EUROPEAN ORGANIZATION FOR NUCLEAR RESEARCH
CERN — BEAMS DEPARTMENT

CERN-BE-2011-028 BI

LHC Beam Loss Monitoring System Verification Applications

B. Dehning; E. Fadakis; S. Jackson, C. Zamantzas

CERN – Geneva/CH

Abstract

The LHC Beam Loss Monitoring (BLM) system is one of the most complex instrumentation systems deployed in the LHC. In addition to protecting the collider, the system also needs to provide a means of diagnosing machine faults and deliver a feedback of losses to the control room as well as to several systems for their setup and analysis. It has to transmit and process signals from almost 4'000 monitors, and has nearly 3 million configurable parameters. The system was designed with reliability and availability in mind. The specified operation and the fail-safety standards must be guaranteed for the system to perform its function in preventing superconductive magnet destruction caused by particle flux. Maintaining the expected reliability requires extensive testing and verification. In this paper we report our most recent additions to the numerous verification applications. The developments have been made using LabVIEW and CERN custom made libraries and allow the user to connect either directly to the front end computer (FEC) or through a dedicated server.

Paper presented at DIPAC2011 Conference – Hamburg/DE from 16 to 18 May 2011

Geneva, Switzerland
August, 2011

LHC BEAM LOSS MONITORING SYSTEM VERIFICATION APPLICATIONS *

E. Fadakis, B. Dehning, S. Jackson, C. Zamantzas CERN, Geneva, Switzerland

Abstract

The LHC Beam Loss Monitoring (BLM) [1] system is one of the most complex instrumentation systems deployed in the LHC.

In addition to protecting the collider, the system also needs to provide a means of diagnosing machine faults and deliver a feedback of losses to the control room as well as to several systems for their setup and analysis. It has to transmit and process signals from almost 4'000 monitors, and has nearly 3 million configurable parameters.

The system was designed with reliability and availability in mind. The specified operation and the fail-safety standards must be guaranteed for the system to perform its function in preventing superconductive magnet destruction caused by particle flux. Maintaining the expected reliability requires extensive testing and verification. In this paper we report our most recent additions to the numerous verification applications. The developments have been made using LabVIEW and CERN custom made libraries and allow the user to connect either directly to the front end computer (FEC) or through a dedicated server.

INTRODUCTION

General

The Beam Loss Monitoring system [1] is one of the most critical among the numerous systems installed for the protection of the LHC. It has to prevent quenches in the superconducting magnets and protect the machine components against damage. The system comprises of nearly 4'000 detectors, ionisation chambers and secondary emission-based monitors, mounted onto the elements under supervision. The analogue output signal of the sensors is digitised by data acquisition cards [2], generally referred to as Current to Frequency Converter (CFC), installed in the tunnel. The data is then transmitted to the Threshold Comparators (TC) [3] via redundant broadband optical links. The TCs, installed in VME crates distributed in surface buildings around the LHC, collect and analyse the data. Their FPGA-based processing algorithm calculates integrals of the signals over different time windows, compares them to their respective abort thresholds and can trigger a beam abort as appropriate through the Combiner and Survey (CS) card installed in the same VME crate.

Due to the great complexity and sequential nature of the design, the integrity of the whole signal chain needs to be verified to ensure that the system provides the required level of protection. This is achieved by implementing different verification procedures, each of them focusing on different aspects of the system.

Controls Middleware [4]

The CERN custom made libraries named CMW Wrapper provides access to scientific equipment software components based on Front End System Architecture (FESA) and other CMW devices from LabVIEW applications.

VERIFICATION STRATEGY

Each application was created to verify several procedures throughout the BLM system but at the same time target a specific module of our system:

- The processing module is targeted by BLETC_TESTER.
- The analogue to digital module (for specific modules) is targeted by BLECF_TESTER.
- The analogue to digital modules of the entire BLM system in the LHC is targeted by OpSys_TESTER.
- The SRAM of the processing module is targeted by SRAM_TESTER.**

A more detailed overview of the BLM system, the modules, the processes and corresponding applications is given in figure 1.

Verifying the Processing Module

This test application is to be executed prior to installing each new BLM mezzanine card in the operational crates, and at every technical stop to ensure the cards in the operational crates to continue to perform as required. The test procedure is based on reading out and checking the evolution of numerous status fields.

