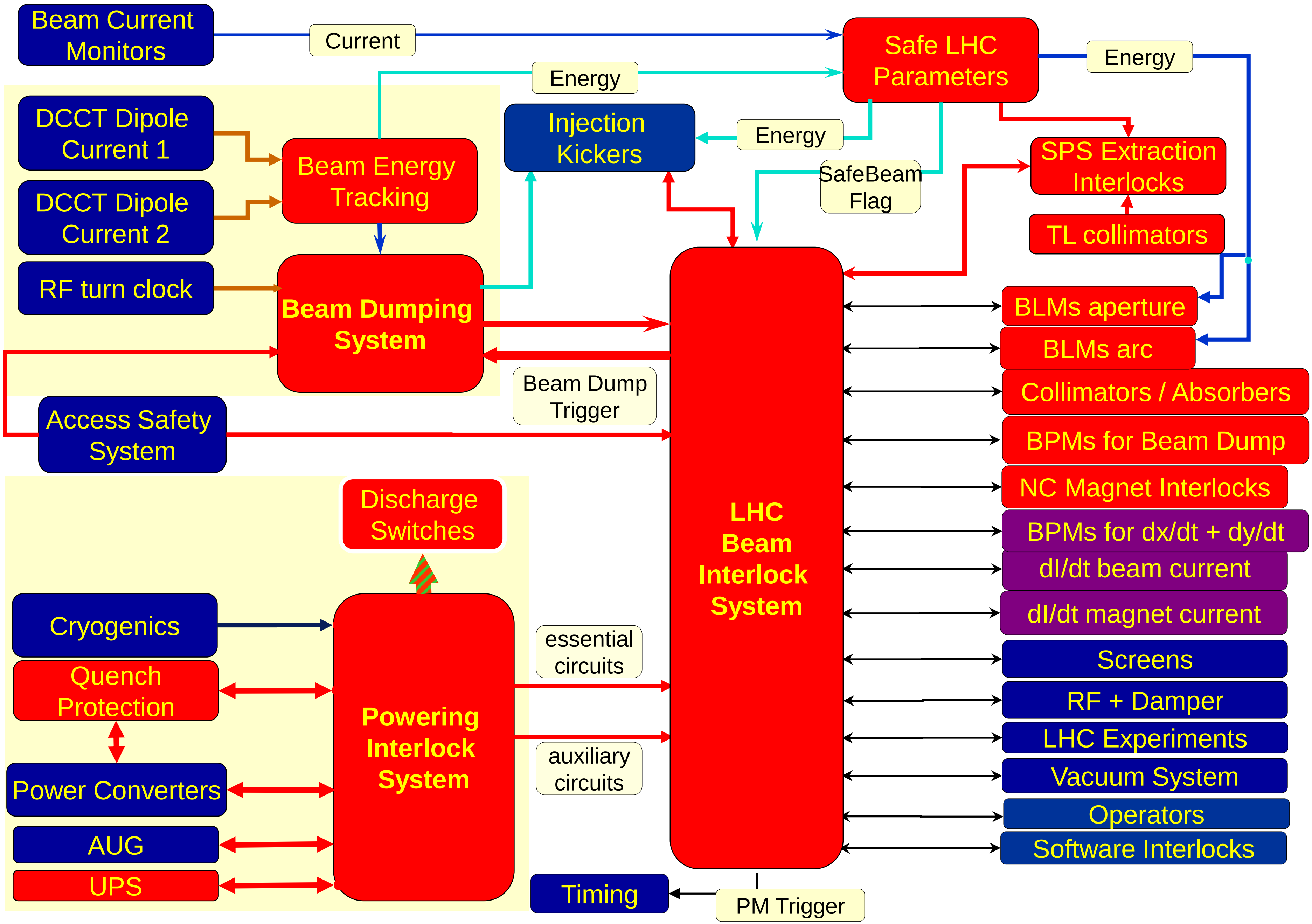
Machine protection system integration, software progress - collecting ideas -

RS, JW, BG, RA, ML, VK, BD, RL, VB, BP, MZ, BT, MJ

as preparation for MAC 9 December 2005

Recalling machine protection systems
What area of software are concerned?
Operational phases and protection
Critical settings
Conclusions

All systems and hardware links



"Machine protection system integration, software progress" – what software ?

In general, LHC machine protection done by hardware. Software for machine protection being used as little as possible….

Software related to protection

- Management of critical settings (= configuration data ?)
- Software interlocks
- Sequencing
- Post-Mortem

M.Harrison as MAC member: I believe that the MAC is probably interested in all the topics you mention. However since the MPS review raised the issue of configuration control as the biggest problem from their perspective then I think that addressing this issue directly and in some depth would be useful.

