基于SiTCP通信协议的FPGA可回滚远程固件更新方法

陈 长[1,2,3] 王 铮[1,3] 胡 俊[1,3]

1（中国科学院高能物理研究所 北京 100049）

2（中国科学院大学 北京 100049）

3（核探测与核电子学国家重点实验室 北京 100049）

摘要 针对高能物理实验的电子学系统中采用传统方式更新现场可编程门阵列（Field Programmable Gate Array，FPGA）固件，存在所处环境复杂不便现场操作和设备数量众多的限制问题，提出了一种利用SiTCP（Silicon Transmission Control Protocol）通信协议向远端电路板发送固件信息、并由板上的FPGA对Flash进行编程以更新固件的方法。该方法无需额外芯片，内建安全机制保证FPGA正常工作，适合通过网络远程操作，具备同时更新多块FPGA固件的能力。

关键词 现场可编程门阵列，远程更新，SiTCP，回滚

中图分类号 TL82

DOI: 10.11889/j.0253-3219.2020.hjs.43.110401

FPGA remote firmware update method based on SiTCP communication protocol with rollback function

CHEN Zhang[1,2,3] WANG Zheng[1,3] HU Jun[1,3]

1(*Institute of High Energy Physics*, *Chinese Academy of Sciences*, *Beijing 100049*, *China*)

2(*University of Chinese Academy of Sciences*, *Beijing 100049*, *China*)

3(*State Key Laboratory of Particle Detection and Electronics*, *Beijing 100049*, *China*)

Abstract **[Background]** Field programmable gate array (FPGA) is widely used in many places, including readout system of large-scale high-energy physics experiments. This kind of experiments usually has large electronic systems with thousands of channels implemented together with FPGAs. Furthermore, these detectors and electronics are often located in special environments such as radiation field, under water or underground, hence the traditional single FPGA update method with joint test action group (JTAG) cable becomes unsuitable or inapplicable. **[Purpose]** This study aims to realize FPGA remote firmware update without additional Ethernet chips or network protocol, and ensure the security mechanism of the process and multi-FPGA updating extendibility in the future. **[Methods]** A new approach using silicon transmission control protocol (SiTCP) technique was proposed. The update firmware in the UDP packages was sent under the SiTCP protocol by MATLAB in host computer to FPGA, and the process of Flash memory programming to update firmware was dominated by FPGA, placing the role of PHY and MAC chips. The secure rollback function was implemented in the modified structure of FPGA firmware with separate update data area and original data area. **[Results]** UDP broadcasting has the ability to multi-FPGA updating, remote firmware update

第一作者：陈长，男，1994年出生，2016年毕业于南华大学，现为博士研究生，研究领域为核电子学与核探测技术

通信作者：王铮，E-mail：wz@ihep.ac.cn

收稿日期：2020-07-24，修回日期：2020-08-15

First author: CHEN Zhang, male, born in 1994, graduated from University of South China in 2016, doctoral student, focusing on nuclear electronics and nuclear detector technology

Corresponding author: WANG Zheng, E-mail: wz@ihep.ac.cn

Received date: 2020-07-24, revised date: 2020-08-15

is achieved and tested the secure rollback mechanism well. **[Conclusions]** This method is suitable for remote operation with advantages such as no need for additional Ethernet chips, built-in safety function to fall back to a known situation, and extendibility of multi-FPGA updating.