BLETC_TESTER provides an automatic verification of several crucial aspects of the processing module (BLETC):

- Correct integration of mezzanine to the complete module, checking if the card is present in the crate and transmitting data.
- "Quality" of the data that are being processed by the BLETC card allowing verification of the conformity of the Gigabit optical communication

*Work supported by Eleftherios.Fadakis@cern.ch
**Application under development

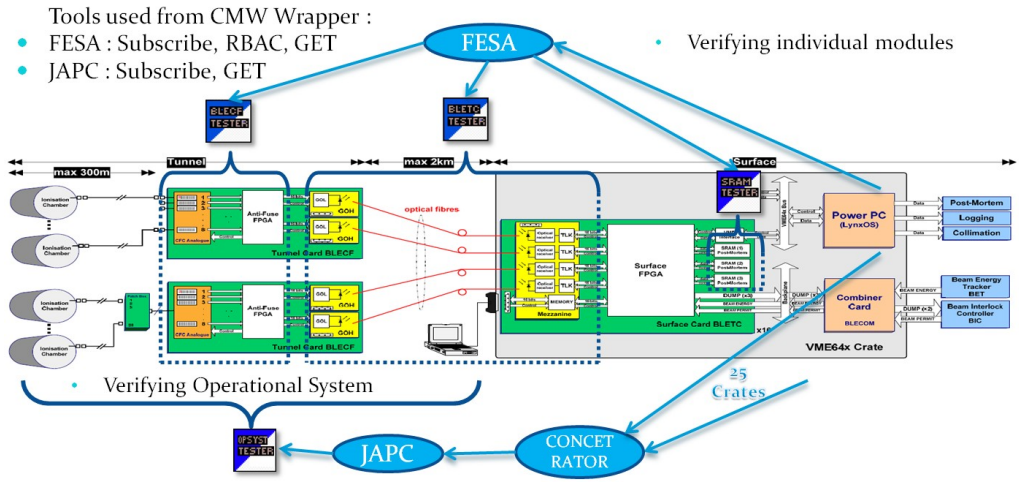

Figure 1: Overview of the BLM system, the modules, the processes and which of them are targeted by each application.

- The redundancy of the transmission, by checking all connections
- The processing module is performing within the desired Bit Error Rate. A system that has a maximum cable connection of 2,3km is likely to have errors in the transmission of data.

In order to create a user friendly application the front panel is comprised of 4 different screens divided into tabs for easier access and scalability (figure 2). Some important controls are common to all tabs. These controls from top to bottom are: the "credentials" fields, where the user must insert information to have access directly to devices concerning the LHC, run the application and retrieve the data. The "device" field, where the user chooses which out of the 25 crates he wants to connect. The "property" field, which shows the name of the property has all the system fields with the data to be verified. The "Cycle" field which refers to how long the application should keep the communication with the crate active and continue to receive data. The "hours of testing" as well as the "time of testing in seconds", are the controls responsible for how long the application is going to run. The user can choose to run the test only for a few seconds by using the "time of testing in seconds". Finally the user inserts the path where the logging file should be created and presses run to initialize the application.

The default tab is named "data" (figure 2) and depicts the names of the fields whose data are being verified. Each crate has a maximum 16 BLETC cards. When a card is in place a green LED indicates its presence, specifying also its position on the crate. The central array contains data each field (columns) and each card (rows).

The second tab named "LED" gives a clear indication by means of red LEDs when the desired beat error rate level is exceeded.

Figure 2: Default tab (1 of 4 in total) of the BLETC_TESTER, named "data" depicting the names of the fields whose data are being verified.

The third tab, "SumOfErrors" gives information about the accumulation of errors. Each line corresponds to one card and each column is one field.

The final tab, "Frames & Cards & Token Info / Time/ Error Messages" contains information about which cards are present in the crate under verification, the serial number of the cards and the full name of the fields that have produced errors above the desired threshold. On the right side of the tab information is displayed about the "token" the user receives from the RBAC (a token is created for 7 hours so in that time the application does not need to create a new one for the same user). There is information about the time of the verification procedure, i.e. the time it started and the duration until completion. Finally if an error occurs related to the application (e.g. internally or a bad connection) a message is displayed informing the user about the nature of the error.

After the verification procedure is finished four log files are created. Each log file gives different information about the entire procedure and any errors that have occurred.

A general log file giving the serial numbers of the cards that where inside the crate and the place they were

inserted as a statistical means to see if the connections of the crate are producing some errors.

An individual log file is created for each BLETC by serial number, indicating which fields have exceeded the defined BER and by how much.

An individual log file for each BLETC by serial number with the accumulation of all errors and the time they appear.

