Design of a 10-Gbps Random Number Recorder

Yi Qian , Futian Liang , Houbing Lu, Xinzhe Wang , and Ge Jin

***Abstract*–We design a Data Acquisition (DAQ) system for a 10-Gbps true random number generator to verify the quality of the random number. The prototype of the DAQ is based on a Xilinx Vertex-6 FPGA evaluation board. The DAQ system has three parts: acquisition, cache, and data up-link. Acquisition is the interface to the high-speed random data, and we use Gigabit Transceiver (GTX) in FPGA to deserialize the random data. The 1Gbps high speed serial random data in each channel is deserialized into 62.5Mbps with 16bit width parallel data. The low speed parallel data can be handled by the FPGA code and cache the data in an external DDR3 memory. When enough random data is stored, the random data is upload to PC via Gigabit Ethernet for the finial verification. The BERT test shows that the total data error rate of the data link in the prototype is less than 6.25×10^{-10} with 1Gbps input. The prototype can cache up to 16Gbits random data with 1Gbps serial input, and it meets the requirements of the data acquisition for one channel of the random number generator and proves the DAQ structure.**

I. INTRODUCTION

Random numbers are required in many areas: cryptography both classical and quantum, Monte Carlo computation, numerical simulation, statistical research, randomized algorithms, etc. There are two kinds of generators, namely pseudo-random generator (PRNG) and true random number generator (TRNG). PRNG expands a relatively short key into a long sequence of random bits based on a deterministic algorithm, their outputs have better statistical properties and the numbers generated are predictable. TRNG generates random bits based on random physical phenomenon or signal source, their output is unpredictable and they have to pass very rigorous tests to be used confidently. TRNG is preferred in applications with high security requirements, such as the cryptographic and security applications.

Nowadays, high density and high data output rate are as important as the quality of the TRNG in the true random number required devices and instruments. For certain cryptographic application, we have design a 10-Gbps true random number generator mircochip which is named TRNG2015 in our previous work. The random number output data rate is up to 1Gbps per channel and up to 10Gbps in total with ten channels.

In order to verify the quality of the random number, we need to record enough continuous data generated from the generator for the National Institute of Standards and Technology Special Publication 800-22 statistical tests (NIST statistical test).

Because of the high data generating speed, we need an ultra-fast data cache device to acquire very long continuous random bit sequence. To get a credible result from the test suite, we plan to acquire at least 1giga continuous random bits for each generator channel at 1Gbps generate rate.

To acquire and store enough quantity of the true random data generated by TRNG2015, we need a high-speed data acquisition which have high data throughput ratio. The system need acquiring and storing the random bits in real time. Therefore, we should concern the speed and capacity of the data acquisition mainly.

With these requirements, the commercial instruments such as the oscilloscope or the logic analyzer cannot acquire the random data at the high rate nor the record depth. So we design a data acquisition system to record the continuous random bits in real time to meet the requirements.

II. HARDWARE IMPLEMENTATION

In this paper, we design a high speed data acquisition to receive and cache these data generated by TRNG2015, then send them to PC for further test, and the prototype is based on a Xilinx Vertex-6 FPGA ML605 evaluation board.

The scheme of the data recording of the TRNG2015 is shown in Fig.1.

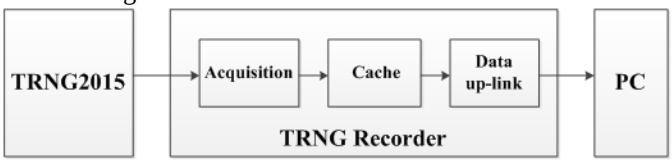

Fig.1 TRNG2015 testing scheme

A. Acquisition

Acquisition is the interface to the high-speed random data. The Virtex-6 FPGA cannot process 1Gbps data directly, when serial data are received, the transceiver must use the same serial clock that serialized the data to deserialize it.

At high line rates, providing the serial clock with a separate wire is very impractical because even the slightest difference in length between the data line and the clock line can cause significant clock skew.

Gigabit Transceiver (GTX) have Clock Data Recovery (CDR) module, so it can recover the clock from the data directly. CDR can operate over much longer distances at higher speeds than their non-CDR counterparts[2].