Key words FPGA, Remote update, SiTCP, Roll back

在大型高能物理实验领域，探测器的集成度越来越高，对后端读出电子学数据处理及数据传输能力的要求也越来越高；现场可编程门阵列（Field Programmable Gate Array，FPGA）作为可编程器件以其强大的数据处理能力、丰富的高速数字接口设计和灵活的功能实现，成为高能物理实验电子学系统中的核心器件之一。常用的FPGA多属于掉电易失器件，每次上电时都需要从板上Flash存储器加载固件到片上内存（Random Access Memory，RAM）才能实现相应功能。

需要更新固件时，专用上位机软件通过JTAG（Joint Test Action Group）加载器将数据发送给FPGA，对Flash进行编程，修改存储内容；再次上电时，FPGA从Flash内加载更新后的固件。JTAG加载器还能直接向FPGA的片内RAM发送固件，这种方式耗时更少，但重新上电后内容丢失。这两种方式都需要在现场通过线缆接到电路板上的预留JTAG接口进行操作，而大型高能物理实验的探测器和电子学系统往往安装在地下、水下、辐射场等特殊环境中；因此，使用传统的专用JTAG线缆对单个FPGA进行更新变得不再合适。

1 背景介绍

大型高能物理实验的电子学系统中普遍实现了FPGA远程更新功能。北京谱仪第三代（Beijing Spectrometer，BESIII）改造工程的Muon鉴别器电子学读出系统采用了PLD（Programmable Logic Device）器件控制的Multi-Passive Serial配置方式[1]：更新固件通过VME（Versa Module Eurocard）总线发送给接口FPGA，对其附属的Flash进行编程；接口FPGA再向各条链路的主控FPGA发送固件，主控FPGA完成对其附属Flash的编程；最后每条链路的主控FPGA向各电子学插件下发固件，完成665块FPGA的更新。

CMS（Compact Muon Solenoid）实验的电磁量能器off-detector电子学系统共有738块使用FPGA的电路板，研究人员设计了JTAG分发板（JTAG Distribution Board，JDB），它和其他电子学插件都安装在VME机箱内；JDB作为电脑和需要远程更新的电路板之间的桥梁，电脑连接到JDB，通过VME机箱背板的MTM（Module Test and Maintenance）总线来连接其他插件，或者由JDB直接接出多根JTAG信号线到其他插件[2]。

ITER（International Thermonuclear Experimental Reactor）实验由于处于强中子辐射场，其电子学系统主控板通过PCIe（Peripheral Component Interconnect express）链路连接到上位机，由上位机接收远端发来的更新固件并下发给FPGA[3]。江门中微子实验（Jiangmen Underground Neutrino Observatory，JUNO）为了精确采集波形而采用了源端数字化方案，整个读出电子学系统包含近7 000块电路板，密封置于水下靠近探测器的位置。该电路板上使用一块较小的FPGA作为控制器，通过网络接收固件，专用于给主FPGA进行更新[4]。其他如北京同步辐射装置上实验站的像素探测器读出系统，也因为处于辐射环境而采用基于XVC（Xilinx Virtual Cable）技术的远程更新方法[5]，利用ARM处理器模拟JTAG时序对FPGA片内RAM进行配置。

综上所述，现有的FPGA远程更新方法，一般需要额外的器件或设备，如PLD、ARM等，增加了硬件设计复杂度和成本；额外器件也降低了系统的可靠性，如更新过程中额外辅助器件出错且无法恢复，将造成无法修复的系统崩溃。本文提出并实现了一种基于SiTCP（Silicon Transmission Control Protocol）协议的可回滚远程更新方法，利用板上现有的数据传输接口，无需额外硬件；且带有安全机制，保证FPGA能从更新故障中恢复，提高可靠性。

2 方法及实现

本设计在FPGA内实现纯硬件的TCP/IP网络协议，结合Xilinx的QuickBoot功能，无需外部额外硬件配合，实现远程通过网络协议更新FPGA固件的目标。同时调整Flash内固件存储的结构，添加跳转指令和一块存放早前版本固件的区域，实现故障情况下的回滚功能；更新出错后，下次上电会加载早前正确版本的固件。

2.1 硬件设计

本设计中的FPGA更新方式不依赖于外部硬件设计，因此采用了一块自设计的板卡。硬件电路包括一块Xilinx XC7K325T系列FPGA，一块用于存储FPGA固件的Micron N25Q256A Flash存储器，外部

