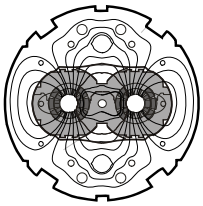
CERN
CH-1211 Geneva 23
Switzerland



the
Large Hadron Collider
project

LHC Project Document No.
LHC-CI-ES-0004 rev 0.1

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

EDMS Document No.
810607

Date: 2006-12-22

Functional Specification

SAFE LHC PARAMETERS GENERATION AND TRANSMISSION (SLPT)

Abstract

For safe operation of the LHC, several systems require machine parameters that must be generated and distributed around the LHC and to the SPS extraction interlock system with very high reliability. This specification defines the functionality of a system that generates and distributes these parameters.

Prepared by :	***Checked by :***	***Approved by :***
R. Schmidt AB/CO	**E.Carlier AB/BT** **B.Goddard AB/BT** **J.Serrano AB/CO** **J.Lewis AB/CO** **M.Lamont AB/OP** **B.Puccio AB/CO** **B.Todd AB/CO** **J.Wenninger AB/OP** **B.Dehning AB/BI** **R.Assmann AB/ABP** **J.Uythoven AB/BT** **V.Kain AB/CO** **M.Jonker AB/CO**	**H.Schmickler AB/CO** **R.Garoby AB/BI**

Distribution list: MPWG members, P.Odier AB/BI, R.Lauckner AB/CO, D.Belohrad AB/BI, D.Swoboda TS/LEA

History of Changes

Rev. No.	*Date*	*Pages*	*Description of Changes*
0.1	2004-07-30		First version
	2004-08-10		After initial comments
	2005-07-10		Major revision, SIL levels included
	2006-01-11		Restructuring document
	2006-02-22		Squeezing factor included
	2006-06-19		Failure scenarios updated, Names updated
	2006-10-30		Comments M.Lamont implemented, SIL calculation appended
	2006-12-22	All	Submission for engineering check

Table of Contents

1. INTRODUCTION

For safe operation of the LHC, several machine parameters must be generated and distributed around the LHC and to the SPS with high reliability by the **S**afe **L**HC **P**arameter generation and **T**ransmission system (SLPT).

A parameter, the "LHC ENERGY" is derived by a very reliable system [1] installed in IR6. The parameter is derived from the current in the main dipole magnets in several sectors. Several systems, such as beam loss monitors and injection kickers require this information.

When the LHC is operating with beam below damage threshold, not all protection devices are required. This will be the case during commissioning, but also for re-commissioning, special studies and in case of problems. This information will be distributed via the "SAFE BEAM FLAG". This flag is derived from the "LHC ENERGY" and from the beam intensity.

Injection of high intensity beam is only permitted when there is already circulating beam in the LHC [2]. The presence of circulating beam is detected, for example by beam current transformers [3]. A parameter, the "BEAM PRESENCE FLAG" is derived from the beam current and indicates if it is above a predefined threshold.

Several operational modes are defined in [4] [5], such as Filling, Ramping, Adjust, and Stable Beam for Physics. The system will distribute the modes that are required for safety critical systems.

The system should allow the transmission of a few other parameters, if required. An example is the "squeezing factor". If the beta function at an IP is not squeezed, this factor would be 1. In case of squeezing, the factor is proportional to the $\beta_{squeeze}/\beta_{unsqueezed}$. Changing the beta function is possible individually at each of the 4 IPs, and there could be 4 different squeezing factors. Since the beta squeeze determines the aperture of the LHC, the squeezing factor might be used for monitoring the position of the collimator jaws.

This specification defines generation and transmission of SAFE LHC PARAMETERS and addresses several questions:

- How are the parameters generated?
- Who uses the parameters?
- How are the parameters used?
- What reliability and availability (SIL levels) are required?
- What default value to take if an error is detected?

A table in appendix A lists the different SAFE LHC PARAMETERS with their corresponding features. In appendix B the SIL levels are given according to the IEC norm 61508 [6].

The details on the interface between the users of SAFE LHC PARAMETERS will be defined in a future specification.

1.1 DEFINITION OF THE LHC ENERGY

The LHC ENERGY is a parameter equal to the energy of a particle in the LHC, and ranges from 450 GeV to, say, 7.6 TeV. This parameter will be represented by a 16-bit value in order to allow a resolution of better than 10^{-4} on the maximum energy. It is proportional to $B \cdot \rho$ and will be derived from the current in the main bending magnets.

1.2 GENERATION OF LHC ENERGY

The LHC ENERGY is generated by a reliable energy tracking system installed in IR6 [1] and transmitted to the SLPT.

