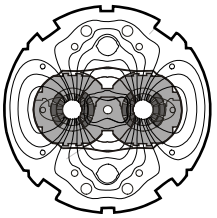
CERN
CH-1211 Geneva 23
Switzerland



the
Large
Hadron
Collider
project

LHC Project Document No.
LHC-CI-ES-0003

CERN Div./Group or Supplier/Contractor Document No.
AB/OP

EDMS Document No.
706584

Date: 2006-02-24

Functional Specification

MANAGEMENT OF CRITICAL SETTINGS AND PARAMETERS FOR LHC MACHINE PROTECTION EQUIPMENT

Abstract

Management of **C**ritical **S**ettings (MCS) and parameters is required as part of the LHC control system to handle interlock settings and other critical parameters for machine-protection related equipment for the SPS, CNGS and LHC. The required functionality and scope are described. This document also specifies the general operational and performance requirements, the equipment systems concerned, the data exchange paths and the safety requirements.

Prepared by :	***Checked by :***	***Approval Group Leader:***
V. KAIN AB/OP	**R. BAILEY** AB/OP	**P. COLLIER** AB/OP
R. ASSMANN AB/ABP	**A. BUTTERWORTH** AB/RF	
B. GODDARD AB/BT	**E. CARLIER** AB/BT	
M. JONKER AB/CO	**B. DEHNING** AB/BDI	
M. LAMONT AB/OP	**J.J. GRAS** AB/BDI	
R. SCHMIDT AB/CO	**R. LAUCKNER** AB/CO	
R. STEINHAGEN AB/OP	**B. PUCCIO** AB/CO	
J. WENNINGER AB/OP	**A. REY** AB/OP	
	M. SOBCZAK AB/CO	
	M. ZERLAUTH AB/CO	

Approval Group Members:

G.Arduini, J.Axensalva, M.Benedikt, R.Billen, O.Brüning, B.Frammery, E.Hatziangeli, W.Hofle, L.Jensen, R.Jones, Y.Kadi, R.Losito, V.Maire, M.Meddahi, V.Mertens, K.H.Mess, S.Myers, J.L.Nougaret, P.Proudlock, S.Redaelli, H.Schmickler, K.Sigerud, B.Todd, J.Uythoven

History of Changes

Rev. No.	*Date*	*Pages*	*Description of Changes*
0.1	2006-02-24	all	Submission for approval

1. SCOPE

Software to manage interlock settings of safety-critical equipment for the SPS, CNGS and LHC is required as part of the LHC control system. The required functionality and scope of this software, denoted **M**anagement of **C**ritical **S**ettings (MCS), are described and a possible architecture outlined. This document specifies the general operational and performance requirements as well as signal exchange paths and the safety requirements. The equipment systems and interlock settings that are concerned by this settings management system are presented. The document:

- describes why MCS is required for parts of the SPS, CNGS and LHC,
- specifies the required functionality of the MCS system,
- specifies the requirements for safety,
- presents the different equipment systems and signals which will be managed by MCS,
- specifies schedules and milestones for prototyping, testing and deployment.

The scope of the specification covers the machine protection systems in the SPS extraction channels, the TT40-TT41-TI 8 transfer lines, the TT60-TI 2 transfer line and the LHC machine.

2. INTRODUCTION

2.1 INTERLOCKING

The hardware interlock systems for machine protection [1,2] are based on a distributed Beam Interlock System, which uses Beam Interlock Controllers (BICs) to collect User Permits from the client systems. A Beam Permit signals is generated from the User Permits and transmitted to the SPS extraction systems, LHC injection systems and LHC beam dumping system.

The Beam Permit signals are based on the status of the User Permits, the status of the mask settings and the SPS and LHC Safe Beam Flags [3]. For the SPS extraction, the CNGS transfer line and the SPS to LHC transfer lines [4,5,6], additional functionality is required including timing aspects inherent to a cycling machine.

Many systems which provide key User Permit signals to the BICs must perform a comparison in the front-ends between a measured equipment parameter and a reference value. The difference must remain within a pre-defined safety tolerance (interlock settings). If the measurement is outside tolerance, an interlock signal (User Permit) is generated to guarantee safe operation.