接口为基于SFP(Small Form-factor Pluggable)的网络接口,实物如图1所示。

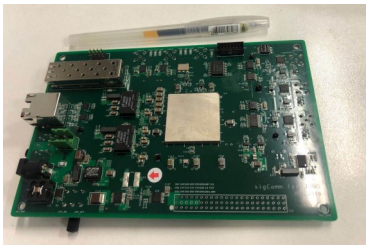

图1 测试板实物图
Fig.1 Photograph of a test board

2.2 FPGA固件设计

FPGA固件主要包括以下模块:基于SiTCP的网络传输模块、FIFO(First In First Out)缓存、远程更新的FSM(Finite State Machine)状态机和控制Flash读写的SPI(Serial Peripheral Interface)接口[6]。

SiTCP协议[7]是一款商用的、基于硬件的TCP/IP协议,用FPGA硬件描述语言的代码和Xilinx的IP核实现了从传输层到数据链路层的功能,因而不需要MAC(Media Access Control)硬件控制器。本设计中,使用FPGA的高速数字接口GTX(Gigabyte Transceiver)作为物理层的PHY(Physical)接口,因此无需外部额外的PHY芯片,从而完全在FPGA内实现了硬件的TCP/IP协议。这种基于FPGA实现TCP/IP协议的方法,无需额外以太网芯片,降低了硬件设计复杂度和成本,有较好的灵活性,被一些高能物理实验的电子学读出系统所采用[8-9]。

经SiTCP解析后的数据,以8 bit的长度送入FIFO进行缓存,然后以32 bit的长度送给FSM状态机。作为远程更新功能的核心控制模块,状态机完成以下功能,其状态转换如图2所示。

1)查询指定寄存器的值,确定是否开始远程更新操作。

2)远程更新开始后,先执行擦除Flash内跳转指令的动作。跳转指令的作用是当FPGA加载到此处时,指定跳转到特定位置继续加载。所以当跳转指令存在时,FPGA会跳转到更新区域去加载固件;反之则会在当前位置继续向后加载,读取到的就是回滚区域内的早前版本的固件。因此跳转指令是保证更新异常后FPGA仍能正常工作的关键。

3)擦除更新区域的内容;接收上位机发送的固件数据,写入更新区域。

4)回读更新区域的内容,计算CRC(Cyclic Redundancy Check)校验值,并与写在更新区域末尾的校验值进行比较。

5)CRC校验通过后,进行写跳转指令的操作,更新完成。

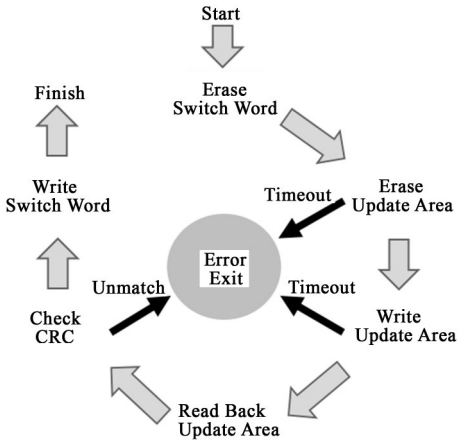

图2 远程更新状态机跳转示意图
Fig.2 State transition diagram of the remote update process

SPI接口模块是一个串行/解串器,接收状态机的8 bit数据输出,以串行方式输出到Flash的DQ0管脚。模块输出的Flash读写时钟spiclk需要通过原语STARTUPE2连接到FPGA专用管脚CCLK上,再连接到Flash,用于驱动Flash读写,如图3所示。