1.3 USE OF THE LHC ENERGY

- The Beam Loss Monitor System requires the energy since the thresholds for generating alarms and beam dump requests depend on the energy.
- The injection kickers installed in IR2 and IR8 use the energy in order to prevent deflecting the beam at an energy that does not correspond to 450 GeV.

The LHC ENERGY should be evaluated and distributed to the different users with a frequency of at least 1 Hz.

1.4 DEFAULT VALUE IN CASE OF ERROR

If an error is detected at any stage of the generation and transmission of the energy, the energy should set to a defined value outside the possible range. This value will be defined by the hardware designers.

Example: *if the receiver does not receive new values for the energy due to a failure, the energy is set to the default value for the error. The default value will be defined in the technical specification.*

2. LHC SAFE BEAM FLAG

2.1 DEFINITION OF THE SAFE BEAM FLAGS

The SAFE BEAM FLAG has two states:

- "SAFE BEAM FLAG = TRUE" ⇔ LHC is operating with beam **below** damage threshold
- "SAFE BEAM FLAG = FALSE" ⇔ LHC is operating with beam **above** damage threshold

There is one SAFE BEAM FLAG" for each beam: "SAFE BEAM FLAG for beam 1 (SBF_1) and beam 2 (SBF_2).

2.2 GENERATION OF THE SAFE BEAM FLAG

The SAFE BEAM FLAGS are derived from the LHC ENERGY and from the beam intensities. Theirs inputs are:

- The reliable energy tracking system installed in IR6 for the LHC ENERGY
- The BCT system installed in IR4 measuring:
  - Intensity of beam 1 (I_{beam1}) required for SBF_1
  - Intensity of beam 2 (I_{beam2}) required for SBF_2
- Threshold for beam 1: SBI_TH_1, and for beam 2: SBI_TH_2

It is assumed that the damage potential for beam 1 is proportional to the beam energy and the beam current and given by $I_{beam1} \cdot Energy^{1.5}$. For beam 2 the equation is $I_{beam2} \cdot Energy^{1.5}$. Further studies will validate this assumption, or propose an equation with different energy dependence.

If ($I_{beam1} \cdot Energy^{1.5} < SBI\_TH_1$) then "$SBF_1$ = TRUE", else "SBF_1 = FALSE"

If ($I_{beam2} \cdot Energy^{1.5} < SBI\_TH_2$) then "$SBF_2$ = TRUE", else "SBF_2 = FALSE"

The values for the thresholds should normally be fixed. It must be possible to set it to different values, for example using the system for management of critical settings [7]. The values of the thresholds must be logged.

2.3 USE OF THE SAFE BEAM FLAGS

- Beam Interlock System with 16 controllers around the LHC [8]: when the SAFE BEAM FLAG = TRUE, and a mask for a specific user is set, the USER PERMIT = FALSE is ignored and beam operation is still permitted. Only part of the user permit signals can be masked.
- Injection interlock system: the LHC SAFE BEAM FLAG is transmitted to the SPS extraction interlock system. If SAFE BEAM FLAG = TRUE, no injection of high intensity beam into the LHC is permitted by the extraction interlock. Extraction of high intensity beam is only permitted when the SAFE BEAM FLAG = FALSE [9]. If SAFE BEAM FLAG = TRUE, it would therefore not be possible to inject high intensity beam. The SAFE BEAM FLAG must be forced to become FALSE about 2 sec (time to be confirmed) before high intensity beam is injected into the LHC, for a time to be defined (approx. 3 sec). Before forcing the SAFE BEAM FLAG to FALSE, it should be verified that the circulating beam would not be dumped, since an interlock condition that is masked is violated.
- Aperture kickers: operation of these kickers is allowed only if SAFE BEAM FLAG = TRUE.
- Collimators and beam absorbers: the use of the flag needs to be specified in the upcoming functional specification for the collimators and beam absorbers.

The SAFE BEAM FLAG should be evaluated and distributed to the different users with a frequency of at least 1 Hz.

2.4 DEFAULT VALUE IN CASE OF ERROR

If an error is detected at any stage of the generation and transmission, the value should be set to SAFE BEAM FLAG = FALSE.

3. LHC BEAM PRESENCE FLAGS

3.1 DEFINITION OF THE BEAM PRESENCE FLAGS

The BEAM PRESENCE FLAG is TRUE when there is circulating beam in the LHC, and FALSE if there is no circulating beam. There is one BEAM PRESENCE FLAG for beam 1, and a second flag for beam 2.

3.2 GENERATION OF THE BEAM PRESENCE FLAGS

Inputs to the BEAM PRESENCE FLAG are from the AC transformers in the LHC. The signal from the transformer will be compared with a threshold.