Operational phases and protection

- Circulating beams in LHC
  – detecting failures and dumping the beams
  – protection systems must be ready during a fill at any time
  – relies on correct settings in the protection systems (example: BLMs must use correct thresholds)
  – collimators / absorbers should be correctly positioned (relies on correct settings)
- Scheduled and non scheduled transients when dumping the beam
  – safe extraction of beam to the beam dump blocks (kicker and septum)
  – (some) collimators and beam absorbers should be correctly positioned (correct settings)

- Scheduled transients when filling the LHC
  – safe transmission of beam from SPS to LHC
  – a trigger is required to extract beam from SPS (no trigger = no risk)
  – safe transmission relies on correct settings (magnet currents, position of collimators, local orbit during extraction, ….)
  – verifying correct settings before extraction / injection (procedures)

Software for protection with circulating beams

- Core of the protection systems: software processes are not required to detect a failure and to trigger a beam dump
  - for some systems must be very fast, not possible to do with software
  - therefore done with hardware (incl. FPGA with safety functions not remotely reprogrammable)
  - for some systems can be slow: safety PLCs

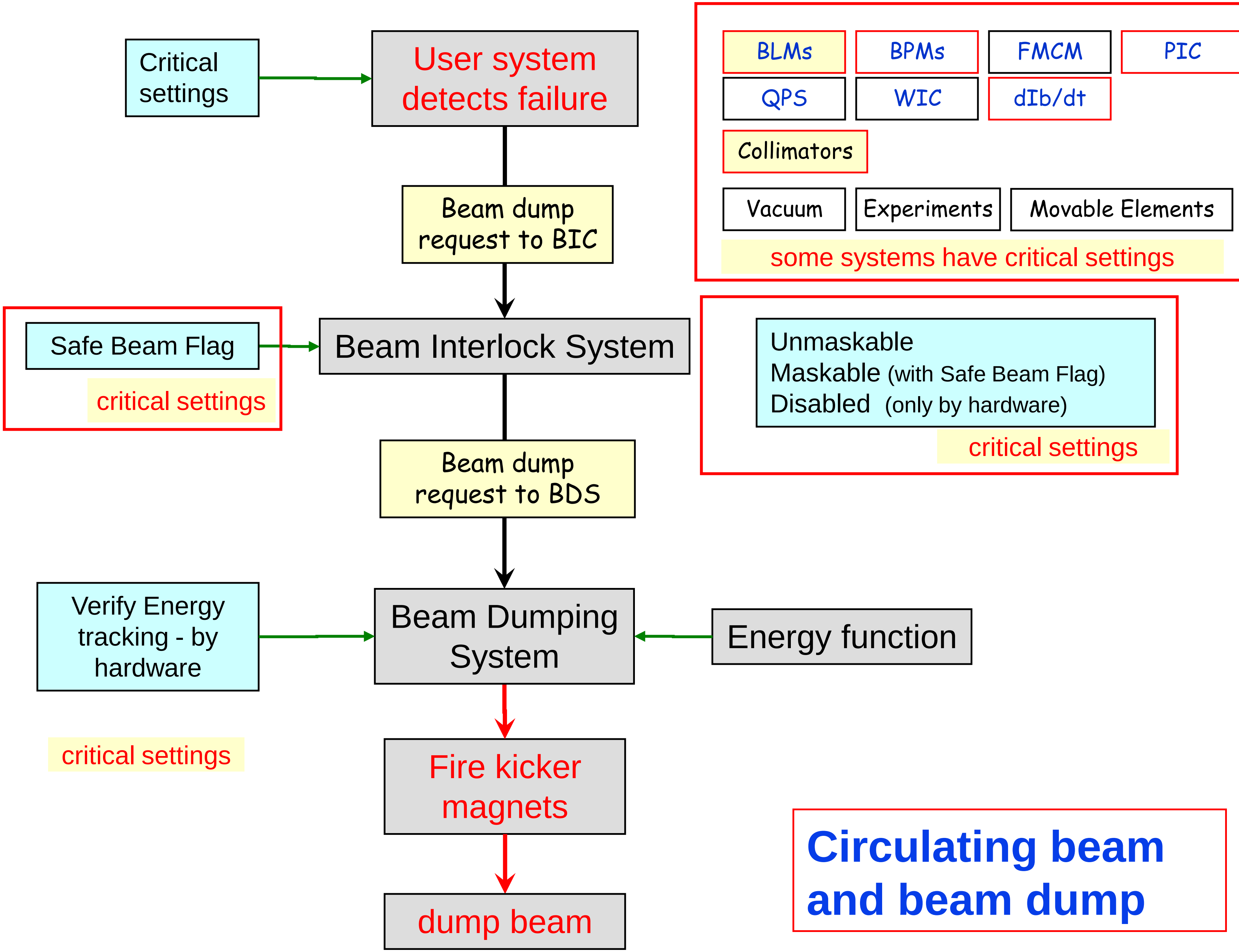
- Critical settings
  - several systems use settings for interlock levels. A wrong value in a setting might compromise protection

- Post Mortem
  - to ensure that the beam dump was correctly executed, with no degradation of the protection systems (for example, no loss of redundancy)

