REAL-TIME SYSTEM SUPERVISION FOR THE LHC BEAM LOSS MONITORING SYSTEM AT CERN

C. Zamantzas*, B. Dehning, E. Effinger, J. Emery, S. Jackson, CERN, Geneva, Switzerland

Abstract

The strategy for machine protection and quench prevention of the Large Hadron Collider (LHC) at the European Organisation for Nuclear Research (CERN) is mainly based on the Beam Loss Monitoring (BLM) system. The LHC BLM system is one of the most complex and large 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 feedback of the losses to the control room as well as to several systems for their setup and analysis. In order to augment the dependability of the system several layers of supervision has been implemented internally and externally to the system. This paper describes the different methods employed to achieve the expected availability and system fault detection.

INTRODUCTION

The strategy for machine protection and quench prevention of the LHC is heavily dependant on the Beam Loss Monitoring (BLM) system. At each turn, there are several thousands of data values recorded and processed in order to decide if the particle beams should be permitted to continue circulating or their safe extraction is necessary to be triggered. The decision involves a proper analysis of the loss pattern in time and a comparison with predefined threshold levels that need to be chosen dynamically depending on the energy of the circulating beam. The processing of the acquired data is needed to be performed in real-time and thus requires dedicated hardware to meet the demanding time and space requirements.

To maximize the reliability of the BLM system and allow a feasible implementation, this complexity needed to be minimized by all means. At the same time, in order to provide the necessary fail-safety and achieve the expected availability a large number of additional processes was necessary to be added that generate, collect and monitor the state of the system in real-time. It becomes obvious that by recording and relaying such information it can identify weaknesses or failing components and provide a history to understand the events that forced an unforeseen beam extraction request. Thus, a subsequent effort has been done to tap into its resources, extract and provide the most relevant parts.

FRONT-END CHECKS

The front-end modules (BLECF) were given the main task of acquiring, digitising and transmitting the analogue signal provided by the detectors [1]. These modules reside in the tunnel, usually in a crate below the magnet under observation. Due to their exposure in ionising radiation, the generation of supervision data is done by dedicated circuits and the collection of the data by an one-time-programmable FPGA. The collected information is packaged and then transmitted to the back-end part of the system where it is checked and actions are initiated if found necessary [2].

Analogue Circuit Operation

For the monitoring of the continuous operation of the acquisition two independent techniques are used. The first consists of a *Schmitt trigger* circuit, which monitors the integrator output level that flags an excess of 2.4 V. The second survey technique introduces a constant input current of 10 pA and monitors if the recorded acquisitions are above this level. In specific, the additional current corresponds to one extra count output form the current-to-frequency converter every 20 s. The output is constantly monitored and in case of 120 s without a count, an error flag is generated and transmitted.

Further, due to increasing negative leakage current of the analogue circuit's amplifier with the radiation dose, an active compensation has been added to ensure a constant 10 pA input current. The compensation current is produced using an 8-bit digital to analogue (DAC) converter with a 10 GΩ resistor connected to the channel's input. This circuit is also monitored and two flags are raised and forwarded for notification; one flag is raised when the DAC level exceeds a value of 155 and a second when it reaches the maximum, i.e. 255.

Low Voltage Power Supplies

To survey the voltage supplies of the BLECF module, several comparator circuits, i.e. checking the 2.5 V and ±5 V to be inside operational tolerances, are monitored and the results are transmitted together with the data frame.

The processing electronics will receive those check results and request the safe extraction of the beams if they carry information of a fault in a critical location. Specifically, the processing module (BLETC) will exclude faults from triggering a beam abort request if at least one of the following conditions is satisfied: (a) the module has *'0000'* as Card ID defined in the settings database, i.e. it is defined as not active, or (b) the complete set of 8 channels in a module's configuration are set to *'not connected to the LHC Beam Interlock System (BIS)'*, i.e. none of the channels is part of the Machine Protection System.