- For BPF_1, the intensity measurement from the AC transformer beam 1: I_{b1}
- For BPF_2, the intensity measurement from the AC transformer beam 2: I_{b2}
- Preset threshold value, minimum intensity: MINIMUM_BEAM_INTENSITY

If (I_{b1} < MINIMUM_BEAM_INTENSITY) then “BPF_1=FALSE”, else “BPF_1=TRUE”

If (I_{b2} < MINIMUM_BEAM_INTENSITY) then “BPF_2=FALSE”, else “BPF_2=TRUE”

The BCTs to measure the beam current that determine the BEAM PRESENCE FLAGS are installed in IR4. The value for the threshold should normally be fixed. It must be possible to set it to a different value after receiving authorisation (to be defined). The value of the threshold must be logged. It is acceptable that the bunch intensity is used to derive the

flag. If there is no bunched beam, it is therefore not possible to inject high intensity beam in LHC.

3.3 USE OF THE BEAM PRESENCE FLAGS

The LHC BEAM PRESENCE FLAGS must be TRUE in order to extract high intensity beam from the SPS and inject it in the LHC. The flags are used in the Beam Interlock Controller that permits extraction from the SPS [9], one for the extraction into TI 8 (flag for Beam 2) and one for extraction into TI 2 (flag for Beam 1).

In order to prevent failures that appear during the last moment before injection, the BEAM PRESENCE FLAG should be evaluated and distributed to the SPS extraction interlock controller with a frequency of 1 kHz or higher. The flag is generated using the Fast Beam Current Transformer.

3.4 DEFAULT VALUE IN CASE OF ERROR

If an error is detected at any stage of the generation and transmission of the flag, the value should be set to BEAM PRESENCE FLAG = FALSE.

4. LHC BEAM MODES

4.1 DEFINITION OF THE BEAM MODES PARAMETER

The LHC beam modes are defined in another document [4]. The LHC will operate in several different beam modes:

- PREPARE INJECTION
- INJECTION
- FILLING
- RAMP
- ADJUST
- UNSTABLE BEAMS
- STABLE BEAMS
- BEAM DUMP
- RECOVER
- PRE-CYCLE

The LHC machine mode will be distributed with 8 bits. The frequency of generation and distribution should be 1 Hz or higher.

4.2 GENERATION OF MODES

Modes are either defined automatically, or by an operator. The mode “RAMP” can be detected automatically, by reading the energy. Only an operator can judge to enter into the mode “stable beams”. Some verification should be performed:

- For a running period, a value of the physics energy is defined (e.g. 7 TeV).
- If an operator declares “STABLE BEAMS” or “UNSTABLE BEAMS” when the LHC is not at physics energy (in the example not at 7 TeV $\pm$ dE), this is not accepted by the system generating the Safe LHC Parameters and it should not be possible to distribute the corresponding “STABLE BEAMS” or “UNSTABLE BEAMS” mode.
- The mode “FILLING” can only be true if the energy corresponds to injection (450 GeV).

- After an end of the fill the magnets are ramped down. If the operator forgets to change the mode and the magnets start to ramp down, the interlock system will detect that the energy does not correspond to the physics energy and trigger a beam dump (if not yet done) and possibly set the mode to BEAM DUMP.

Independent of the SLPT system, the high level control system must prevent inappropriate and potentially dangerous mode changes as far as possible.

4.3 USE OF THE LHC BEAM MODES

In this specification only the use of the beam modes for safety critical systems that receive the information via the SMPT system is discussed. The modes will be used elsewhere, but in systems that are not part of machine protection.

- The experiments are only allowed to move their detectors towards the beam (away from OUT position) when MODE = STABLE BEAMS.
- If the MODE is not equal to STABLE BEAMS or UNSTABLE BEAMS, the beam must be dumped if the experimental detectors are not in OUT position.
- The injection kickers should always be switched off when MODE ≠ FILLING.
- The beam absorbers for injection protection should always be in the “close” position when the MODE = FILLING.
- Other uses of the LHC modes might be identified in the future.

5. LHC SQUEEZING FACTOR

5.1 DEFINITION OF THE LHC SQUEEZING FACTOR

The LHC SQUEEZING FACTOR is a parameter proportional to the beta function at an IP with an experiment. This parameter will be represented by an 8-bit value for each of the 4 IRs for a resolution of about 10^{-2} to describe the squeezing process. Currently beta squeezing is foreseen only when the energy for physics is reached. If the energy is not equal to the physics energy, the squeezing factor should be set to one (one = not squeezed).

5.2 GENERATION OF LHC SQUEEZING FACTOR

The LHC SQUEEZING FACTOR will be derived from the current in the quadrupole magnets in the insertions. The current of at least two quadrupole magnets is required to determine the factor. The current will be acquired via the controls system (to be defined).