Manuscript received May 29, 2016. This work is supported by the National Natural Science Foundation of China under grant number 61401422, 11375179, 11375263.

Yi Qian is with State Key Laboratory of Particle Detection and Electronics, University of Science and Technology of China, Hefei, Anhui 230026, and with Hefei Electronic Engineering Institute, Hefei, Anhui 230037, P.R. of China (e-mail: yiqian@mail.ustc.edu.cn).

Futian Liang, Xinzhe Wang, Houbing Lu and Ge Jin are with State Key Laboratory of Particle Detection and Electronics, University of Science and Technology of China, Hefei, Anhui 230026, P.R. of China (e-mail: ftliang@ustc.edu.cn,wxzyf@mail.ustc.edu.cn,luhb@mail.ustc.edu.cn,goldjin @ustc.edu.cn).

978-1-5090-2014-0/16/$31.00 ©2016 IEEE

GTX is a SerDes capable of operating at serial bit rates above 1Gbps. GTXs are used increasingly for data communications because they can run over longer distances, use fewer wires, and thus have lower costs than parallel interfaces with equivalent data throughput.

The Virtex-6 FPGA GTX transceiver is a power-efficient transceiver. The GTX transceiver is highly configurable and tightly integrated with the programmable logic resources of the FPGA. The Virtex-6 FPGA GTX transceivers cover data line rates from 600 Mbps to 6.6 Gbps [3].

Gigabit Transceiver (GTX) in FPGA is used to deserialize the random data. The GTX module works at 1Gbps and deserializes the 1bit width random data to 62.5Mbps and 16bit width parallel data.

B. Cache

To store the high speed true random data from processed from GTX, we need a high speed memory from which we can read and write to easily.

The Virtex-6 FPGA on ML605 is XC6VCX240T，which have 416 block ram blocks and each block ram is 36Kb, and the total ram is 14,976Kb [5]. The on-chip memory space of Virtex-6 FPGA is too small to meet the large quantity of data acquisition.

It is necessary to use an extra memory. DDR3 stands for double-data-rate three and is a random access memory technology used for high speed storage of the working data of a computer or other digital electronic device. The primary benefit of DDR3 is the ability to transfer data for I/O at 8 times the speed of its memory cells, thereby enabling faster bus speeds and higher peak throughput than earlier DRAM memory technologies. In addition, the DDR3 standard allows for chip capacities of 512Mb to 8Gb, effectively enabling a maximum memory module size of 16GB. With the advantage of high speed and large capacity, DDR3 SDRAM is applied as the memory device of high speed data acquisition in this paper.

The Virtex-6 FPGA supports DDR3 memory interface and has memory controller IP which is an interface between a memory controller and a memory device, which can be used and adjusted easily. Memory Interface is a free software tool used to generate memory controllers and interfaces for Xilinx FPGAs and supports DDR3 SDRAM. In this paper, MIG (Memory Interface Generator) IP is used to provide high-performance connections to DDR3 SDRAMs. The DDR3 memory controller is created using the MIG.

We use a DCFIFO_MIXED_WIDTHS to match the data rate and data width between the GTX output and the DDR3 memory controller. Under the control of the DDR3 memory controller, 64 bit width parallel data is cached in an external DDR3 memory at the rate of 800 Mbps, and fill the 2GB memory with continuous random bits.

C. Data up-link

When the DDR3 memory is full filled, the random data is upload to PC for verification. We prefer to transfer these random data via Gigabit Ethernet.

In computer networking, Gigabit Ethernet is a term describing various technologies for transmitting Ethernet frames at a rate of 1Gbps, as defined by the IEEE 802.3-2008 standard. Gigabit Ethernet is more advanced technology than Fast Ethernet having speed of 1000Mpbs, 10 times more than speed of Fast Ethernet, which is 100Mbps. Due to more bit transfer speed and higher bandwidth, Gigabit Ethernet results in better performance than Fast Ethernet.

Xilinx Virtex-6 FPGA provides an optimized TEMAC (Tri-Mode Ethernet Media Access Controller) IP core [8], which can deploy the Xilinx Core generator to configure and generate TEMAC wrapper files that contain a user configurable Ethernet MAC physical interface, e.g., GMII, RGMII. Xilinx also provides a scheme for the physical interface as well as a simple FIFO-loopback example design which is connected to the TEMAC client interface.

