Design of a Softdog based on FPGA*

Yulin Zhang, Xinggang Wang
School of Information Science and Engineering, University of Jinan, Jinan, China
wxg23@163.com

Abstract—**This paper presents a design of softdog based on FPGA and describes hardware and software design. PC applies the CP2103 to transfers data via the USB to the FPGA device without modifying the application. The SPARTAN XC2S200 FPGA is the core of the softdog. It completes acquiring, processing and sending data. Taking the AES as Encryption algorithm, the design can be working at 255.875MHz using 1520 slices to encrypt data. This method is suitable for the application of the low-cost encryption chip that the data throughput is not critical.**

***Keywords*—Softdog; FPGA; AES**

I. INTRODUCTION

Softdog[1] is combined with hardware and software, which is used by software developers to protect research achievements and software copyright. The difference between the traditional software encryption and pure hardware one is a kind of intelligent Personal Computer (PC) software encryption methods. Pure software encrypted password is mainly comprised by password way, calibration style and key disk. What's more, it can use some unique ways to verify the legitimacy of the users, which does not need additional hardware support, such as software installation key, registered ways. But the shortcomings are poorly encrypted intension, easily copied and decoded features. Pure hardware encryption is usually realized by adding certain circuit in parallel or serial and pulling up or down the signal and control lines. And it is easily copied. Softdog is a smart encryption tool which is installed in parallel, serial port or USB interface with CPU processor. When the software is running, procedures command to the encryption dog plugging in computer. And encryption dog make quick calculation, inquiry, encryption transformation and response instantly. Only the correct response can guarantee the software running smoothly. If not, the program will not run correctly. Compared with traditional methods, the softdog is more strong and difficult. And each encryption dog can combined with a kind of software, which will strictly control software access.

The design of softdog has not stereotyped pattern to follow. Also because of this, softdog is worth of existing for software encryption. The paper introduced a kind of softdog which the SPARTAN XC2S200 FPGA [2] is the core. It uses the USB port to communicate with the PC. Softdog achieves with this method has its unique characteristics such as the structure is simple, is very difficult to explain, stable and reliable.

The rest of the paper is organized as follows. Section 2 deals with the hardware design of this softdog. Section 3 presents the software. Section 4 shows the result of our implementation. Finally, Section 5 concludes the paper.

II. HARDWARE DESIGN

The FPGA is the core of the softdog. We choose the SPARTAN XC2S200 FPGA for our design .It has 4320 logic cells, 30Kbits of total block RAM, 216Kbits of total distributed RAM, four Digital Clock Managers (DCMs) and so on. It is ideally suited to a wide range of consumer electronics applications, including broadband access, home networking, display/projection and digital television equipment. Through the use of the DCM feature, this device provides flexible, complete control over clock frequency, phase shift and skew. Fig.1 shows the hardware design of this softdog which the core is SPARTAN XC2S200 FPGA. We use the CP2103 chip [3] which can translate the USB format data to the UART one. So the FPGA can use this method to communicate the data with the Virtual COM Port (VCP) device.

A. CP2103

The CP2103 is a highly-integrated USB-to-UART Bridge Controller providing a simple solution for updating RS-232/RS-485 designs to USB using a minimum of components and PCB space. The CP2103 includes a USB2.0 [4] full-speed function controller, USB transceiver, oscillator, EEPROM, and asynchronous serial data bus (UART) with full modem control signals. No other external USB components are required. We can program the on-chip EEPROM to make the chip as a COM port which is called as virtual COM port (VCP). It implements all RS-232/RS-485 signals, including control and handshaking signals, so existing system firmware does not need to be modified. The UART supports RTS/CTS, DSR/DTR, and X-On/X-Off handshaking. The UART is programmable to support a variety of data formats and baud rates. If the Virtual COM Port drivers are used, the data format and baud rate are set during COM port configuration on the PC. The details of this chip are shown in [3].

The used signals of the CP2103 are shown in Table I. We use only nine pins of this chip. The rest are vacant.

The SPARTAN XC2S200 FPGA needs power of 3.3V which is the voltage regulator output of this chip. So we can use this signal to imply the power of the FPGA. This does not require level translation.

* Project supported by Shandong Doctor Fund(03BS005) and NSF of Shandong (Y2007G46)

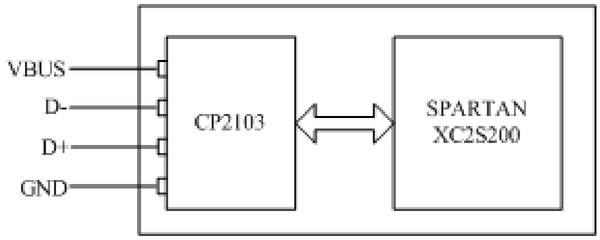

Figure 1. Hardware design

Table I. The Used Signals of the Vcp

Pin#	Signals		
	Name	***Signal***	***Description***
1	VBUS	PC	Ring Indicator control input
2	GND		Ground.
3	D+	PC	USB D+
4	D-	PC	USB D-
6	VDD	VCP	3.3 V Voltage Regulator Output
22	CTS	FPGA	Clear To Send control input
23	RTS	VCP	Ready to Send control output
24	RXD	FPGA	Asynchronous data input
25	TXD	VCP	Asynchronous data output

In order to make softdog system communicate well, we use master-slave mode. The CP2103 chip is the master and the SPARTAN XC2S200 FPGA is the slave. Data frame is the best choice to make the communication very well. The frame of translating or receiving data consists of 20 bytes. The first two and the last two of them are the start and end flag. The 16 bytes in the middle are the valid data. The form of each translating byte which meets the serial communication protocol is shown in Fig.2.