5.3 USE OF THE LHC SQUEEZING FACTOR

The Collimation System requires the squeezing factor to determine if the position of a collimator jaw is correct (Note: there are several methods to perform this verification, and it is not decided that the squeezing factor will be used).

The LHC SQUEEZING FACTOR should be evaluated and distributed to the different users with a frequency of 1 Hz.

5.4 DEFAULT VALUE IN CASE OF ERROR

If an error is detected at any stage of the generation and transmission of the squeezing factor, the factor should set to a defined value outside the possible range. This value will be defined by the hardware designers.

6. APPENDIX A: ESTIMATIONS OF SIL LEVELS

In this appendix some failure scenarios and the results of calculations for the required reliability are given, in order to derive the SIL level.

6.1 FAILURE SCENARIOS FOR USING THE LHC ENERGY

6.1.1 BEAM LOSS MONITOR SYSTEM

Worst case failure

- beam circulates with nominal intensity at 7 TeV,
- **failure**: LHC ENERGY received by the BLM system is 450 GeV,
- the threshold of the BLMs is set to a value corresponding to 450 GeV that is too high,
- **failure**: the beam becomes unstable,
- beam loss is detected by the beam loss monitors,
- the threshold is reached too late, and the beam is dumped later than with the correct threshold,
- the most likely consequences is a damage of one or a few collimator jaws, since the beam is dumped later than required.

The probability for such event is remote, and the consequences are major. The LHC ENERGY should not indicate a value that is too low, with a level of SIL = 2 or better.

Other failures

- beam circulates with nominal intensity at an energy below 7 TeV,
- **failure**: LHC ENERGY received by the BLM system is 7 TeV,
- the threshold of the BLMs is set to 7 TeV that is too high,
- **failure**: the beam becomes unstable,
- beam loss is detected by the beam loss monitors,
- since the threshold is too low, it is reached and a beam dump is requested,
- the fill is lost,
- downtime of some hours.

The probability for such event is remote, and the consequences are minor. The LHC ENERGY should not indicate a value that is too high, with a level of SIL = 1 or less.

6.1.2 INJECTION KICKER SYSTEM

Worst case failure

- beam circulates with nominal intensity at 7 TeV, or another energy above 450 GeV,
- **failure**: LHC ENERGY received by the injection kicker system is 450 GeV,
- **failure**: the injection kicker deflects part of the beam with full strength. This is very unlikely, since the kicker must be accidentally charged, and receive either a trigger, or discharges spontaneously,
- part of the beam would be deflected by 0.056 mrad. Many collimators could be damaged, magnets could also be damaged.

The probability for such event is remote, and the consequences are major. The LHC ENERGY should not indicate 450 GeV when the machine operates at an energy above 450 GeV, with a level of SIL = 1 or better.

6.2 FAILURE SCENARIOS WHEN USING THE SAFE BEAM FLAG

6.2.1 LHC BEAM INTERLOCK SYSTEM

Worst case failure

- **failure**: LHC SAFE BEAM FLAG = TRUE although there is high intensity beam in LHC,
- some user permits are masked,
- **failure**: the beam becomes unstable,
- the corresponding USER_PERMIT that would trigger a beam dump is masked,
- **failure**: no other monitor detects the failure,
- the beam is dumped too late,
- damage of a superconducting magnet is expected, or of other machine equipment.

The probability for such event is remote, and the consequences are major. The LHC SAFE BEAM FLAG should not be TRUE in presence of high intensity beam with a level of SIL = 2.

Other failure

- LHC SAFE BEAM FLAG = FALSE although there is only non destructive beam in LHC,
- user permits are not masked,
- injection is blocked,
- downtime of less than one hour.

The probability for such event is remote, and the consequences are minor. Such event should be avoided with a level of SIL = 1 or less.

6.2.2 SPS EXTRACTION INTERLOCK SYSTEM

Worst case failure

- LHC SAFE BEAM FLAG = TRUE,
- some user permits are masked,
- injection of high intensity beam into the LHC is foreseen,
- **failure**: the LHC SAFE BEAM FLAG should be set to FALSE before injection, but it remains TRUE,
- **failure**: the SPS extraction interlock system receives the incorrect value (= FALSE) of the LHC SAFE BEAM FLAG,
- extraction of high intensity beam is not inhibited by the SPS extraction interlock system,
- **failure**: in the LHC, there is a equipment failure that would be prevented if a user permit would not be masked,
- high intensity beam is injected, and lost within one or a few turns,
- damage of a superconducting magnet is expected, or of other machine equipment,
- downtime of 30 days and financial loss of about 1 MCHF.

The probability for such event is negligible, and the consequences are major. The LHC SAFE BEAM FLAG should not be TRUE before the injection of high intensity beam with a level of SIL = 1.