[*] christos.zamantzas@cern.ch

ISBN 978-3-95450-139-7

Table 1: Truth Table for the Data Selection and Interlock Generation Based on the Checks of the Redundant Optical Links

LINK		CRC		Ignore	Decision/Output		Remarks
A	B	A	B	BLECF	Data used	Beam Permit	
OK	OK	OK	OK	x	Link B	True	all OK (Link B is the default)
OK	OK	OK	ERR	x	Link A	True	Link B has errors
OK	OK	ERR	OK	x	Link B	True	Link A has errors
OK	OK	ERR	ERR	x	Link B	False	Link A & Link B have errors
OK	ERR	OK	x	x	Link A	True	Link B is down
OK	ERR	ERR	x	x	Link A	False	Link B is down & Link A has error
ERR	OK	x	OK	x	Link B	True	Link A is down
ERR	OK	x	ERR	x	Link B	False	Link A is down & Link B has error
ERR	ERR	x	x	NO	Link B	False	Both Link A & Link B are down
ERR	ERR	x	x	YES	Link B	True	Non-active BLECF

Definitions: *CRC A & B* for the Cyclic Redundancy Check results of packets coming from links A and B respectively; *Ignore BLECF* for not installed acquisition modules; *x* = don't care

Operating Temperature

The BLECF is also actively monitoring the operating temperature of the board and provides notification when it exceeds two levels. Those are set to 35°C and 60°C respectively. The processing electronics concentrate this information from all modules and forward them to the Logging database [3] for off-line analysis.

DATA TRANSFER CHECKS

Due to the hostile environment in the tunnel, i.e. ionising radiation and magnetic fields, the processing capabilities of the FPGA are limited and therefore the evaluation of the detector signal has to be performed in the surface buildings. This leads to long transmission distances of up to 2 km between the front-end in the tunnel and the processing module on the surface.

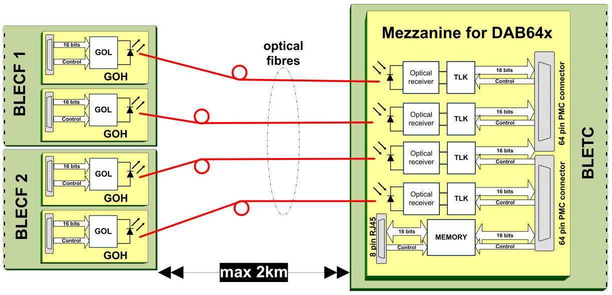

Figure 1: Schematic diagram of the communication link for transporting the data between the tunnel and surface installations.

The strict design specifications require the system to request the safe extraction of the beams if it is does not have or is unable to evaluate the detector levels at each acquisition period. The BLETC's FPGA hosts the Receive, Check and Compare (RCC) process, which is part of the effort to provide very reliable implementations of the physical and data link layers for the system.

Optical Links

The unidirectional communication link operates in the gigabit region to minimise the system latency and it is using radiation tolerant devices for the parts residing in the tunnel installation. Fig. 1 shows a schematic diagram of the communication link implemented.

The optical links are redundant and employ the CERN developed GOL [4] devices. Both links carry identical information that includes the operating status of both transmitting devices. In effect, the two links are monitoring each other and in the case one of them is in fault the second will convey this information.

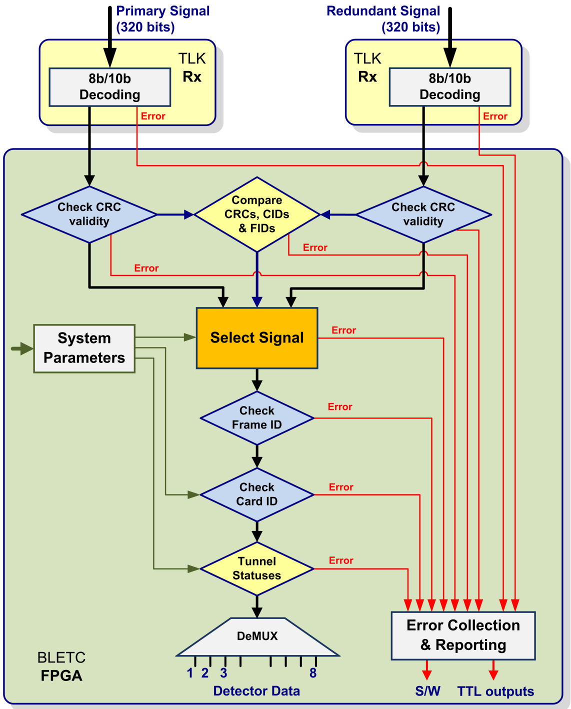

Figure 2: Simplified block diagram of the checks performed in the communication link by the RCC process.

