EUROPEAN ORGANIZATION FOR NUCLEAR RESEARCH
European Laboratory for Particle Physics

Large Hadron Collider Project

LHC Project Report 931

THE IMPORTANCE OF LAYOUT AND CONFIGURATION DATA FOR FLEXIBILITY DURING COMMISSIONNING AND OPERATION OF THE LHC MACHINE PROTECTION SYSTEMS

J. Mariethoz, F. Bernard, R. Harrison, P. Le Roux, M. Peryt, M. Zerlauth
CERN, Geneva, Switzerland

Abstract

Due to the large stored energies in both magnets and particle beams, the Large Hadron Collider (LHC) requires a large inventory of machine protection systems, as e.g. powering interlock systems, based on a series of distributed industrial controllers for the protection of the more than 10'000 normal and superconducting magnets. Such systems are required to be at the same time fast, reliable and secure but also flexible and configurable to allow for automated commissioning, remote monitoring and optimization during later operation. Based on the generic hardware architecture of the LHC machine protection systems presented at EPAC 2002 [2] and ICALEPS 2003, the use of configuration data for protection systems in view of the required reliability and safety is discussed. To achieve the very high level of reliability, it is required to use a coherent description of the layout of the accelerator components and of the associated machine protection architecture and their logical interconnections. Mechanisms to guarantee coherency of data and repositories and secure configuration of safety critical systems are presented. This paper focuses on the first system being commissioned, the complex magnet powering system, to become fully operational before first injection of beam into the LHC.

Presented at
EPAC'06, Edinburgh, UK,
June 26-30, 2006

CERN,
CH-1211 Geneva 23,
Switzerland
Geneva, June 2006

THE IMPORTANCE OF LAYOUT AND CONFIGURATION DATA FOR FLEXIBILITY DURING COMMISSIONNING AND OPERATION OF THE LHC MACHINE PROTECTION SYSTEMS

J.Mariethoz, F.Bernard, R.Harrison, P.Le Roux, M.Peryt, M.Zerlauth, CERN, Geneva, Switzerland

Abstract

Due to the large stored energies in both magnets and particle beams, the Large Hadron Collider (LHC) requires a large inventory of machine protection systems, as e.g. powering interlock systems, based on a series of distributed industrial controllers for the protection of the more than 10’000 normal and superconducting magnets. Such systems are required to be at the same time fast, reliable and secure but also flexible and configurable to allow for automated commissioning, remote monitoring and optimization during later operation.

Based on the generic hardware architecture of the LHC machine protection systems presented at EPAC 2002 [2] and ICALEPS 2003, the use of configuration data for protection systems in view of the required reliability and safety is discussed. To achieve the very high level of reliability, it is required to use a coherent description of the layout of the accelerator components and of the associated machine protection architecture and their logical interconnections. Mechanisms to guarantee coherency of data and repositories and secure configuration of safety critical systems are presented. This paper focuses on the first system being commissioned, the complex magnet powering system, to become fully operational before first injection of beam into the LHC.

THE LHC MAGNET POWERING SYSTEM

The powering system of the LHC is of unprecedented complexity, including more than 10’000 superconducting and normal conducting magnets distributed around the LHC circumference of 27 km. The interconnection of the superconducting magnets throughout the continuous cryostats is done with more than 80’000 splices and they are connected via a large number of HTS current leads and air and water cooled cables to more than 1700 different power converters, located in the LHC underground areas and in various surface buildings.

The concept of powering subsectors

In order to limit the stored energies in the electrical circuits and to avoid cables carrying high currents across the insertions, the main magnets are powered separately in each of the eight symmetrical sectors. In each sector there are several cryostats housing the magnets, in total more than 40 around the LHC. In order to further simplify installation, commissioning and operation, the powering system is subdivided into 28 powering subsectors for the superconducting magnets and 8 powering subsectors for normal conducting magnets. For the protection of the described magnet powering system of the LHC, a dedicated Powering Interlock System has been put in place, interfacing with the power converters, the quench protection system (QPS) and energy extraction facilities to assure the protection of magnets and electrical equipment [3]. The system is based on 44 industrial controllers, installed in a number of racks located in various LHC underground areas, whereas the installations and the protection process have to be customized depending on the layout of the machine and the connected user systems and devices [4].

THE LHC FUNCTIONAL LAYOUT DATABASE

Machine Layouts

More than 82’000 individual components have to be interconnected in the LHC tunnel for magnet powering. In view of this complexity and the need for coherent data during the installation, commissioning and operation of the machine, a complete description of the machine and powering layout has been realised in the LHC Functional Layout Database [1] [2], representing an essential part of the complete database model shown in Figure 1.