6.2.3 APERTURE KICKER

Worst case failure

- **failure**: LHC SAFE BEAM FLAG = TRUE although there is high intensity beam in LHC,
- the aperture kicker is unlocked by the special key,
- **failure**: an operator uses the aperture kicker, despite that it should not be used with high intensity beam,
- the energy of the machine is at, say, 500 GeV,
- the beam is deflected with an amplitude that corresponds to about 5 sigma,
- several collimator jaws could be damaged, a massive quench might lead to cold diodes being damaged.

The probability for such event is remote, and the consequences are major. The LHC SAFE BEAM FLAG should not be TRUE in presence of high intensity beam with a level of SIL = 2.

6.2.4 USE AT INJECTION FOR THE INJECTION COLLIMATORS

Worst case failure

- **failure**: LHC SAFE BEAM FLAG = TRUE although there is high intensity beam in LHC,
- the injection absorbers (TDI and others) are set to a position that does not protect the LHC, from and unsynchronised kick of the injection kicker, or during a failure for the injected beam,
- the LHC is in filling mode, and injection of beam is requested,
- **failure**: there is a failure of the kicker (spurious kick, unsynchronised kick) and the circulating beam is deflected, or the injected beam is wrongly deflected, in the vertical plane (for example, when the kicker does not fire),
- damage of the D1 and/or of the triplet.

The probability for such event is remote, and the consequences are major. The LHC SAFE BEAM FLAG should not be TRUE in presence of high intensity beam with a level of SIL = 2.

6.3 FAILURE SCENARIOS FOR USING THE BEAM PRESENCE FLAGS

Worst case failure

- **failure**: LHC BEAM PRESENCE FLAG = TRUE although there is not circulating beam in the LHC,
- **failure**: there is a failure of equipment in the LHC that would not permit beam to circulate in LHC,
- high intensity beam is injected and lost in the LHC,
- depending on the loss mechanism, damage of a superconducting magnet is expected, or of other machine equipment.

The probability for such event is remote, and the consequences are severe. The LHC BEAM PRESENCE FLAG should not be TRUE in presence of high intensity beam, with a level of SIL = 2.

Other failure

- LHC BEAM PRESENCE FLAG = FALSE,
- there is circulating beam in LHC,
- injection of high intensity beam into the LHC is requested,
- the extraction from the SPS is blocked,
- downtime of less than one hour.

The probability for such event is remote, and the consequences are minor. The scenario should be excluded with a SIL level of 1 or less.

6.4 FAILURE SCENARIOS FOR USING THE LHC BEAM MODES

6.4.1 FAILURE SCENARIOS USING THE STABLE BEAM MODE BY EXPERIMENTS

Worst case failure

- the machine is set up for injection,
- **failure**: the mode is set wrongly to STABLE BEAMS,
- the experiments receive the mode STABLE BEAMS and drive their detectors (roman pots, LHCb VELO) into the nominal position for data taking, without touching the already circulating beam,
- beam with high intensity is injected,
- the beam hits the detector,
- the Roman pots would be damaged, the LHCb VELO would be damaged.

The probability for such event is remote, and the consequences are major. The MODE should not be STABLE BEAM during injection, with a level of SIL = 2.

Other failure

- the machine is operating with circulating beam,
- **failure**: the mode is set to STABLE BEAMS, although stable beam have not yet been declared,
- the experiments receives the mode STABLE BEAMS and drive their detectors (roman pots, LHCb VELO) into the nominal position for data taking,
- **failure**: the detectors touch the beam,
- **failure**: the machine protection systems do not work, e.g. the particle showers generated by this event are not detected,
- the Roman pots would be damaged, the LHCb VELO would be damaged,
- downtime of 30 days and financial loss of about 1 MCHF.

The probability for such event is remote, and the consequences are major. The STABLE BEAM MODE should not be there during any other mode than STABLE BEAMS, with a level of SIL = 2.

6.5 FAILURE SCENARIOS FOR USING THE SQUEEZING FACTOR

The use of the SQUEEZING FACTOR for the collimators needs to be defined first, and only then the failure scenarios can be discussed.

7. ERROR HANDLING

In order to achieve the required safety levels, the SLPT system will be connected to the Beam Interlock System. If a failure or an inconsistency is detected, the beams will be dumped.

The error conditions when to dump the beams will be defined later, since it requires a more accurate knowledge of the hardware realisation.