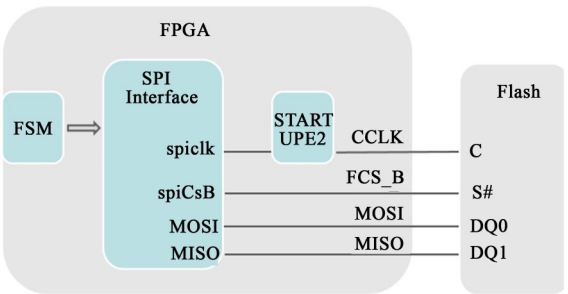

图3 spiclk共享FPGA专用管脚CCLK连接示意图
Fig.3 Block diagram for user spiclk pin connected to FPGA dedicated CCLK pin using Xilinx STARTUPE2 primitive

2.3 FPGA固件的生成与处理

FPGA固件设计完成后,用Xilinx提供的ISE设计软件生成bit文件,该文件可写入FPGA片内RAM用于直接加载,但掉电后会丢失固件信息;也可进一步生成mcs文件写入Flash中,掉电后不会丢失,FPGA将在上电后自动加载Flash中的固件信息。

为了实现回滚功能,需要在生成mcs文件时进行一些特殊处理。普通的mcs文件只包含一块存放固件的区域,本设计中的mcs文件包含两块区域(回滚和更新区域)及跳转指令,示意图见图4。首先,将这份包含跳转指令、回滚区域和更新区域的固件通过传统的JTAG方式下载到Flash。当需要更新固件时,新的固件也要含有§2.2中所述的必要FPGA功能模块,且状态机内的更新区域起始地址保持不

变。由于mcs文件中不仅包含要写入Flash的数据，还有地址和校验位；而新的固件会在状态机的控制下写入特定的Flash地址，因此需要生成不含地址和校验位的bin文件，用于上位机向FPGA发送。

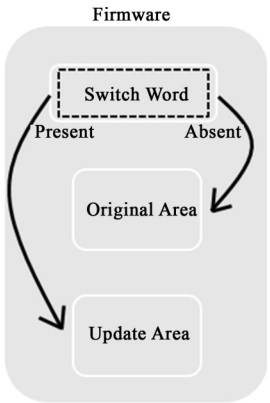

图4 实现回滚功能所需的固件结构，跳转指令是否存在将决定加载方向

Fig.4 Firmware structure for rollback function, existence of switch word determines FPGA loading process

2.4 上位机固件发送程序

使用MATLAB编写发送程序，该软件封装了UDP函数，使用方便。写好FPGA的IP地址和端口号，即可建立UDP连接。以读的形式打开bin二进制文件，遍历文件以获取字节数。按照SiTCP的UDP包格式[7]来组装要发送的数据，设置一个包内的数据长度，按照数据长度读取二进制文件，向FPGA进行发送。程序流程图如图5所示。FPGA解析得到数据后由两个功能模块分别完成Flash编程的状态控制，以及与Flash的SPI接口功能。

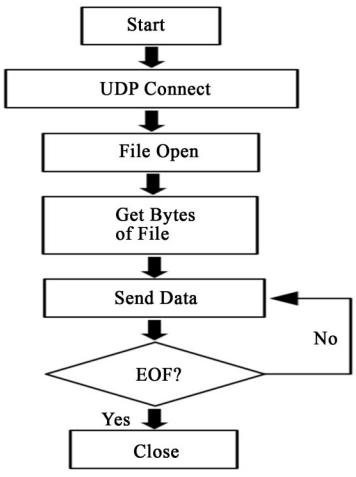

图5 上位机固件发送程序流程图

Fig.5 Flow chart of MATLAB sender in host computer

3 功能测试

按照§2.3的步骤生成一份三段式的固件，通过JTAG方式下载到Flash并加载到FPGA。拨动板上拨码开关以置位寄存器，开始远程更新流程。等待Flash擦除操作完成后，上位机运行MATLAB程序，通过网络协议向FPGA发送一个版本号和功能均不同的更新固件，开始写Flash。CRC校验以及写跳转指令完成后，一系列寄存器会置位以表示不同的状态，如CRC校验是否通过、跳转指令是否写入、更新是否完成，以及一系列错误提示如超时等。提示更新正常完成且无错误指示，重新上电；可见LED以不同的方式闪烁，使用Xilinx的iMPACT软件读取到正确的自定义版本号UserID，说明远程更新成功。