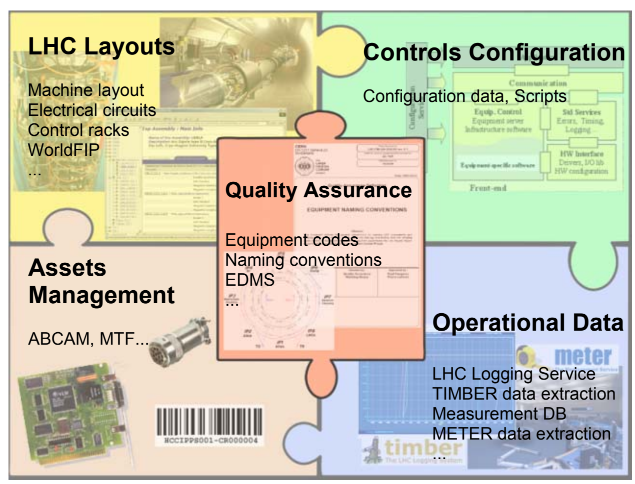

Figure 1: The LHC Functional Layout Database

This layout data is closely related with tools for component tracking (assets management), controls configuration, operational data and quality assurance.

Assets Management

As the protection systems interact closely with the installed powering infrastructure, a complete description of the machine protection system and its logical interconnections with the protected hardware is integrated into the layout database. Graphical representations in the form of web navigators allow for browsing the variety of installations and rack contents as shown in Figure 2 [5].

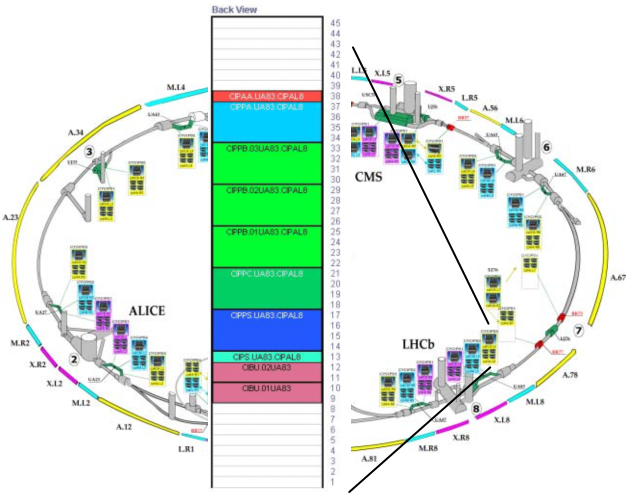

Figure 2: Layout of Powering Interlock Systems and Controls Navigator of the Functional Layout Database

Logical connections representing the physically installed cables can be defined in between the various components of the equipment systems. Dedicated tools allow for the management, tracking and unique identification of each individual system component throughout their complete life-cycle (such as industrial controllers, power supplies, PCBs, etc), using dedicated naming conventions and bar codes as defined in the LHC quality assurance plan [6].

Controls Configuration and Operational Data

Due to the generic design of the powering interlock system, the industrial controllers, programmable logic devices and the according supervision application require a configuration of the process with respect to the particularities of the electrical circuits to be protected in the powering subsector.

This configuration data (i.e. the part for physical I/O addresses) is derived from the system layout and the defined logical interconnections. In addition, a number of operational parameters are included for each electrical circuit, determining the final process parameters for its protection.

Operational data hereby also includes the definition of alarms being sent to the operators in the control room and a consistent naming of each individual signal of the protection systems. Such a naming scheme will allow the operators and system experts an easy access and analysis of the Post Mortem Data, based on automated tools. The history of all interlock signals is captured in the SCADA system and sent for long time storage to the LHC Logging Database.

Although the most basic protection features are always assured by the hardware level of the machine protection systems, the coherency and correctness of process data in the different components of the protection system is vital for the safety, reliability and in particular the availability for operation of the powering interlock system. To ensure this, a single data source is used for the generation of the various configuration data blocks and several verification mechanisms are applied throughout the generation, downloading and use of the configuration data as described in the following section.

MECHANISMS FOR SECURE CONFIGURATION

Data Verification within the LHC Functional Layout Databases

Ensuring consistency and correctness of data is a major challenge and has to start at the very source of the configuration process. A unique source of data and clear interdependencies in between the various parts of a database model are a pre-requisite for a reliable configuration process.

To ensure the correctness of layout data in the LHC Functional Layout Databases, a rigorous versioning scheme is applied, including a series of verification mechanisms and an approval process before the migration to a new data version is approved.

Generation of Configuration Data

Based on this layout and configuration data, a dedicated generation script will be used to produce the set of configuration files for each of the 44 instances of the interlock system as shown in Figure 3. It is important to note that the generation scripts are part of the controls configuration database and that the same mechanisms for the tracking of changes are applied as for the data itself.

A set of configuration files consists hereby out of four individual files, one for the configuration of the SCADA system (in our case PVSS), one for the PLC process, one for the configuration of a programmable logic device and one for the configuration of the controls middleware (CMW), mainly used during the commissioning process of the system. Even if format or content change from one file type to another, for consistency the same data source is used depending only on the previously defined layout.

In order to assure coherency of the individual files at any time, the set of configuration files will always be created in parallel and signed with a Cyclical Redundancy Check (CRC). While the individual checksums are written to all four configuration files, the configuration file for the SCADA system will contain all four checksums of a system, as it will assure the overall coherency during operation.