8. APPENDIX B: SUMMARY SIL LEVELS FOR SAFE LHC PARAMETERS

Name	Format	Rate	Latency	Derived from (producer name)	Distributed to	Safety level
LHC ENERGY	2 bytes	1Hz	0.1 second	Current in main dipoles (BEM)	Beam Loss Monitors	SIL=2
					Injection Kickers	SIL=2
SAFE BEAM FLAGS	2 bits (SBF_1& SBF_2)	1Hz	0. 1 second	LHC ENERGY (SMPG) and Beam Intensities (BCT)	LHC Beam Interlock System	SIL=2
					SPS Extraction Interlock	SIL=1
					Aperture Kickers	SIL=2
BEAM PRESENCE FLAGS	2 bits (BPF_1 & BPF_2)	1kHz	1 ms	Beam Intensities (BCT)	SPS Extraction Interlock	SIL=1
LHC BEAM MODES	1 byte	1Hz	1 second	Automatic process with operator input possible	Experiments	SIL=2
					Injection Kickers	tbd
					Beam Dilutors (at injection)	tbd
LHC SQUEEZING FACTORS	4 bytes	1Hz	1 second	Automatic process with operator input possible	tbd, possibly collimation system	tbd

The above table summarizes the main characteristics of the different SAFE LHC PARAMETERS.

9. APPENDIX C: DEFINITION OF SIL LEVELS

SIL levels are defined in the norm IEC 61508. The following tables were taken from this norm, and adopted to the accelerator environment.

TABLE I: Category of accidents used for LHC consequences definition

Category	**Injury to personnel**		**Damage to equipment**	
	Criteria	**# fatalities**	**CHF Loss**	**Downtime**
Catastrophic	Multiple fatalities events	≥1	$> 5 \cdot 10^7$	> 6 months
Major	Single fatality events	0.1	10^6 – $5 \cdot 10^7$	20 days to 6 months
Severe	Serious, but not fatal, injury events	0.01	10^5 – 10^6	3 to 20 days
Minor	Minor injuries events	0.001	0 – 10^5	< 3 days

TABLE II: Frequency table used for LHC risk definition

Category	**Description**	**Frequency (per year)**
Frequent	Events which are very likely to occur	> 1
Probable	Events that are likely to occur	10-1 - 1
Occasional	Events which are possible and expected to occur	10^{-2} – 10^{-1}
Remote	Events which are possible but not expected to occur	10^{-3} – 10^{-2}
Improbable	Events which are unlikely to occur	10^{-4} – 10^{-3}
Negligible	Events which are extremely unlikely to occur	< 10^{-4}

TABLE III: Failure rate (SIL) and Risk table used for LHC risk evaluation

Event Likelihood	**Consequence**			
	Catastrophic	**Major**	**Severe**	**Minor**
Frequent	SIL 4	SIL 3	SIL 3	SIL 2
Probable	SIL 3	SIL 3	SIL 3	SIL 2
Occasional	SIL 3	SIL 3	SIL 2	SIL 1
Remote	SIL 3	SIL 2	SIL 2	SIL 1
Improbable	SIL 3	SIL 2	SIL 1	SIL 1
Negligible	SIL 2	SIL 1	SIL 1	SIL 1

TABLE IV: Failure rate and SIL level		
SIL	Probability of a dangerous failure per hour	MTBF (years)
1	$10^{-6} < PR < 10^{-5}$	10 - 100
2	$10^{-7} < PR < 10^{-6}$	100 - 1000
3	$10^{-8} < PR < 10^{-7}$	1000 - 10000
4	$10^{-9} < PR < 10^{-8}$	10000 - 100000

10. APPENDIX D: SIL CALCULATIONS (MATHCAD SREADSHEET)

For some of the failure cases, the calculations to come to the SIL level are appended.

Parameters used for the SIL calculations

Number of fills at 7 TeV per year: $N_{fills\_y} := \frac{400}{yr}$

Hours per fill: $T_{fill} := 10hr$

Probability that during a fill a failure requires an emergency beam abort: $P_{Abort} := 0.4$

Time per injection and ramp: $T_{inj} := 1hr$

Number of injection processes per year (not every injection process leads to a fill at 7 TeV): $N_{inj\_empty} := N_{fills\_y} \cdot 2$

Correspondence between SIL level and MTBF :

SIL1 := 50yr SIL2 := 500yr SIL3 := 5000yr SIL4 := 50000yr

SIL Levels for Safe LHC ENERY (LSE)

1) Failure Mode: wrong LHC ENERGY for BLM thresholds

Beam circulates with nominal intensity at 7 TeV.

Failure A: SAFE LHC ENERGY received by the BLM system is 450 GeV.

The threshold of the BLMs is set to a value for 450 GeV that is too high for 7 TeV.

Failure B: An equipment or an operational failure causes the beam to become unstable.

Beam loss is detected by beam loss monitors.

The threshold is exceeded too late, and the beam is dumped later than with the correct threshold.

The most likely consequence is the damage of one or several collimators, leading to downtime of 30 days or more and financial loss of about 1 MCHF or more.