2.2 MANAGING INTERLOCK SETTINGS

For some of the equipment systems the interlock settings may be “hard-coded” as they are “never” changed. However, many systems require configurable interlock settings to provide sufficient flexibility or margin for beam operation. For example some systems require settings adjustments during setting-up or other operational reasons.

A special settings management system, the MCS, is required as part of the LHC control system to interface to a repository of interlock settings, and to manage interlock setting changes in a secure way. **It is important to ensure that critical settings may only be changed through the MCS by equipment experts or trained persons and not by uncontrolled direct access to the front-end machines or through any other software.** The MCS must provide a unique ‘entry point’ into the SPS and LHC control

systems for critical settings to ensure tracking of changes, to prevent as much as possible human errors, to reject out-of-limits changes for some systems and to provide safe down-loading of settings to the equipment systems, etc. Uncontrolled write access to critical settings at the level of the front-end systems has to be prevented, since this makes proper management of settings quasi-impossible or incomplete.

It should be noted that the MCS will not be able to guarantee full protection against malicious damage from knowledgeable persons inside or outside CERN. However, it should be designed to provide maximum security against accidental or uncontrolled interlock threshold modification, and strictly to limit and log the access to these critical settings.

2.3 INTERLOCK SETTINGS DATA

The structure of the settings data to be managed by the MCS can be categorized as follows:

- Single values:

  Typical examples are beam loss monitor thresholds in the SPS or position tolerances at position monitors in the CNGS transfer line.

- Functions:

  Parameters may be functions of time in the cycle (typical for the SPS), energy, β^* or the LHC mode.

- Tables:

  Two-dimensional tables of settings are required for the LHC beam loss monitor thresholds (thresholds as a function of energy and loss duration).

3. REQUIRED FUNCTIONALITY OF MCS

The functionality required for the MCS corresponds to a subset of that provided by the LHC controls system (LSA settings management [7,8]), where settings need to be managed, generated and sent to the equipment. Additional requirements for the MCS include security and traceability.

The system must in a secure way:

- Provide a repository to store the interlock settings;
- Manage the changes of interlock settings for different operational scenarios (e.g. TOTEM run, ions, different separation/crossing polarities, SPS cycle changes,…) and record all changes with reason and person responsible;
- Provide a secure procedure to change settings. E.g.: reject out-of-limit changes for certain systems, issue warning for large changes or request to type value again;
- Send the interlock settings to the hardware;
- Read back the new interlock settings from the hardware, compare them with the repository, log results of comparison and (possibly) generate a software interlock.

Hardware limits which could cause an interlock, like over-temperature or movement limits, should be configured in a non-modifiable way (hard-coded or hardwired) in the front-ends.

3.1 SCOPE AND EXPECTED FREQUENCY OF USE

The MCS should handle only the key machine protection related interlock settings, with a limited functionality in terms of possible actions, and restricted to only the necessary machine elements.

Interlock settings should be modified only infrequently, during initial commissioning, setting-up, recovery from interventions or machine stops etc. It is not anticipated that the

MCS will be used every fill for managing normal operational changes; rather it should be used only to update the critical interlock thresholds which are normally considered as “almost locked”.

For the case of the LHC: although interlock settings should only be modified infrequently via the MCS, the MCS will be required to send down and check the interlock settings from the repository **before every LHC fill**. This is to minimize risks of data corruption due to re-boot of front-end machines or other problems.

3.2 MCS IN THE LHC CONTROL SYSTEM

The MCS application should be separate from the application software used for the normal equipment control. Access to the configuration and settings repository must be limited, with established procedures for any modification or update.

3.3 ACCESS TO MCS APPLICATION

Read access via the MCS application must be possible within the control room for the machine operation crews.

Write access via the MCS application to modify interlock settings must be restricted to experts and well trained personnel. It must be ensured that each expert can modify only the relevant subset of the parameters. Individual logins and possibly the requirement of a certain number of additional signatures for settings changes are probably the easiest way to accomplish this.