Transmission Error Detection

The implementation of the data reception process, hosted at the entry stage of the surface FPGA, has been done in a way that ensures first the correct reception and then a highly capable detection of erroneous transmissions. This is achieved by making use of redundancy in the transmission lines and digital techniques like the Cyclic Redundancy Check (CRC) and the 8B/10B algorithms. Fig. 2 shows a block diagram of the checks implemented for the communication link in the RCC process.

Nevertheless, it should be noted that exceptional effort has been put into designing those checks, not only to be rigorous and strict but also to avoid unnecessary beam abort requests as much as possible and, in some cases, even provide an increase in the availability of the system.

Table 1 shows the truth table used for the selection of a valid packet for further processing. It can be seen that it exploits the redundancy of the optical links and allows the continuation of beam operation if a certain amount of checks validate at least one of the redundant data packets received. Further, in order to avoid unnecessary stops, beam abort requests generated by checks in cards which have none of their channels connected to the BIS are automatically inhibited.

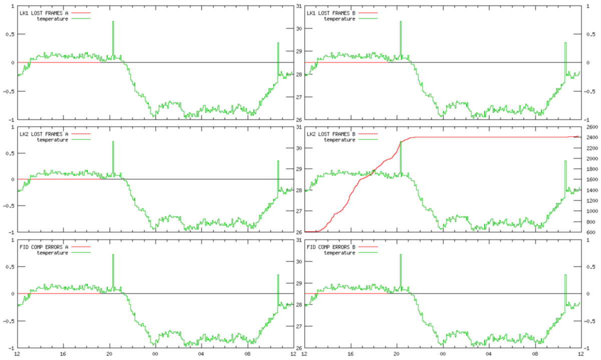

Figure 3: Example of the data transfer error reporting function for different types of checks presented over a period of 24 h (where red: check error count, green: temperature).

Transmission Watchdog

In order to allow keeping track of lost frames on the optical links two techniques are employed. The first one utilises a free-running *'modulo 1600'* counter. This function counts the 25 ns clock cycles passed from the last transmission and if it does not receive a new packet in the time specified, i.e. a *Start-of-Frame* has not been received by either channel, it issues a request for a beam abort. The second technique makes use of the frame identity number (FID) embedded on each packet. The BLECF produces the FID by incrementing a 16 bit counter every sent frame. At the receiver part, the frame number received from each optical link is checked that is an increment of one from the previous.

Furthermore, both techniques have enough intelligence built in to avoid requesting the beams extraction when one of the redundant optical links has erroneous transmissions or becomes completely unavailable as long as at least one valid packet per transmission period can be extracted. Effectively the redundancy is again used to increase the availability of the system without compromising the safety and allows the non-operational links to be be repaired in the next maintenance stop.

BACK-END CHECKS

The processing electronics will receive the acquired data and will need to create histories for each channel and compare results with predefined thresholds that are unique per detector stored locally at the BLETC modules. Thus, it is imperative the system maintain the correct interconnection between modules and hold up-to-date threshold parameters.

Correct Module Connections

Each BLECF card transmits a set of statuses embedded at each packet for checking the correct connection of the tunnel installation. The monitoring is done by the BLETC card. Their purpose is to protect from misplacement of the electronic cards and optical link connections. Failure to detect such case would compromise severely the protection capabilities since the thresholds and masking tables stored on-board are unique per detector and vary significantly between them.

At the BLECF FPGA, a shift register is introduced to read out the card identity number (CID), which is stored as the silicon signature of the FPGA. The signature is programmed into each single chip and readout via the JTAG. The CID is read and checked at every frame transmitted. Similarly, the BLETC and BLECF modules read the unique serial number provided by dedicated identification devices attached to their FPGAs.

As a first step, the BLETC module verifies that the CIDs and the FIDs received from the main and the redundant optical links match. Then, it verifies that the serial numbers for the BLECF, BLETC or BLECS modules attached match the values stored in the database. Failure in any of the above checks will immediately initiate a request for the extraction of the beams.

Consistency of Parameters

The unique per BLETC card set of parameters is stored on the on-board non-volatile memory and consecutively copied in the FPGA internal static memories [5]. Those parameters include the threshold values for the detectors attached to this module and the various serial numbers and system settings.

Using the parameters all the FPGAs used by the system will perform a self-check after their initialisation if they have the correct firmware by comparing the embedded version number against that declared in the database.