The TEMAC IP core enables system designers to implement a broad range of integrated Ethernet designs, from low cost 10/100/1000 Mbps Ethernet to higher performance 2.5 Gigabit ports. The function of the MAC is well defined and fixed for Ethernet protocol. For this reason, the TEMAC IP is used for this design.

In order to match the data rate between the output of DDR3 memory controller and TEMAC IP, The random data read from the DDR3 memory controller is send to a FIFO. 8 bit width data read from the FIFO is send to Gigabit Ethernet transceiver at the speed of 125Mbps, and transmitted to PC at the speed of 1Gps via the RJ45 port.

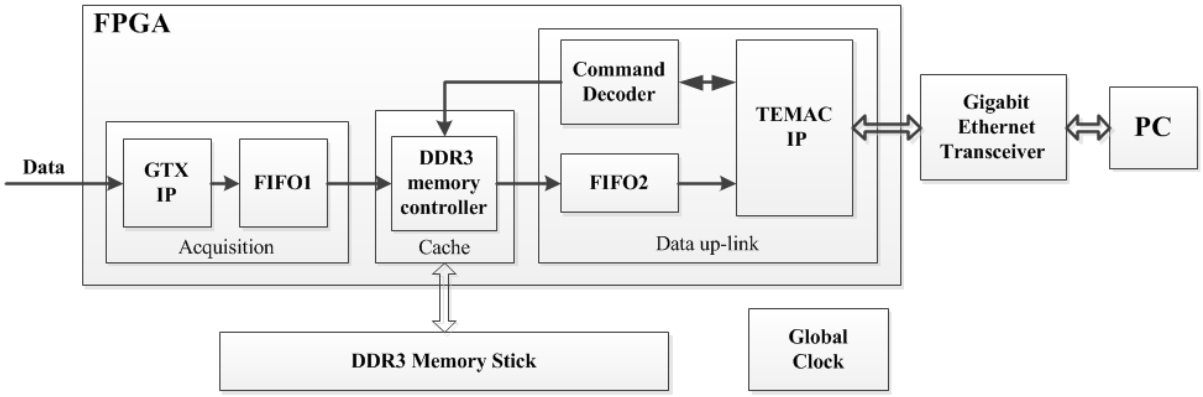

Fig.2 Schematic block diagram of the 10-Gbps Random Number Recorder

D. User interface

In order to operate the DAQ system, a Graphical User Interface (GUI) has been built. The main function of this GUI is recording the data generated by TRNG2015, facilitating the reading and writing, through the user interface. The data memorized will be sent to PC and operated according to the command.

E. Summary

The schematic block diagram of the 10-Gbps Random Number Recorder is illustrated in Fig.2.

The 1bit width random data is connected to GTX IP in FPGA via SMA connectors. GTX IP is the key to slow down the data rate. GTX is pre-configured during the FPGA coding process. 1Gbps and 1bit width data is deserialized to 62.5Mbps and 16 bit width parallel data by the GTX. FIFO1 is used to match the data rate and data width between GTX output and the DDR3 memory controller. The DDR3 memory controller created by MIG IP is the interface of the DDR3 memory stick. 64bit width random data is stored to and read from the DDR3 memory stick at the speed of 800Mbps. When enough data is stored, the data is upload to FIFO2 under the control of the DDR3 memory controller. FIFO2 is used to match the data rate between the output of the DDR3 memory controller and TEMAC IP. 8 bit width data read from the FIFO is send to Gigabit Ethernet transceiver at the speed of 125Mbps. The TEMAC IP in FPGA and transceiver on board is the data link between the user interface on PC and FPGA board. All the process is controlled by the command from the user interface on PC. The different commands can be derived from the command decoder.

III. BERT TEST

A Bit Error Rate Test (BERT) is applied to validate the correctness of the DAQ system. We use some common PRBSs (pseudo random binary sequence) as input data for BERT, such as PRBS7, PRBS15, PRBS23, and PRBS31. The polynomials we use are defined as: PRBS7 = $x^7 + x^6 + 1$; PRBS15 = $x^{15} + x^{14} + 1$; PRBS23 = $x^{23} + x^{18} + 1$; PRBS31 = $x^{31} + x^{28} + 1$.