3.4 ALARMS

Several systems have planned to generate a warning if the actual setting is close to the interlock threshold or tolerance limit. Such alarms should be handled within the front-end systems that are permanently monitoring the parameter with respect to the interlock tolerances and will not be managed by the MCS.

3.5 TIMING AND CYCLE ASPECTS

Some systems are sensitive to a change of the LHC operational scenario or SPS cycle and therefore need different operational and interlock settings for different scenarios or SPS cycles.

In the SPS all front-end systems are cycle-aware, both for their operational settings as well as for their interlock settings. It is crucial to ensure a proper association of settings and cycles within the repository. In particular the cycle structure of the MCS settings must follow the same structure used for operational SPS settings. This aspect is very important for correct update when the SPS cycle configuration is changed and both operational and interlock settings must be reloaded.

For the LHC it is foreseen to only download the set of interlock levels corresponding to the current LHC operational scenario. Central LHC scenario-awareness of the MCS is thus required, with a link to the LHC sequencer system. The data sent to the front-ends could include a tag to denote the scenario, which then could be cross-checked by the software interlocking system, see below.

3.6 LOGGING, TRIM HISTORY AND ACCOUNTABILIY

A complete history of changes (trim history) must be maintained by the MCS to track changes to interlock parameters. For each trim a comment with reason of change must be

given. The trim must be time-stamped and the user responsible for the changes must be identified.

It must be possible to reverse or undo individual trims or groups of trims (for example all trims of a given system).

An appropriate procedure to insert INITIAL settings into the MCS repository must be provided.

For the SPS a settings copy mechanism must be provided to copy existing settings for a cycle into the INITIAL settings of a new cycle. Such a mechanism avoids lengthy manual copying of settings where typing errors may easily be introduced.

The result of the comparison in the MCS from the read back of the interlock settings of the different system after downloading must be logged and time-stamped in the SPS respectively LHC logging database.

3.7 MCS VISUALISATION

The interface between the operators and the MCS system must be via application software that will present a detailed view of all interlock settings. It may be desirable to also provide a coherent view of alarm levels, settings, and measurements, together with the hardware limits (if applicable), possibly in the form of fixed or on-demand displays (not necessarily via the MCS application).

3.8 SIGNAL EXCHANGE

The MCS applications must be able to read interlock settings from the repository, to safely send interlock settings to the equipment front-ends and read back the settings from the front-ends. There must be an adequate method of ensuring that any data corruption is detected and that interlock settings which are managed by the MCS cannot be modified in any other way by bypassing the MCS.

A possible standard solution would be to use **public key digital signature**, see Fig. 1. The MCS would sign the data with a private key and the front-ends would only accept data with the correct signature which they verify by means of the public key residing in the front-ends. The signature could be generated while initialisation or modification of the interlock settings and stored with the data to also protect against data corruption in the repository.

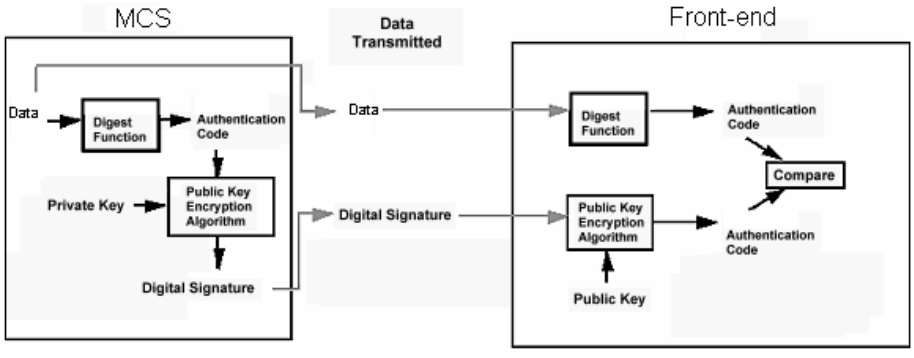


Fig. 1: The principle of public key digital signature between the MCS and Front-ends.

3.9 SOFTWARE INTERLOCK SYSTEM

The software interlock system (SIS) of the SPS and LHC will periodically compare the interlock settings between the values resident in the equipment front-ends and the MCS according to the SPS cycle or LHC operational scenario.

