THE CERN BEAM INTERLOCK SYSTEM: PRINCIPLE AND OPERATIONAL EXPERIENCE

B. Puccio, A. Castañeda Serra, M. Kwiatkowski, I. Romera Ramirez, B. Todd, CERN, Switzerland

Abstract

A complex Machine Protection System has been designed to protect the LHC machine from an accidental release of the beam energy, with about 20 subsystems providing status information to the Beam Interlock System that is the backbone of machine protection. Only if the subsystems are in the correct state for beam operation, the Beam Interlock System receives a status flag and beam can be injected into LHC (Large Hadron Collider). The Beam Interlock System also relays commands from the connected subsystems in case of failure for triggering the LHC Beam Dumping System. To maintain the required level of safety of the Beam Interlock System, the performance of the key components is verified before every fill of the machine and validated after every emergency beam dump before beam operation is allowed to continue. This includes all critical paths, starting from the inputs from connected systems triggering a beam dump request, followed by the correct interruption and propagation sequence of the two redundant beam permit loops until the final extraction of the beam via the LHC beam dumping system. In this paper we report about the experience with the Beam Interlock System that has been deployed for some years in the Super Proton Synchrotron (SPS), in its transfer lines and recently in LHC.

BACKBONE OF THE MACHINE PROTECTION

The Beam Interlock System (BIS) is the backbone of the beam related protection. It takes inputs from subsystems, and inhibits beam operation if a subsystem indicates that there is a problem or that it is not ready for beam operation.

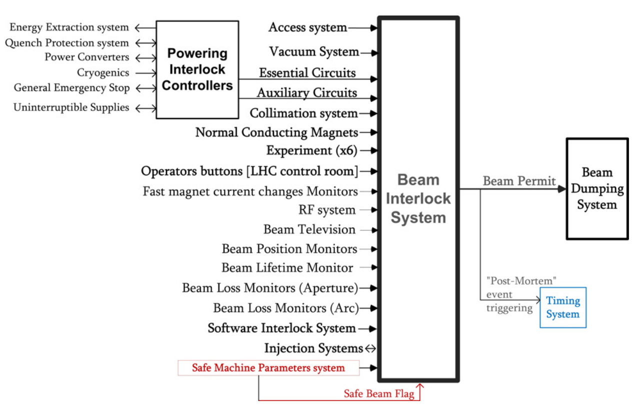

Figure 1: The LHC Beam Interlock System links.

To insure the overall LHC protection, about twenty different subsystems are connected to the BIS (Figure 1).

TWO MAIN ARCHITECTURES

Beam related Machine Protection Systems are used in two different types of environment:

- Protecting ring accelerators: Failures during circulating beam must be quickly detected, and the command for controlled extraction must be issued from any location to the Beam Dumping System.
- Protecting transfer lines: The conditions for beam transfer between the machines must only be permitted when all involved subsystems are in the correct state.

Fundamentally the BIS sub-components have been designed to accommodate both cases without modification. Connecting the system components together differently creates distinct layouts. It has two main architectures, analogous to the implementations of the Machine Protection Systems (Figure 2):

- 'Ring' for protecting the accelerators.
- 'Tree' for protecting the transfer line systems.

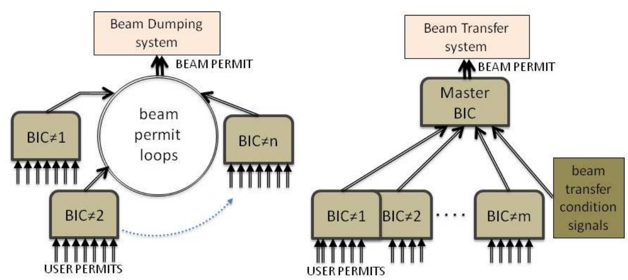

Figure 2: Ring versus Tree Architectures.

The central element of the BIS is the Beam Interlock Controller (BIC). Each BIC acts as a local concentrator, collecting *User Permit* signals from *User System* situated in its vicinity and generating a *Local Beam Permit* signal.

In the 'ring' architecture, the (*Global*) *Beam Permit* is the product of the different *Local Beam Permits* produced by the BICs that are connected to the beam permit loops.

The 'tree' system connects *Local Beam Permit* from BICs installed along the transfer line to the relevant beam transfer system, through a special Master Controller. The latter is a special instance of the BIC as the equation implemented is not a simple 'AND' but it's an 'AND of OR'. Therefore, additional conditions (like beam destination) could be taken into account for permitting safe beam transfers. More details are given in [1].

As generic solution to the interlocking requirements existing throughout the CERN accelerators complex, seven Beam Interlock Systems are currently installed: SPS ring, both SPS Extraction lines, both LHC injection regions and both LHC rings.