The protocol for the CP2103 is as follow.

- When the PC has data to be encrypted, the CP2103 get the data and translate to the XC2S200 FPGA using the VCP. It waits for a moment to get the responding data frame.
- The CP2103 communicate with the XC2S200 FPGA before getting the responding data frame.
- In every frame, the first two bytes is the start flag and the last two are end one.
- Every translating byte meets the serial communication protocol.

When the CP2103 translates data to the FPGA using the VCP, the RTS signal which XC2S200 FPGA monitors. The XC2S200 FPGA makes the counters zero to get ready to receive the data and set the CTS high to respond. The CP2103 gets the signal and starts to translate data using the TXD signal. The first two bytes are the 'FFFF' which is the beginning of the frame. The third byte is the first byte of valid data and so on. The last two bytes are the 'FFFF' which is the end of the frame.

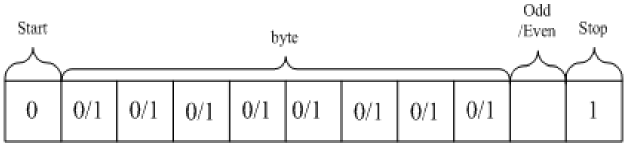

Figure 2. The form of each translating byte

The CP2103 receives data from the XC2S200 FPGA using the only RXD signal. The frame of data is the same as the translating data. It does not stop because the VCP of the CP2103 can receive the data automatically. The CP2103 translate this data to the PC.

B. =SPARTAN XC2S200 FPGA Design

The SPARTAN XC2S200 FPGA is the core of the softdog. It completes acquiring, processing and sending data. The operations of acquiring, processing and sending data can be implemented using the Verilog HDL language. The ModelSim simulator is used.

1) Acquire and send data

The receiving data meet the serial communication protocol. We can implement the serial-to-parallel converter. This can get the valid bytes one by one. In our design, we process the data unit of 128 bits. With the funnel principle, we splice bytes to get the 128 bits using counter. Fig.3 shows the funnel principle.

When receiving the valid byte, it can pull into the top of the funnel instead of the former one. The former one is send into the situation whose number is 15. The next bytes do the same treatment. When the counter's number is 16, the valid data of the frame is completed. So the 128 bits data can be taken away and be processed. Fig.4 shows the simulating result of acquiring data.

When sending the processed data, we can implement the opposite way. The data should be in the funnel. Completed sending one byte, we can get another from funnel. When the counter's number is 16, the processed data is sent over. The simulating result of sending data is shown in Fig.5