The SIS provides additional protection against data corruption or uncontrolled access and modification of settings under the control of MCS directly inside the front-ends. It also ensures that the interlock settings which are sent to the equipment by the MCS are not modified in an uncontrolled way.

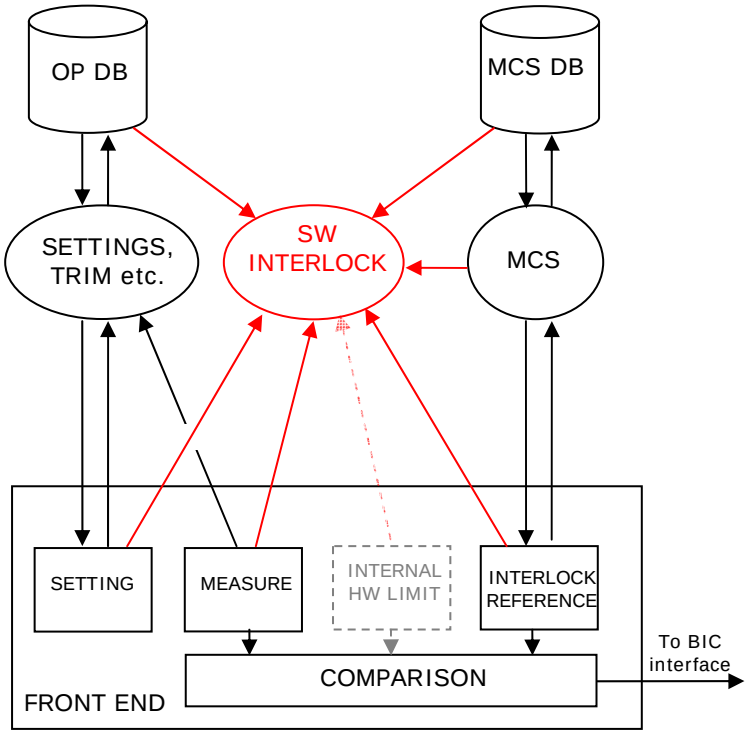


Fig. 2: The role of the software interlocking system in guaranteeing correct interlock settings.

3.10 OTHER ASPECTS

For maximum safety (all consistency checks involve software processes and need time), MCS downloading of settings must **only** be allowed **before operation with beam**, e.g. before filling the LHC. This could be achieved by a request from the MCS to remove the beam/extraction permit via the SIS before downloading and the requirement of "no beam/extraction permit" for downloading unless safe beam intensity is used.

Downloading of interlock settings before **every** fill, as was mentioned earlier, does not only prevent data corruption from fill to fill in the front-ends but also data corruption in the MCS repository, as the front-ends only accept data corresponding to the digital signature from the repository.

Data corruption **during** beam operation can only be detected by the SIS via periodic comparison between data in the MCS database and the front-ends. The consistency of the MCS database itself has to be periodically checked by the SIS. The authentication code corresponding to the stored signature and the one corresponding to the data have to be compared using the public key. The SIS hence also has to have the public key.

With the condition of "no beam/extraction permit" the MCS cannot download during beam operation. Accidental front-end re-boots during operation with beam are likely. If safe recover from such a re-boot for certain systems is desirable (without having to strain the SIS too much), interlock settings must be retrievable without involving the MCS. FESA equipment normally takes care of this by creating an image of the front-end memory on a server which is updated every couple of minutes. Another possibility would be to store the

interlock settings in “local” non-volatile memory as soon as they are downloaded from the MCS.

4. EQUIPMENT SYSTEMS CONCERNED

4.1 MOVABLE PROTECTION DEVICES AND BEAM CLEANING COLLIMATORS

The movable protection devices (TCDI, TDI, TCLI, TCSG, TCDQ) provide critical User Permits for the injection BICs and LHC ring BICs; TRUE if the jaws are correctly positioned to the ‘PROTECT’ setting within the interlock settings and ‘FALSE’ if the jaws are positioned otherwise. For the TCSG/TCDQ in IR6, the interlock settings will change through the LHC operational cycle and will therefore be either functions of time or functions of energy and minimum β^*.