Further deployments are already scheduled in the LHC injectors' chain, like for the future LINAC4.

REDUNDANCY CONCEPT

By design the BIS is fully redundant. This redundancy is maintained from the *User Permit* connections right through to the Beam Dump System connections. Thanks to this feature, the BIS meets the strenuous safety requirements imposed by the specification of the LHC Machine Protection System.

CONTROLLER & USER INTERFACES

The Beam Interlock Controller

The Beam Interlock Controller routes up to 14 *User Permit* signals to two redundant Complex Programmable Logic Devices (CPLD). The latter are used to 'AND' together the *User Permit* inputs in order to determine the value of *Local Beam Permits*. The BIC is also including a significant monitoring part; the latter is mainly handling a history buffer for logging any inputs/outputs change with precise time stamping (UTC time with 1µS accuracy).

The User Interface Unit

The *User Interface* box is a small rack mounted module, installed in the *User System* rack. Its role is to receive the redundant *User Permit* signals supplied by the *User System* and transmit them to the nearest BIC in a safe and reliable manner. Each unit is equipped with a CPLD. Thanks to a dedicated full-duplex communication, this component allows online testing and monitoring of links on request. More details are given in [2].

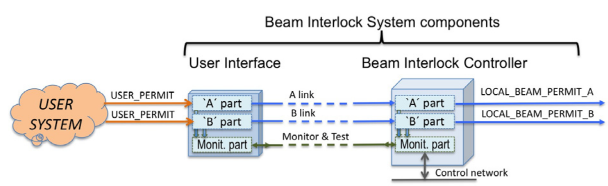

Figure 3: Simplified view of the critical/non-critical paths.

SYSTEM PERFORMANCE

<u>Safety:</u> According to specifications set to meet the dependability requirements for LHC, the system must:

a) React with a probability of unsafe failure of less than 10^{-7} per hour (Safety Integrity Level 3 was used as a guideline).

b) Beam-abort less than 1% of missions due to internal failure (2 to 4 failures per year).

<u>Reaction Time:</u> From the *User Permit* change detection to the corresponding *Local Beam Permit* change, the response time is around 20µS.

<u>Hardware process:</u> The *Beam Permit* is processed in using only hardware. The functionality is programmed into the redundant matrices, with a VHDL code written by different engineers following the same specification.

<u>Critical versus Non-Critical:</u> At the conception level, the critical functionality is always separated from the non-critical. Therefore, the monitoring elements are fully independent of the two redundant safety channels.

<u>Fail-Safe:</u> Any failure along the critical path signal transmission is designed to bring about a Fail-Safe state.

<u>Flexibility:</u> By design, half of the *User Permit* signals could be remotely masked by an Operator under defined condition (the other half, the critical ones, can be never masked). The condition is defined by the "*Safe Beam Flag*" state. This signal is received by each BIC as an additional input. It indicates if the beam is considered to be safe or not. When it becomes false, the masks are no longer taken into account. For the LHC, the "*Safe Beam Flag*" is derived from beam intensity and energy.

<u>Availability:</u> Power supply redundancy is implemented in the Controllers and also in the *User Interfaces.*

<u>100% Online Test Coverage:</u> Using redundant channels in parallel with a monitoring channel, the system can be easily tested from end-to end in a safe manner. This feature allows the BIS to be recovered "good as new".

<u>Failure Modes Effects and Criticality Analysis (FMECA):</u> To quantify the expected performance, the whole design has been studied [3] using Military and Failure Modes Handbooks. The probabilities resulting from the LHC analysis are: P (false beam dump) per hour = 9.1×10^{-4}

P (missed beam dump) per hour = 3.3×10^{-9}

LHC INSTALLATION

LHC Layout

For protecting both LHC rings, the BIS is composed of 17 Controllers connected to the LHC Beam Dumping System (Figure 4) via four optical loops, two for beam-1 and two for beam-2; one each in a clockwise and anti-clockwise path. Two counter-rotating loops imply that the *beam permit* signal always takes the shortest path back to the beam dumping system, giving the optimum response time. Depending of its layout, a LHC sub-system provides one or several *User Permit* connections. In total, around 230 connections are gathered by the different BICs installed around the LHC.

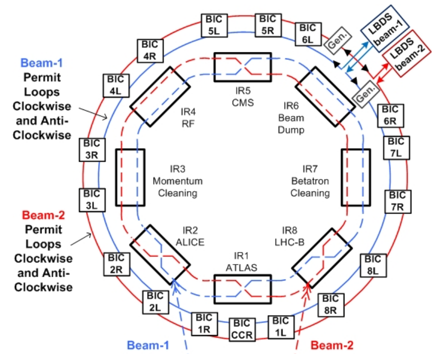

Figure 4: LHC Beam Interlock System layout.