ISBN 978-3-95450-139-7

Furthermore, during a system parameter update operation, the front-end computer (FEC) calculates a checksum of the data passed to each module and appends it to the on-board non-volatile memory. Thereafter, it is checking at regular intervals, i.e. once per minute, the consistency of the parameters by reading the data, recalculating the checksum and comparing it with the one stored. Similarly, the check of whether the parameters are synchronised with the database is executed before each beam injection. The BLECS module monitors the results of this check and enforced its execution in the worst case once every 24 h [6].

EXTERNAL CHECKS

The FEC publishes the data collected by each BLETC and BLECS at 1 Hz. Several systems are subscribed to receive this information, such as the Software Interlock System (SIS) and the Logging Database Concentrator, and act on them either in real-time or after regular off-line analysis.

Power Supply of Detectors

For the operation of the detectors a high voltage power supply pair is available for each of the eight LHC sectors. The powering network uses localised distribution boxes and a set of detectors is powered in series with the end connection arriving to the BLECF module.

At that point, the voltage level is monitored and the output of this check is propagated first to the relevant FEC. There, it becomes active only if it is found for each module separately to be persistently for a predefined time period outside the allowed operating range. Also, the FEC masks the output when the system is under test, the module and none of the detectors acquiring is part of the machine protection and therefore not connected to the BIS.

The result is tracked by the SIS client, which triggers the beam abort operation when found at fault.

Energy Value Used

The BLM system uses the broadcast LHC energy value to select a beam loss threshold limit from a pre-calculated series of 32-windows. During operation, if the energy value received by the system is higher than the actual energy, then LHC availability can be compromised, as a lower beam loss threshold will be used. Conversely, if the value received is lower than the actual energy then LHC safety is compromised, as a higher beam loss threshold will be used, this is therefore safety critical.

To avoid either case, the SIS subscribes to each FEC of the BLM system and received the energy value used by each BLETC module and compares it every 3 s with the actual LHC value. If found different, a request for the safe extraction of the beams is requested since the system cannot guarantee its ability to protect the machine from beam related damage.

Data Concentration and Logging

After collecting all these data, it is necessary to ensure that the information from the system propagates correctly to the on-line displays for the operators and is stored in the Logging database. For this, a set of warnings is generated by a connected to all FECs client process. The warnings are shown to the LHC consoles whenever the transfer of measurement or status data is failing to reach the applications or the database. It has the ability to provide distinct warnings for each of the main elements in the infrastructure, i.e. the devices, the concentration and logger processes, the transportation layer or the unavailability of the database.

FUTURE WORK

As it was shown, the system generates, checks and logs a large number of data with the purpose of detecting the correct status and the validity of its operation. There are several more checks that can be added that could guarantee even further the safety provided as well as augment the discovery of faults.

Nevertheless, due to the fact that the operators of the system or the accelerator could be overwhelmed by the vast amount of information, initially focus will be given in standardising the off-line analysis and the interface to the user. For this, work has started to build a framework for data analysis that will streamline and accelerate the development of more checks [7], as well as to develop a dashboard for displaying the results of the checks.

REFERENCES

[1] E. Effinger et al., “The LHC Beam Loss Monitoring System’s Data Acquisition Car”, 12th Workshop on Electronics for LHC and future Experiments, Valencia, Spain, 2007.

[2] C. Zamantzas et al., “An FPGA Based Implementation for Real-Time Processing of the LHC Beam Loss Monitoring System’s Data”, Nuclear Science Symposium Conference Record, 2006. IEEE, vol.2, no., pp.950-954.

[3] C. Roderick et al., “The LHC Logging Service : Handling terabytes of on-line data”, 12th International Conference On Accelerator & Large Experimental Physics Control Systems, Kobe, Japan, 2009.

[4] P. Moreira et al., “A Radiation Tolerant Gigabit Serializer for LHC Data Transmission”, 7th Workshop on Electronics for LHC Experiments, Stockholm, Sweden, 2001.

[5] C. Zamantzas et al., “Configuration and Validation of the LHC Beam Loss Monitoring System”, 9th European Workshop on Beam Diagnostics and Instrumentation for Particle Accelerators, Basel, Switzerland, 2009.

[6] J. Emery et al., “LHC BLM Single Channel Connectivity Test using the Standard Installation”, 9th European Workshop on Beam Diagnostics and Instrumentation for Particle Accelerators, Basel, Switzerland, 2009.

[7] S. Jackson et al., “A Framework for Off-Line Verification of Beam Instrumentation Systems at CERN”, 14th International Conference on Accelerator & Large Experimental Physics Control Systems, San Francisco, CA, USA, 2013.