Use of Configuration Data during machine commissioning

In order to facilitate and speed up the commissioning of the interlock systems, procedures have been put in place which allow for a semi-automatic testing of the interlock functionalities (with the exception of some main circuits where the manual intervention of specialists is inevitable). This automated test functionality is performed by a high level tool with access to all involved client systems through the controls middle ware (CMW).

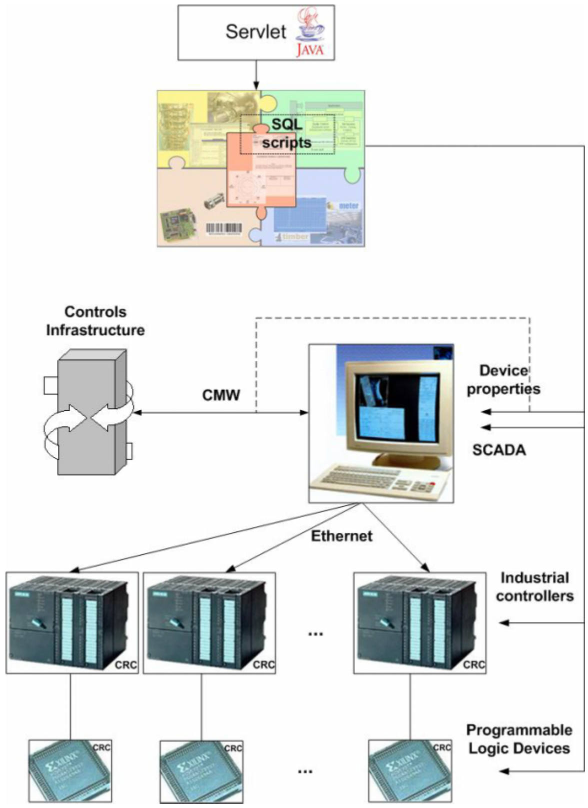

Figure 3: Generation and Deployment of Configuration Data for the Powering Interlock System

The communication towards the involved hardware is derived from the same layout data in a dedicated CMW configuration file. In order to allow for a maximum of flexibility during the dynamic commissioning period (where many circuits will have to be temporarily suspended from the test procedures for fault finding and repair), the CMW configuration will be adapted to the currently active set of circuits under test. During the commissioning phase, any active CMW configuration is clearly made visible via the SCADA system.

After the successful commissioning of a complete instance of the powering interlock system, the CMW configuration is removed in order to avoid any interactions with an operational system other than via the dedicated SCADA system. The same procedures will later on be used to efficiently re-commission the interlock system after shut-downs and possible modifications.

Use of Configuration Data during machine operation and maintenance

Once the powering interlock controllers have been commissioned for a certain configuration, the according set of configuration data is stored in a dedicated repository, allowing for a chronological history of the file versions.

To maintain the high level of security, none of the configuration files is to be changed during operation without repeating the commissioning procedures for this system. Nevertheless one will encounter situations where a configuration file has to be reloaded (e.g. after the replacement of a faulty PLC unit) or operational parameters are to be changed to optimize beam operation. While a simple re-configuration of a PLC is done with commissioned configuration blocks from the repository, any change of layout data or operational parameters has to be done via the creation and commissioning of a new set of configuration files.

Once downloaded, the SCADA system will repetitively verify the coherency of all active configuration files. The various components of the interlock system publish the versions and checksums of their current configuration and the SCADA system will compare this data against its own configuration file, containing the expected checksums of the related components. In addition the IP addresses of the PLC and the SCADA system of the communicating components will be included in the configuration file to avoid erroneous download to a wrong device.

As by design the SCADA system is not involved in the safety critical functions of the system but only required for monitoring and start-up procedures of magnet powering, a verification of the configuration data is performed every time before circuit powering is permitted for any of the electrical circuits. If any of the configurations has changed when starting a new machine cycle, the SCADA system will inhibit powering of any of the circuits of this device.

CONCLUSIONS

In view of the required dependability of the LHC interlock systems, secure configuration of the various interacting system levels is vital. A completely data driven mechanism has been put in place for the controls configuration of the powering interlock system, allowing for flexibility during the installation, commissioning and operation of the protection system whilst maintaining the required level of safety. Changes of any layout or operational data will be directly propagated to all system levels and the coherency of the operated data sets are continuously verified by the SCADA system.

REFERENCES

[1] P. Le Roux, S.Chemli, A.Jimeno Yepes et al., "LHC Reference Database: Towards a mechanical, optical and electrical Layout Database", EPAC'04, Lucerne, July 2004.

[2] M. Zerlauth, A. Jimeno, G. Morpurgo, R. Schmidt, "The Electrical Circuit Description for the LHC", EPAC'02, Paris, June 2002.

[3] F. Bordry et al., "Machine Protection for the LHC: Architecture of the Beam and Powering Interlock Systems", Project Report 521, December 2001.

[4] M.Zerlauth, B.Puccio, R.Schmidt et al., "From the LHC Reference Database to the Powering Interlock System" ICALEPS'03, Gyeongju, October 2003.

[5] http://layout.web.cern.ch

[6] R.Billen, "Naming of LHC Entities and their Parameters for the CCC", EDMS Doc.Nr. 462585, Geneva, CERN 2004.