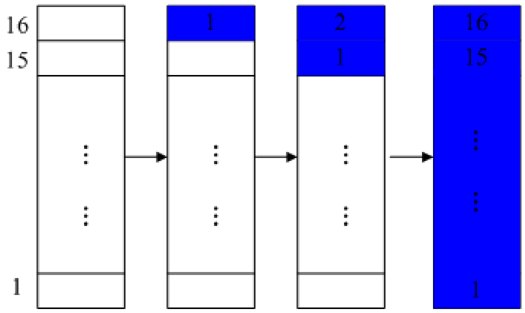

Figure 3. The funnel principl

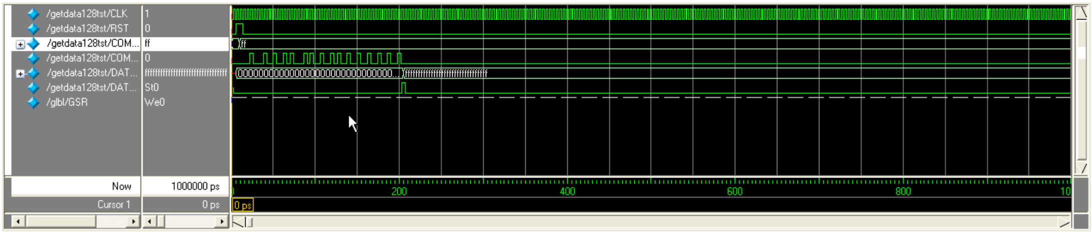

Figure 4. Acquiring data

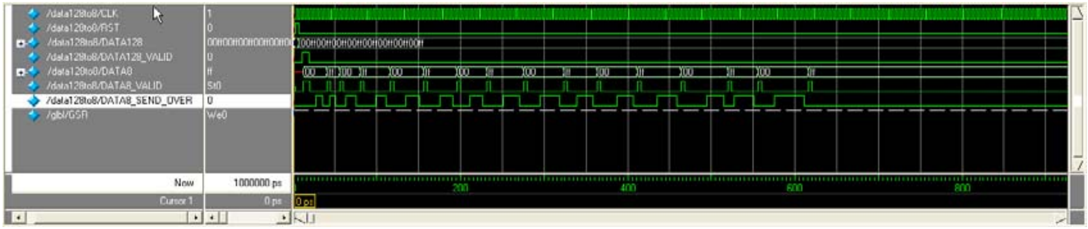

Figure 5. Sending data

2) AES design

The important part of this design is the processing data. We take the AES [4] as Encryption algorithm. The AES algorithm is a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. The algorithm may be used with the three different key lengths and therefore these different "flavors" may be referred to as "AES-128", "AES-192", and "AES-256". In our design, The AES-128 is implemented. It includes the encryption process and the key expansion process. The encryption process includes an initial round of the initial key addition (AddRoundKey), nine rounds transformation (Round) and final round transformation (FinalRound). Every round, except the final round does not have the MixColumn, has SubBytes, ShifRow, MixColumn and AddRoundKey. The key expansion process produces the round key which is needed in the AddRoundKey process. The details of the AES algorithm are in [4].

Fig.6 shows the simulating result of the processing data operation.

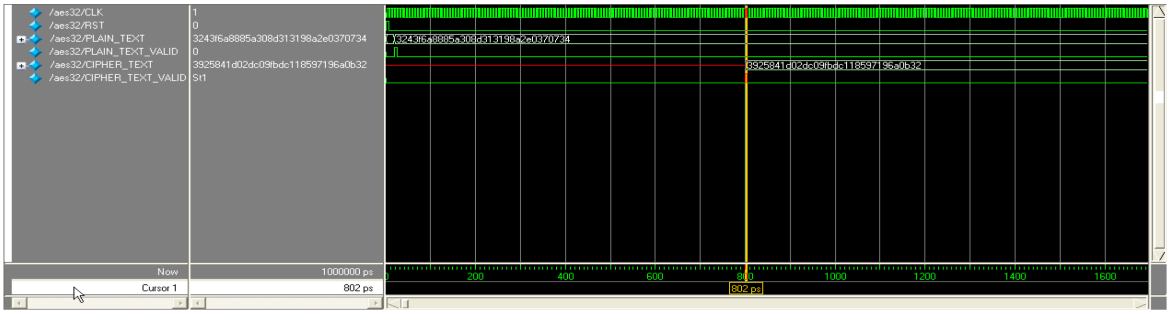

Figure 6. The simulating result of the processing data operation

III. Software design

The parts of software design are the VCP device driver, the USB driver and the application.

We can download the VCP device drivers from the chip development company. It allows a CP2103-based device to appear to the PC's application software as a COM port. Application software running on the PC accesses the CP2103-based device as it would access a standard hardware COM port. Existing COM port applications may be used to transfer data via the USB to the CP2103-based device without modifying the application.

The USB driver connects the underlying hardware and the upper applications. In our design, we use the WinSDK developing the driver. The driver should make the encrypted data meet the translating requirements such as the form of the frame data.

Advanced application built on top of the drivers. In this design, it means the interface function of the softdog. We can use the VC6.0 as the development platform to develop this application and make it as the DLL files embedded in protected software and called for by software.

IV. The result of our design

In our design, we use the CP2103 chip, the SPARTAN XC2S200 FPGA and other hard resource. The core of the softdog has been implemented using Veilog HDL. The Xilinx's ISE 9.2i tool for synthesis, place and route is used. The results after synthesis are shown in Table II

Our design for the data processing can be working at 255.875MHz. It supports a variety of baud rates.

V. Conclusion

In this work, we have presented a design of softdog based on FPGA. Our design uses the CP2103 which is a highly-integrated USB-to-UART Bridge Controller and the SPARTAN XC2S200 FPGA. The SPARTAN XC2S200 FPGA completes acquiring, processing and sending data. We take the AES as Encryption algorithm. Our design for the data processing can be working at 255.875MHz using 1520 slices. It supports a variety of baud rates.

Table 2. The Results after Synthesis

	Device Utilization Summary		
Logic Utilization	***Used***	***Available***	***Utilization***
Number of Slices	1520	1920	79%
Number of Slice Flip Flops	1048	3840	27%
Number of 4 input LUTs	2878	3840	74%
Number of bonded IOB	4	141	2%
Number of BRAMS	2	12	16%
Number of GCLKs	3	8	37%
Number of DCMs	1	4	25%

References

1. LI Ming and SHEN Ting, “Design of a USB Software Dog,” Chinese Journal Of Electron Devices, Vol.9, Mar.2006, pp.0205-0208, doi: CNKI:SUN:JDGC.0.2007-07-016.
2. Product Specification, Spartan-3 FPGA Family Data Sheet,2009.
3. SINGLE-CHIP USB TO UART BRIDGE (CP2103),2007.
4. National Institute of Standards and Technology (US), Advanced Encryption Standard.