MTBF for the LHC energy transmission / receiption failure
that leads to a threshold for an energy of 450 GeV instead of 7 TeV: $MTBF_{LE} := SIL2$

$MTBF_{LE} = 500\,yr$

Unreliability that the LHC ENERGY indicates a wrong value: $U_{LE} := \frac{1}{MTBF_{LE}}$

Probability for one fill that LHC ENERGY is not indicating 7 TeV when operating at 7 TeV

$P_{LE\_wrong\_fill} := U_{LE} \cdot T_{fill}$

$P_{LE\_wrong\_fill} = 2.282 \times 10^{-6}$

Probability that beam losses occur, and that the BLMs with low thresholds are required to prevent damage (no other monitor detects the failure in time)

$P_{BLM\_req} := 0.15$

Probability for a fill ended by beam abort, and the BLMs are required with correct thresholds:
$P_{Abort\_BLM\_req} := P_{Abort} \cdot P_{BLM\_req}$
$P_{Abort\_BLM\_req} = 0.06$

Number of fills per year when this event will happen: $P_{Abort\_BLM\_req} \cdot N_{fills\_y} \cdot 1yr = 24$ (high demand)

Probability that for such fill the SAFE LHC ENERGY is wrong:
$P_{failure\_fill} := P_{Abort\_BLM\_req} \cdot P_{LE\_wrong\_fill}$
$P_{failure\_fill} = 1.369 \times 10^{-7}$

MTBUF (mean time between unsafe failures): $MTBUF_1 := \left(P_{failure\_fill} \cdot N_{fills\_y}\right)^{-1}$

$MTBUF_1 = 1.826 \times 10^{4}\,yr$

Possible reduction of the risk:

a) Verification that the energy read by the BLM system corresponds to, say, 7 TeV at the end of the ramp. If the threshold would be then set to a value corresponding to 7 TeV, the time of the fill is not relevant, but only the time of the ramp (30 min instead of 10 hr). This would increase the mean time between unsafe failures by about a factor of 20.

b) Software interlock system that verifies correct correspondence with a frequency of, say, one per minute.

2) Failure Mode: wrong LHC ENERGY for injection kicker magnets

Beam circulates with nominal intensity at 7 TeV. The injection kicker deflects the beam with full strength.

Failure A: LHC ENERGY received by the injection kicker system is 450 GeV

Failure B: The injection kicker system is charged.

Failure C: The kicker receives either a trigger signal, or discharges spontaneously.

Part of the LHC beam is deflected by an angle that corresponds to $n \cdot \sigma$ with σ= beam size

The consequences are difficult to quantify, but could be catastrophic (downtime of more than 6 months and financial loss of more than 50 MCHF).

SIL level of the LHC Energy transmission system: $MTBF_{LE\_k} := SIL1$

Probability that LHC SAFE ENERGY is indicating a wrong value: $P_{LE\_wrong} := \frac{1}{MTBF_{LE\_k}}$

Probability for one fill that LHC SAFE ENERGY is not indicating 7 TeV when operating at 7 TeV

$P_{LE\_wrong\_fill\_k} := P_{LE\_wrong} \cdot T_{fill}$

$P_{LE\_wrong\_fill\_k} = 2.282 \times 10^{-5}$

Probability that the injection kicker is charged during a fill at 7 TeV: $P_{kicker\_charge} := 10^{-3}$

Probability that the kicker receives a timing event when this should not be the case: $P_{trigger} := 0.01$

Probability that for such fill the LHC SAFE ENERGY is wrong:

$P_{failure\_fill\_k} := P_{kicker\_charge} \cdot P_{trigger} \cdot P_{LE\_wrong\_fill\_k}$

$P_{failure\_fill\_k} = 2.282 \times 10^{-10}$

MTBF for such failure: $MTBF_3 := \left(P_{failure\_fill\_k} \cdot N_{fills\_y}\right)^{-1}$

$MTBF_3 = 1.096 \times 10^{7}\ yr$

3) Failure Mode LHC SAFE BEAM FLAG (SBF) for the beam interlock system

Failure A: LHC SAFE BEAM FLAG = TRUE although there is high intensity beam in LHC.

Some input channels of the Beam Interlock System could be masked.

Failure B: An equipment or an operational failure causes the beam to become unstable.

The failure is detected, and a beam dump is requested. The input channel is masked and BEAM PERMIT remains TRUE.

Failure C: No other monitor detects the failure in time.

Damage of a superconducting magnet is expected, or of other machine equipment leading to downtime of 30 days or more and financial loss of about 1 MCHF or more.