The target data rate of our design is 1Gbps, so pseudo random binary sequence is transmitted to the DAQ system at the speed of 1Gbps. The Table I shows the result of the BERT test.

TABLE I. RESULTS OF BIT ERROR RATIO TEST

PRBS	Total Bits	Errors	Error Ratio
PRBS7	1.6×10^9	0	$< 6.25 \times 10^{-10}$
PRBS15	1.6×10^9	0	$< 6.25 \times 10^{-10}$
PRBS23	1.6×10^9	0	$< 6.25 \times 10^{-10}$
PRBS31	1.6×10^9	0	$< 6.25 \times 10^{-10}$

From the test results, the DAQ system can require 2GB continuous 1Gbps random data with a bit error ratio smaller than 6.25×10^{-10}. The result of BERT test shows that the total data error rate of the data link in the prototype is less than 6.25×10^{-10}.

The random data acquired by the DAQ system also passed the NIST statistical test for random number. As a prototype, the design is successful from the above test results.

IV. CONCLUSION

In this paper, a prototype of a DAQ system is designed for recording high speed continuous random bits in real time. 1Gbps serial random data is acquired and deserialized by GTX, then the low speed parallel data is cached in the external DDR3 memory. When enough data is stored, we upload these data to PC via Gigabit Ethernet. It is proven that that the prototype meets our requirement both in speed and capacity. The DAQ system works as we expected from the preliminary electrical test results. The total data error rate of the data link in the prototype is less than 6.25×10^{-10}. The random data acquired by the DAQ system also passed the NIST statistical test for random number. So this prototype meets the requirements of the data acquisition for one channel of the random number generator and proves the DAQ structure. The prototype provides a good reference for the next version with ten channel random bit acquisition. The structure of the DAQ system is also a guidance for the similar instrument.

REFERENCES

[1] W.F. Jones, M. Running, L. Draughn, and J. Reed, “ Advanced Hardware Architecture for On-line Data Acquisition in Clinical 3-D PET_smart DRAM PCI Card for 14M Event_sec Histogramming across Terabytes of DRAM”, Nuclear Science Symposium Conference Record, October.2004, vol. 6, pp. 3663-3667.

[2] Torres J, Reig C, Martínez G, et al. Design of Advanced Digital Systems Based on High-Speed Optical Links [M]. INTECH Open Access Publisher, 2012.

[3] Virtex-6 FPGA GTX Transceivers User Guide UG366 (v2.6), Xilinx, 2011. [Online]. Available: http://www.xilinx.com/support/documentation/user_guides/ug366.pdf

[4] LogiCORE IP Virtex-6 FPGA GTX Transceiver Wizard v1.12 User Guide, Xilinx, 2012. [Online]. Available: http://china.xilinx.com/support/documentation/ip_documentation/v6_gtxwizard/v1_12/ug516_v6_gtxwizard.pdf

[5] Virtex-6 CXT Family Data Sheet, Xilinx, 2014. [Online].Available: http://www.xilinx.com/support/documentation/data_sheets/ds153.pdf

[6] Virtex-6 FPGAs Data Sheet: DC and AC Switching Characteristics, Xilinx, 2014. [Online]. Available: http://china.xilinx.com/support/documentation/data_sheets/ds152.pdf

[7] Virtex-6 FPGA Memory Interface Solutions User Guide, Xilinx, 2013. [Online].Available: http://www.xilinx.com/support/documentation/ip_documentation/mig/v3_92/ug406.pdf

[8] LogiCORE IP Tri-Mode Ethernet MAC v5.4 Product Guide, Xilinx, 2012. [Online]. Available: http://www.xilinx.com/support/documentation/ip_documentation/tri_mode_eth_mac/v5_4/pg051-tri-mode-eth-mac.pdf

[9] The ETHERNET Working Group, “IEEE STD 802.32002 specification,” (Last Update: 07 December 2015), http://www.ieee802.org/3/.