安全回滚功能的测试，以在更新过程中断掉电源的方式进行。经多次验证，在更新过程中不同时点掉电（发生异常），再次上电后FPGA均可以回滚到早前版本的固件，不至于无法工作。

4 结语

本文介绍了一种带有回滚功能的FPGA远程更新方法。该方法基于SiTCP通信协议，由上位机向FPGA发送更新固件，对Flash进行编程，无需增加额外以太网芯片或辅助器件。它有以下特点：利用FPGA自身资源实现PHY和MAC芯片的功能，不需要额外芯片且具有灵活性，降低了硬件设计成本和复杂度；带有保障机制，更新异常时可以回滚到安全的版本正常工作，提高了可靠性；对于使用SiTCP作为网络传输协议的电子学系统，不需要集成其它通信协议；采用UDP协议发送固件，能利用广播向多个FPGA发送，具有扩展性。

参考文献

1 周雷, 梁昊, 虞孝麒, 等. 基于串行存储器的FPGA在线高速重载[J]. 核电子学与探测技术, 2008, **28**(3): 593−595. DOI: 10.3969/j.issn.0258-0934.2008.03.036.
ZHOU Lei, LIANG Hao, YU Xiaoqi, *et al*. FPGA high-speed on-line configuration using flash memory[J]. Nuclear Electronics & Detection Technlogy, 2008, **28**(3): 593−595. DOI: 10.3969/j.issn.0258-0934.2008.03.036.

2 Da Silva J C, Konoplyannikov A, Vlassov E. Remote reprogramming of FPGAs on the CMS ECAL off detector electronics[J]. Jounal of Instrumentation, 2012, **7**(02): C02010.

3 Fernandes A, Pereira R C, Sousa J, *et al*. FPGA remote update for nuclear environments[J]. IEEE Transactions on

Nuclear Science, 2016, **63**(3): 1645−1649. DOI: 10.1109/TNS.2016.2559478.

4 Bellato M, Bergnoli A, Brugnera A, *et al*. Embedded readout electronics R&D for the large PMTs in the JUNO experiment[EB/OL]. [2020-07-08]. https://arxiv. org/abs/2003.08339.

5 薛乾, 曾云, 张杰. 基于XVC网络协议的多FPGA远程更新与调试[J]. 核技术, 2015, **38**(12): 120402. DOI: 10.11889/j.0253-3219.2015.hjs.38.120402.
XUE Qian, ZENG Yun, ZHANG Jie. Remote updating and debugging multi-FPGA based on XVC internet protocol[J]. Nuclear Techniques, 2015, **38**(12): 120402. DOI: 10.11889/j.0253-3219.2015.hjs.38.120402.

6 QuickBoot method for FPGA design remote update[OL]. [2020-07-08]. https://www.xilinx.com.

7 Uchida T. Hardware-based tcp processor for gigabit ethernet[J]. IEEE Transactions on Nuclear Science, 2008, **55**(3): 1631−1637. DOI: 10.1109/TNS.2008.920264.

8 Teoh J J, Hanagaki K, Ikegami Y, *et al*. Development of readout system for FE-I4 pixel module using SiTCP[J]. Nuclear Instruments & Methods in Physics Research Section A - Accelerators Spectrometers Detectors and Associated Equipment, 2013, **731**: 237 − 241. DOI: 10.1016/j.nima.2013.05.161.

9 Satoh S, Muto S, Kaneko N, *et al*. Development of a readout system employing high-speed network for J-PARC[J]. Nuclear Instruments & Methods in Physics Research Section A - Accelerators Spectrometers Detectors and Associated Equipment, 2009, **600**(1): 103−106. DOI: 10.1016/j.nima.2008.11.054.