MTBF for the SBF system to indicate SAFE BEAM when the beam is not safe: $MTBF_{SBF} := SIL2$

Unreliability that the LHC SAFE BEAM FLAG indicates TRUE instead of FALSE:

$$P_{SBF\_wrong} := \frac{1}{MTBF_{SBF}}$$

Probability for one fill that the LHC SAFE BEAM FLAG is wrong:

$P_{SBF\_wrong\_fill} := P_{SBF\_wrong} \cdot T_{fill}$

$P_{SBF\_wrong\_fill} = 2.282 \times 10^{-6}$

Probability that input channels of the BIC system are masked: $P_{mask\_set} := 1$

Probability that a channel is required to dump the beam that is maskable: $P_{maskable\_req} := 0.05$

Probability for the fill that ended by beam losses, and masked monitors are required to prevent damage: $P_{maskmon\_req} := P_{mask\_set} \cdot P_{maskable\_req}$

$P_{maskmon\_req} = 0.05$

$P_{Abort\_maskmon\_req} := P_{Abort} \cdot P_{maskmon\_req}$

$P_{Abort\_maskmon\_req} = 0.02$

Probability that for such fill the SBF is wrong

$P_{failure\_fill\_3} := P_{Abort\_maskmon\_req} \cdot P_{SBF\_wrong\_fill}$

$P_{failure\_fill\_3} = 4.563 \times 10^{-8}$

MTBF for such failure: $MTBF_2 := \left(P_{failure\_fill\_3} \cdot N_{fills\_y}\right)^{-1}$

$MTBF_2 = 5.479 \times 10^{4}\ yr$

Reduction of the risk:
Masking is no default, masks should only be used if operating with low intensity beams. When masks are not set, safety does not depend on the Safe Beam Flag. During normal operation with high intensity beams, masks should not be used. There are several option in order to reduce risks: when operating with high intensity beam, the sequencer could unmask the channels. Before starting the energy ramp, the sequencer could verify that the channels are unmasked when the intensity is above a certain limit.

4) Failure Mode BEAM PRESENCE FLAG for injection into LHC

Failure A: BEAM PRESENCE FLAG is TRUE although there is not curculating beam in the LHC.

Failure B: there is a failure of equipment in the LHC that would not permit beam to circulate in LHC.

High intensity beam is injected and lost in the LHC.

Damage of a superconducting magnets is expected, or of other machine equipment leading to downtime of 30 days and financial loss of about 1 MCHF

SIL level of the BPF system: $MTBF_{BPF} := SIL2$

It is assumed that the correctness of the BPF is always verified before a fill when there is no beam in the LHC. If the flag is TRUE without beam, it must be corrected before injection of beam. It is therefore assumed that the probability of a failure during the injection process is related to the length of this process.

Probability that LHC PBF is indicating a wrong value during the injection process that takes

$T_{inj} = 1\,hr$: $\quad P_{BPF\_wrong\_inj} := \frac{T_{inj}}{MTBF_{BPF}}$

Probability for BEAM PRESENCE FLAG being wrong during one injection process

$P_{BPF\_wrong\_inj} = 2.282 \times 10^{-7}$

Probability that there is a failure in the LHC that prevents beam circulation $P_{LHC\_wrong} := 0.1$

Probability that for one injection process the Beam Presence Flag is wrong AND there is a failure in the LHC:

$P_{injection} := P_{BPF\_wrong\_inj} \cdot P_{LHC\_wrong}$

$P_{injection} = 2.282 \times 10^{-8}$

MTBF for such failure: $MTBF_4 := \frac{1}{P_{injection} \cdot N_{inj\_empty}}$

$MTBF_4 = 5.479 \times 10^{4}\,yr$

REFERENCES

[1] E.Carlier, private communication
[2] J.Wenninger and R.Schmidt LHC Injection Scenarios, CERN-LHC-PROJECT-NOTE-287, Geneva, CERN, March 2002
[3] C.Fischer, R.Schmidt, On the Measurements of the Beam Current, Lifetime and Decay Rate in the LHC Rings, Functional Specification LHC-BCT-ES-0001, EDMS Id: 59172
[4] R.Lauckner, LHC Modes, LHC-OP-ES-0004 rev 1.0
[5] D.Macina, W.H.Smith, J.Wenninger, LHC EXPERIMENTS BEAM INTERLOCKING, Functional Specification LHC-CIB-ES-0002 v.1.0
[6] IEC 60508
[7] V.Kain et al., Management of critical setting, Functional Specification in preparation
[8] Bruno Puccio, Rudiger Schmidt, THE BEAM INTERLOCK SYSTEM FOR THE LHC, Functional Specification LHC-CIB-ES-0001, EDMS Id: 567256
[9]B. Goddard, V. Kain, R. Schmidt, J. Wenninger, INTERLOCKING BETWEEN SPS, CNGS, LHC TRANSFER LINES AND LHC INJECTION, LHC-CI-ES-0002 ver.1.0, EDMS Id: 602470