing by AD converter is the input data of 64-bit plaintext; Reset is the reset key; Clock is the system clock signal; Data_out is the output of the 64-bit cryptograph. The simulation result shows that the data_in=(01213456789ABCDEF)H and the password is setted as the weak password, Key1_in =(1111111111111111)H, Key2_in=(AAAAAAAAAAAAAAAA)H, Key3_in=(FFFFFFFFFFFFFFFF), and the data_out of the encryption result is 6DCE0DC9006556A3H. Fig. 10 is the simulation diagram of decryption system, the key is same as encryption and the result of output is (01213456789ABCDEF)H which is same as input data of encryption. Thus, the result verifies the correctness of 3DES encryption/decryption algorithm. We also can conclude from the test results that the procedure time of encryption/decryption is only 10 us per time, and it also verifies the characteristics of high speed of the hardware implementation of 3DES encryption/decryption algorithm.

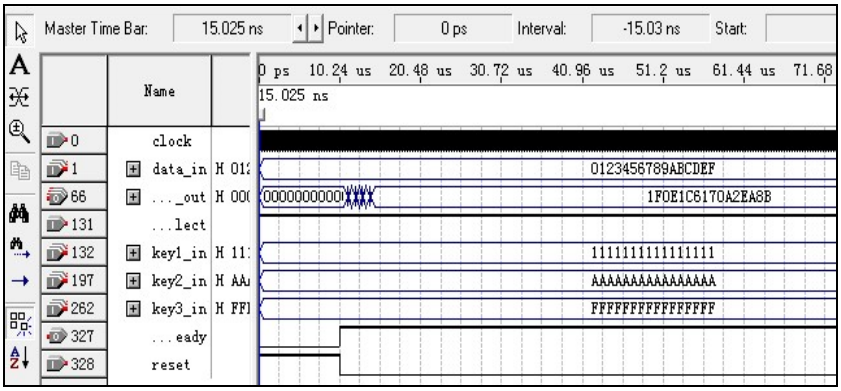

Fig. 9. The simulation diagram of 3DES encryption algorithm.

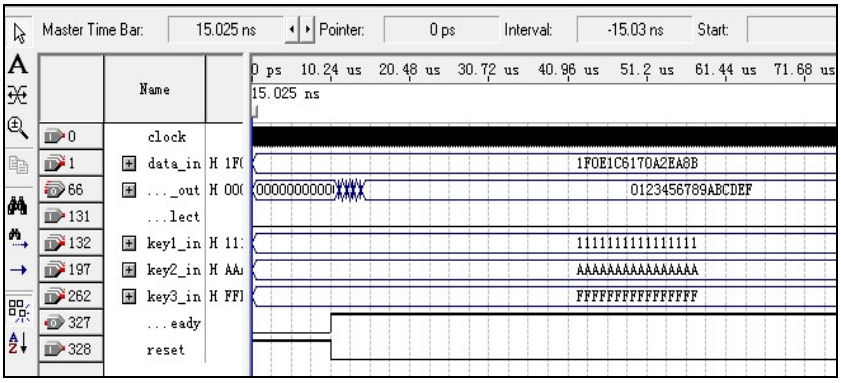

Fig. 10. The simulation diagram of 3DES decryption algorithm.

6. Conclusions

With the development of computer and network technology, the industrial control network in industrial enterprise is applied more and more widely, in order to ensure the confidentiality of the network data transmission, 3DES encryption algorithm of encryption and decryption of data transmission is used in the system, and the 3DES encryption components are implemented with hardware, and it make the encryption intensity high, the speed fast. At the same time, in order to further improve the security of local area network, the custom data transmission protocol of local area network is used, and it improve the flexibility of data transmission [8].

Application of the 3DES encryption technology based on FPGA makes it true that the industrial control network has a broad and safe prospect. The encryption/decryption system is designed in this paper, including the field encryption hardware board and the host decryption hardware board, using the high processing ability of FPGA, the implementation of DES and 3DES in FPGA chip is designed, and the

simulation of the algorithm is completed. The hardware implementation of the algorithm obviously improves the speed of the algorithm from the simulation results, its reliability is greatly enhanced, and the algorithm takes up less hardware resources. After the encryption algorithm is integrated into industrial control network, the information security of the communication network is ensured through the implementing of 3DES encryption for data collected and transmitted in the field. Thus this system can be widely used in the scene of important data encryption or some other scene of needing first-hand information.

References

[1]. Liu Bai Fen, Zhang Hua, Wang Yi, Application of the encryption technology based on DSP in industry, *Application of Electronic Technique*, March 2008, pp. 130-132.

[2]. Liu Ze-Wen, Tang Liu-Chun, Design and Implementation of Security Network Adapter Based on SOPC, *Computer Engineering*, Vol. 34, No. 14, July 2006, pp. 246-248.

[3]. PCI9030 Data Book Version 1.4, *PLX Technology Inc.*, May 2002.

[4]. Li Qian, Wang Xue Gang, Li Han Zhao, An implementation of FPGA security based on 3 - DES algorithm, *Application of Electronic Technique*, January 2008, pp. 132-134.

[5]. Yao Ji, Liu Jian Hua, Fan Jiu Lun, FPGA implementation of DES encryption arithmetic with dynamic key management, *Application of Electronic Technique*, July 2009, pp. 145-148.

[6]. Chen Yan, Wei Xing, Zhong Wei, Application of DES encryption algorithm based on FPGA to optical transmission equipment, *Optical Communication Technology*, October 2012, pp. 47-49.

[7]. Wang Li, Wang Youren, Design of Reconfigurable System of DES and tri-DES, *Computer Measurement & Control*, Vol. 17, No. 4, 2009, pp. 751-753, 772.

[8]. Xia Shu-Hua, DES and RSA encryption algorithm based on the data security transmission technology research, *Manufacturing Automation*, Vol. 33, No. 1, January 2011, pp. 180-182.

[9]. Xue Shang Wu, Hardware Design of Secured Module of Network Interface, *Xidian University*, Xian, pp. 25-27.

[10]. Zhao Yong Chao, The Design and Implement of 3DES in CA System, Shang Hai, *Fu Dan University*, pp. 31-38.