21st International Conference on Computing in High Energy and Nuclear Physics **CHEP2015** Okinawa Japan: April 13 - 17, 2015

Contribution ID: **436** Type: **poster presentation**

High Speed Fault Tolerant Secure Communication for Muon Chamber using FPGA based GBTx Emulator

The Compressed Baryonic Matter (CBM) experiment is a part of the Facility for Antiproton and Ion Research (FAIR) in Darmstadt at the GSI. This experiment will examine heavy-ion collisions in fixed target geometry and will be able to measure hadrons, electrons and muons. Muon Chamber (MUCH) is used to detect low momentum muons in an environment of high particle densities. Basic read out chain of MUCH consists of MUCH-XYTER (Front End Electronics), Gigabit Transceiver (GBTx), Data Processing Board (DPB), First level event selector interface board (FLIB) [1]. MUCH- XYTER is a self-triggered Application-Specific Integrated Circuit (ASIC), which is directly connected to the detector and send the receive data to the GBTx through serial peripheral interface (SPI) like E-link. GBTx will be connected to the DPB through 4.8 Gbps optical link. In between DPB and FLIB there will be 10 Gbps optical link and at the end FLIB will be connected to the data acquisition system through Peripheral Component Interconnect Express (PCIe).
As a part of the implementation of read out chain of MUCH in India, we have implemented FPGA emulator of GBTx [2]. GBTx is a radiation tolerant ASIC that can be used to implement multipurpose high speed bidirectional optical links for high energy physics (HEP) experiments. It is developed by CERN. It consists of packet generator, scrambler-descrambler, encoder-decoder, interleaver-deinterleaver, gearbox, and transceiver.Packet generator is used to generate test pattern (either static or dynamic) to test the optical link. Scrambler is used to scramble the data so that clock can be recovered properly in the receiver side. In the encoder block single error correcting (15, 11) Reed-Solomon (RS) encoding is used to mitigate error occurred in the communication channel due to radiation. Interleaver is used to simply interleave the encoded data to make the coded data more robust against burst error. Gearbox is used to divide the 120 bit data frame into three 40 bit wards. These 40 bit wards are transmitted through multi gigabit transceiver (MGT) and reference clock used for MGT is 120 MHz. In the receiver side apart from the predefined block one frame aligner block is also used. Frame aligner is used to detect header in the data frame properly in the receiver side. GBTx will be used in highly irradiated area and more prone to be affected by multi-bit error. To mitigate this effect instead of single bit error correcting (15, 11) RS code we have used two bit error correcting (15, 7) BCH code [3]. It will increase the redundancy, which in turn increases the reliability in the coded data. So the coded data will be less prone to be affected by noise due to radiation. Normally in the wired communication between any two fixed points there will be no such security issue. But when multiple stations will be used for long distance communication the question of security will come into play. So to make the data transmitting through optical fiber more secure, we use advanced encryption standard (AES) (a symmetric key cryptography) [4] is used after channel coding. The AES is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES encryption algorithm acts as a block cipher. The data will be always 128 bit block but the key size can be select from 128 bit, 192 bit or 256 bit. Here for testing purpose we used AES- 128 and AES- 256. In this paper our key contributions can be summarized as follows:
• Implementation of multibit error correcting BCH code to make optical communication more robust against error due to radiation.
• Implementation of AES along with GBTx to make the data communication more secure.
We have implemented GBTx emulator on two Xilinx Kintex-7 boards (KC705). One will act as transmitter and other will act as receiver and they are connected through optical fiber using small form-factor pluggable (SFP) port. We have performed the run-time verification of the system using Xilinx Chipscope Pro Analyzer and also measured the resource utilization, throughput and power utilization of the implemented design.

References:
1. FLES/DAQ summary and Outlook, 24th CBM week, Walter F.J. Müller, FAIR, Darmstadt

2. S. Baron, M. Barros Marin, "GBT-FPGA user guide,"Version 1.00.
3. Error Detection and Correction using BCH code, Hank Wallance, 2001.
4. A.M Deshpande, M.S Deshpande, D.N Kayatanavar, "FPGA implementation of AES encryption and decryption,"International Conference on Control, Automation, Communication and Energy Conservation (INCACEC), 2009.

Primary authors: Mr SAU, Suman (Calcutta University); Mr MANDAL, Swagata (VECC,Kolkata)

Co-authors: Dr CHAKRABARTY, Amlan (Cacutta University); Mr SAINI, Jogender (VECC,Kolkata); Dr CHATTAPADHYA, Subhasis (VECC,Kolkata)

Presenter: Mr SAU, Suman (Calcutta University)

Track Classification: Track1: Online computing