Individual System Tests

Subsequent to its installation in the LHC and in following defined procedures, the Individual System Test of the BIS has been performed. Each BIC has been firstly checked in stand-alone mode in order to confirm its correct functioning. Thus, the *beam permit loops* have been constructed around the machine, and their operation has been characterised. Furthermore, the test adds the *User Interfaces* to the BIC (*User Systems* were not yet connected). Hence, the integrity of the *User Interface* connections has been analysed, and the correct operation of these links has been verified. The results of all tests have been recorded in a Database.

Hardware Commissioning

After the above tests have been completed, the *User Systems* and the Beam Dumping System have been connected as required for LHC operation. All physical connections of all links have been individual tested. For example, it has been verified that the corresponding changes TRUE/FALSE of redundant *User Permit* links are correctly detected by the corresponding BIC. In addition, it has been checked that these changes have been correctly logged and time stamped in the history buffer. All results have been recorded in the same Database.

Automated Test

With the aim to ensure that there is no blind failure at the BIS inputs level, the hardware links from *User Systems* to the User Interfaces are re-checked regularly. It ensures that each connected sub-system is able to give/remove the *User Permit* conditions.

OPERATIONAL TESTS

In order to ensure that its safety is not compromised, the verification of the BIS is carried out in three stages: *Pre-Operation* (configuration verification and integrity check), *During Operation* (fault diagnosis and monitoring) and *Post-Operation* (response analysis).

Pre-Operational Check

This check compares various data read back from the Controllers to that stored in a configuration database. For instance, it compares the position of the disabled channels with the Configuration database. It checks also that the *User Interfaces* are well powered and their ID numbers are correct. The BIS pre-operational checks are remotely launched before each fill by the LHC Beam Sequencer.

Online Monitoring

The on-line verification verifies that several critical elements behave correctly. Each checks compares data read back from the BIS to predefined settings. An alarm is generated if an error is detected. Different checks are performed, like: *User Permit* consistency, *permit loop* frequencies, *User Interface* communication, Timing reception quality… The test verifies also if one the redundant power supply units has not failed.

Post-Operational Checks

After each emergency beam dump, it is checked that:

a) An internal fault was not the source of the beam abort

b) BIS sequence, time propagation and redundancy are matching that which is expected. These tests are forming the Individual System Analysis of the BIS and are integrated in the LHC Post-Mortem application.

Key Element for Post-Mortem Analysis

The BIS is the focal point of the Post-Mortem analysis. Thanks to contents of the different history buffers, the beam dump source can be easily identified. As all BICs are time aligned with 1µS accuracy, it is also possible to reconstruct the events sequence that has lead to dump.

OPERATIONAL EXPERIENCE

Originally designed for LHC, the BIS was firstly installed in its pre-injector for validation. Since 2006, the system is fully operational for the SPS ring and its transfer lines. In total, 18 BICs and around 150 *User Interface* units are installed. Valuable experience with *User Systems* and the Beam Dumping System has been gathered. The overall availability is extremely high (99.996%): with only one stop due to a failure from one of the BIC modules. No false dump has been noticed. For the Transfer lines: "millions" of extractions to CNGS (CERN Neutrinos to Gran Sasso) target have been safely managed. Any malfunction has been reported. As foreseen, some power supplies failed; thanks to the redundancy, it has never lead to a beam operation disruption.

Since the LHC restart in November 2009, the corresponding BIS have already been extensively exercised during the beam commissioning period; about 1000 emergency dumps have been already recorded. Here again, the availability is promising, only few failures with redundant Power Supplies have been noticed.

CONCLUSIONS

As the core of the LHC Machine Protection System, the Beam Interlock System has been designed to be a highly dependable backbone for machine operation. It has been carefully designed to be safe, fast and flexible; a significant inner part is including a complete monitoring, giving the facility to verify its function from end-to-end and to allow it to be recovered "good as new" after a test.

After few months of LHC operations and many years of running in the pre-injector, it has been confirmed that the BIS is not only a very reliable system but also a helpful tool for beam dump diagnostics and for beam operation improvements.

REFERENCES

[1] B. Puccio, "Beam Interlock Strategy Between the LHC and its Injector", ICALEPS 2005; http://epaper.kek.jp/ica05/proceedings/pdf/P3_037.pdf

[2] B. Todd, "The Architecture, Design and Realisation of the LHC Beam Interlock System", ICALEPS 05; http://epaper.kek.jp/ica05/proceedings/pdf/P3_031.pdf

[3] B. Todd, "A Beam Interlock System for CERN High Energy Accelerators", Section 4.8, CERN-THESIS-2007-019, CERN, 2006; http://indico.kek.jp/MaKaC/contributionDisplay.py?contribId=63\&sessionId=35\&confId=5