Finally a log file of all the error messages when those are related to the application

Verifying the Analogue to Digital Module

The application created to verify the procedures of the analogue to digital module is called BLECF_TESTER (figure 3), its role is to verify that after a global reset, each BLECF in a specific crate has been correctly connected to the BLETC cards and that the clocking of the acquisition process is initiated correctly.

BLECF_TESTER provides an automatic verification of several statuses which describe the operation of the acquisition card as well as the threshold values of the running sums by checking all 256 channels (1 crate) simultaneously.

The front panel on the left gives information about the token that is needed to access the devices in the LHC. The device field allows the user to choose the crates to be verified. The red LEDs indicate exactly which channel of a BLECF card on the crate exceeded the threshold. The array on the right shows the serial number of the cards.

As a result two log files are created with all possible information needed to resolve the problem.

Verifying the Operational Procedure

OP_SYS_TESTER (figure 4) is executed after a global reset. It uses JAPC to simultaneously retrieve the threshold values of all 4000 channels from the 25 operational crates. The user chooses which running sum he wants to check and sets the threshold value. This allows the user to see immediately if any channel value of any crate for the particular running sum exceeds this value. The application creates a log file containing information about which channel of which BLECF card is giving an error and to which crate it is connected

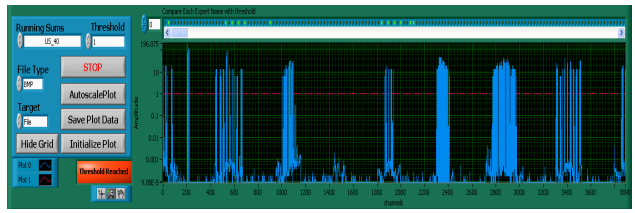

Figure 4: Front panel of the operational procedure verification application.

CONCLUSIONS

The Beam Loss Monitoring system is a critical system with high demands in availability and reliability. Obtaining data with the multiple diagnostic and control applications directly from the crates is possible only during technical stops to keep communication to a minimum and avoid congestion.

While in operational mode, the infrastructure allows multiple clients to retrieve the data in real time from a dedicated concentrator server without affecting the performance of the FECs.

The tools developed allow further augmentation of our verification strategy and ensure the specified system operation. This has been achieved by using CERN custom built libraries and LabVIEW.

REFERENCES

[1] B. Dehning, et al. "*The Beam Loss Monitoring System*", Chamonix 2004

[2] E. Effinger et al., "*The LHC Beam Loss Monitoring System's Data Acquisition Card*", 12th Workshop on Electronics for LHC and future Experiments (LECC 06), Valencia, Spain.

[3] C. Zamantzas et al., "*The LHC Beam Loss Monitoring System's Surface Building Installation*", 12th Workshop on Electronics for LHC and future Experiments (LECC 06), Valencia, Spain.

[4] R. Sorokoletov "CMW Wrapper for LabVIEW User Guide"

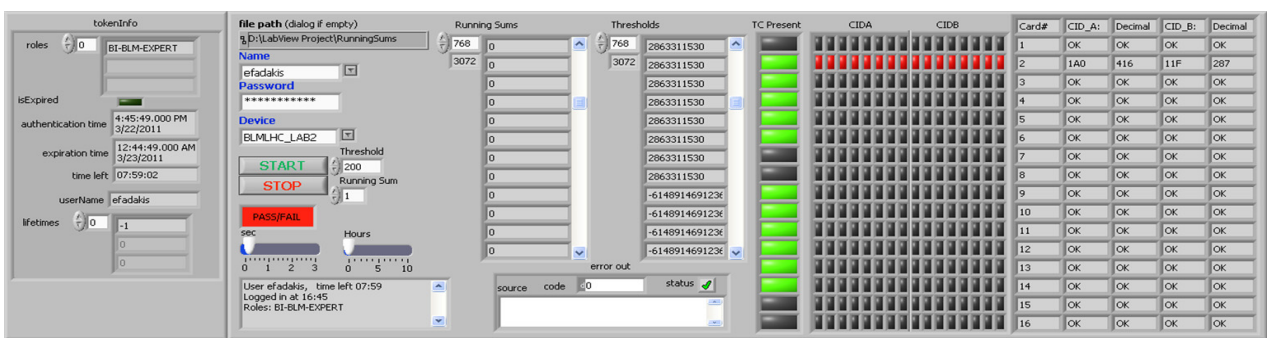

Figure 3: The front panel of the analogue to digital module verification.