The beam cleaning collimators TCP, TCS, TCT, TCLA and TCLP are also part of the machine protection system, in that they define the LHC aperture and also serve as additional protection to the triplet magnets (TCTs). The interlock levels will be functions of time or energy, minimum β^* and crossing/separation bumps at the IPs.

The baseline for managing interlock settings of cleaning collimators and movable protection devices is to store **absolute jaw positions** as a function of time or energy and β^* (jaw positions in mm) in the MCS repository. In this way maximum safety can be achieved. However, settings of collimators and absorbers depend on the orbit and the beta function at the device locations. The choice of absolute jaw positions in the MCS is hence clearly a compromise between operational flexibility and safety of the systems and requires thorough commissioning of collimator setting-up procedures and optimal understanding of beam dynamics. Storing interlock setting functions as **normalised jaw positions** (jaw position in beam sigma) is also possible. These functions would be locally transformed into absolute values, with the orbit and beam size as additional inputs.

The moveable detectors (Roman Pots) of the TOTEM experiment will be controlled via the collimator control system. The interlock settings of the roman pots possibly also have to be managed by the MCS.

4.2 WARM MAGNETS ROCS SURVEILLANCE

For all magnet circuits in the SPS and transfer lines there is a current surveillance system in the ROCS front-ends, which compares the current in the circuit with the interlock setting. For magnets associated with the LSS4 extraction, and those in TT40, there must be different interlock levels resident in the front-ends, according to the cycle type (CNGS or LHC).

The issue of how to deal with corrector magnets, where interlock settings can change each time the trajectory is corrected, will have to be defined through operational experience, and depends on several things, including the long-term stability of the transfer lines.

4.3 SPS EXTRACTION SEPTA GIRDER

For the SPS extraction septa MST and MSE the supervisory PLC surveys the critical position of the movable girder on which the magnets are mounted. There are 3 such girders (1 in LSS4, 2 in LSS6), each with two interlock thresholds. It is expected that the girder in LSS4 will remain in the same position for CNGS and LHC extraction.

4.4 KICKER MAGNETS

The kicker systems for the extraction kickers MKE in LSS4 and LSS6 and the injection kicker MKI in the LHC must survey the charging voltage and timing (kick delay and pulse length), compared to interlock settings. For LSS4 there must be different interlock thresholds resident in the front-end, according to the cycle type (CNGS or LHC), with different values possibly for the two CNGS extractions.

4.5 BEAM INSTRUMENTATION

Interlock settings of various beam instrumentation systems might need adjusting to optimise protection and beam operation and will hence be managed by the MCS.

- Beam Position Monitors
    - BPCE418/618 – the bumped beam position in the SPS extraction is surveyed. For LSS4 there must be different interlock settings resident in the front-ends, according to the cycle type (CNGS or LHC);
    - Beam Excursion in IR6 - 4 dedicated BPMs per beam are used to measure the orbit in the beam dumping region. They will generate an interlock if the orbit has changed beyond the threshold.
- Beam Loss Monitors
    - Losses in the transfer lines above the pre-defined threshold must generate an interlock which inhibits the next extraction from the SPS;
    - For the LHC ring the BLM systems have a set of different interlock thresholds depending on loss duration and on the beam energy. The management of interlock settings for LHC BLMs is not yet completely defined. It has to be decided whether these thresholds should be remotely configurable via the MCS or be hard-coded in the front-ends.
- The Fast Beam Current Transformer will generate an interlock if the current change rate exceeds a certain interlock threshold. This interlock setting might be a function of the LHC mode.

4.6 RF AND TRANSVERSE FEEDBACK

The limit on the RF frequency offset will be managed by the MCS. The transverse feedback generates an interlock in case of a failure. The number of dampers which need to accidentally switch off to generate an interlock depends on the LHC operational scenario and could be managed via the MCS.

4.7 OTHER PARAMETERS MANAGED BY THE MCS

The MCS will also be used to manage a variety of critical parameters which are not directly linked to beam interlocking.

LBDS XPOC: After every LHC beam dump a post mortem analysis has to be carried out to verify the integrity of the dumping process and allow the next fill. Several parameters are compared to reference values (probably partly functions of energy) managed by the MCS:

- BLM readings
- BPM trajectory readings
- BCT intensity readings
- TDE gas temperature, N_2 pressure
- BTVDD: sweep length and sweep axis of the particles dumped on the TDE; possibly also beam size and beam shape

- Abort gap monitor: abort gap population
- Abort gap synchronisation: for example BCT in IR6 versus LHC BCT

Reference values for the SIS: The SIS requires a database for reference values which are compared to the different system parameters. This database must be protected and only modifiable in a secure way. The SIS reference values will hence be managed by the MCS and included in the MCS database.

Hard-coded interlock settings: The MCS database will also be used as a repository for the settings of hard-coded interlocks, which are periodically compared to the hard-coded settings in the front-ends by the SIS.

Operating conditions during commissioning: The MCS could be envisaged to store and manage the "authorised" operating conditions (e.g. maximum current in the LHC, minimum emittance, maximum number of injected bunches) during the beam commissioning of the LHC.

Equipment	**Comment**
Moveable devices: cleaning collimators, protection devices,…	Functions of energy and β^* or time; absolute or normalised interlock settings
ROCS magnet current surveillance	SPS and transfer lines; different settings resident in front-ends for different cycles
SPS extraction septum girder position	
Kicker magnets	For MKI in the LHC and MKE in the SPS; charging voltage, kick delay and pulse length
Beam position monitors BPCE418/618	Bumped beam position in extraction region; LSS4: different settings for LHC and CNGS
Beam excursion in IR6	Orbit in the LHC beam dumping region
BLMs	Transfer lines: single value for upper beam loss limit, interlock inhibits next extraction; LHC: threshold depends on loss duration and energy
RF	Frequency offset limit
Transverse feedback	Number of dampers which can safely switch off

Table 1: Summary table of equipment systems which need the public key in the front-ends.

5. TESTING AND ACCEPTANCE

System tests for the MCS must be performed and formally accepted before it can be used for regular operation. After the hardware commissioning is completed and the LHC controls are operational, a series of acceptance tests need to be performed. A detailed test programme must be formalised in advance, including the test procedures, details and acceptance criteria. The tests should include:

- Application software functionality and acceptance tests;
- Logging functionality and acceptance tests;
- Failsafe behaviour, by stopping process, rebooting servers, front-ends etc.;
- MCS behaviour in abnormal situation, e.g. front-end recovering from e.g. power cut;
- Signal exchange between databases, process and front-ends;
- Signal exchange with software interlock system;

- Cycle-dependent individual user permit interlock level settings;
- Switching between different pre-defined modes for setting-up and filling.

6. FUNCTIONALITY FOR 2006 TESTS

A prototype MCS should be in place for 2006 for the planned SPS extraction-, transfer- and LHC injection tests. This will allow the system functionality and operational procedures to be checked and refined if needed. In addition, the planned LHC injection sequencer tests with interleaved extraction between LSS4 and LSS6, together with the CNGS tests, provide the opportunity for testing the multi-cycling aspects.

7. REFERENCES

[1] R.Giachino et al., Architecture of the SPS beam and extraction interlock systems, CERN-AB-2003-010-OP, 2003.

[2] B.Puccio et al., The beam interlock system for the LHC, CERN-LHC-CIB-ES-0001-00-10 (EDMS # 567256), 2005.

[3] R.Schmidt, J.Wenninger, LHC injection scenarios, LHC-Project-Note-287, 2000.

[4] M.Benedikt et al. (eds.), The LHC design report volume III, Chapter 18, CERN-2004-003-V3, 2004.

[5] M.Benedikt et al. (eds.), The LHC design report volume III, Chapters 21-31, CERN-2004-003-V3, 2004.

[6] W.Herr, M.Meddahi, Aperture and stability studies for the CNGS proton beam line TT41, CERN-AB-Note-2003-020-ABP, 2003.

[7] L. Mestre et al., “A Pragmatic and Versatile Architecture for LHC Controls Software”, ICALEPCS’2005, Geneva, October 2005.

[8] M. Albert et al., “LHC Software Architecture: TI8 Commissioning”, LHC Project Note 368.