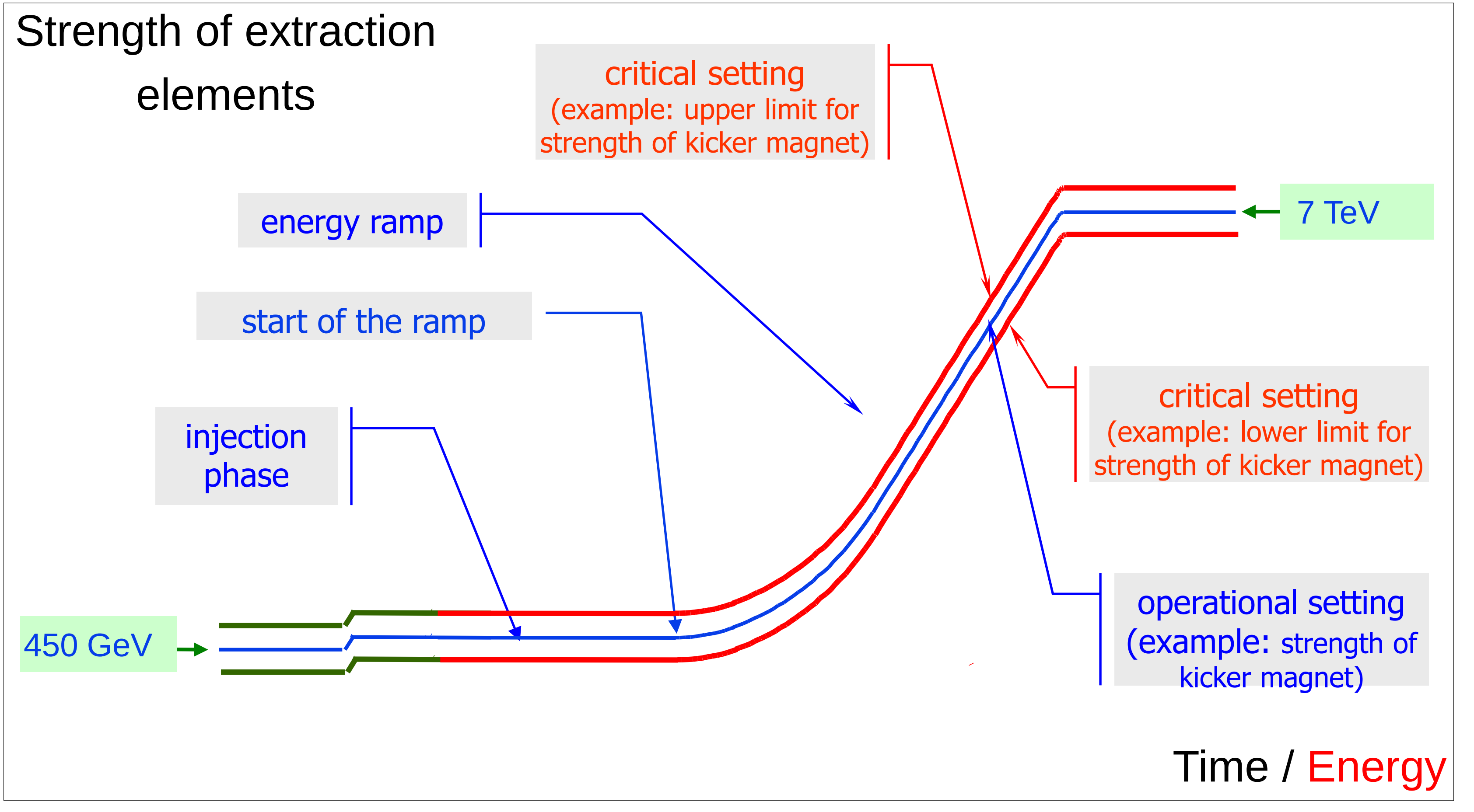
- **S**oftware **I**nterlocks **S**ystem
  - used in SPS to verify the status of a set of equipment, to anticipate failures and to give early alarms
  - complex interlock logic may be implemented in the SIS
  - software interlocks are flexible, new channels may be added ‘rapidly’

Protection when filling the LHC

- The stored energy in the beam from the SPS is 0.5% of the energy in the nominal LHC beams at 7 TeV
  - high intensity beams extraction has been done in the past (a few accidents happened …)
  - required for CNGS in 2006, same interlock logics and hardware as for LHC
- Beam permit from a number of user systems is required to allow extraction from SPS
  - Beam position and magnet current – changes during SPS cycle
  - Collimators positions in transfer lines and LHC are set to a position and remain fixed
- Critical settings: several systems use data for interlock levels
- Software processes to provide beam permit for extraction
- Procedures before the injection of beam into LHC – Sequencer
- Analysis after every extraction – did everything work ok? (Shot-by-Shot Logging ⇔ Post Mortem)
- Slow monitoring of parameters – SPS Software Interlock System

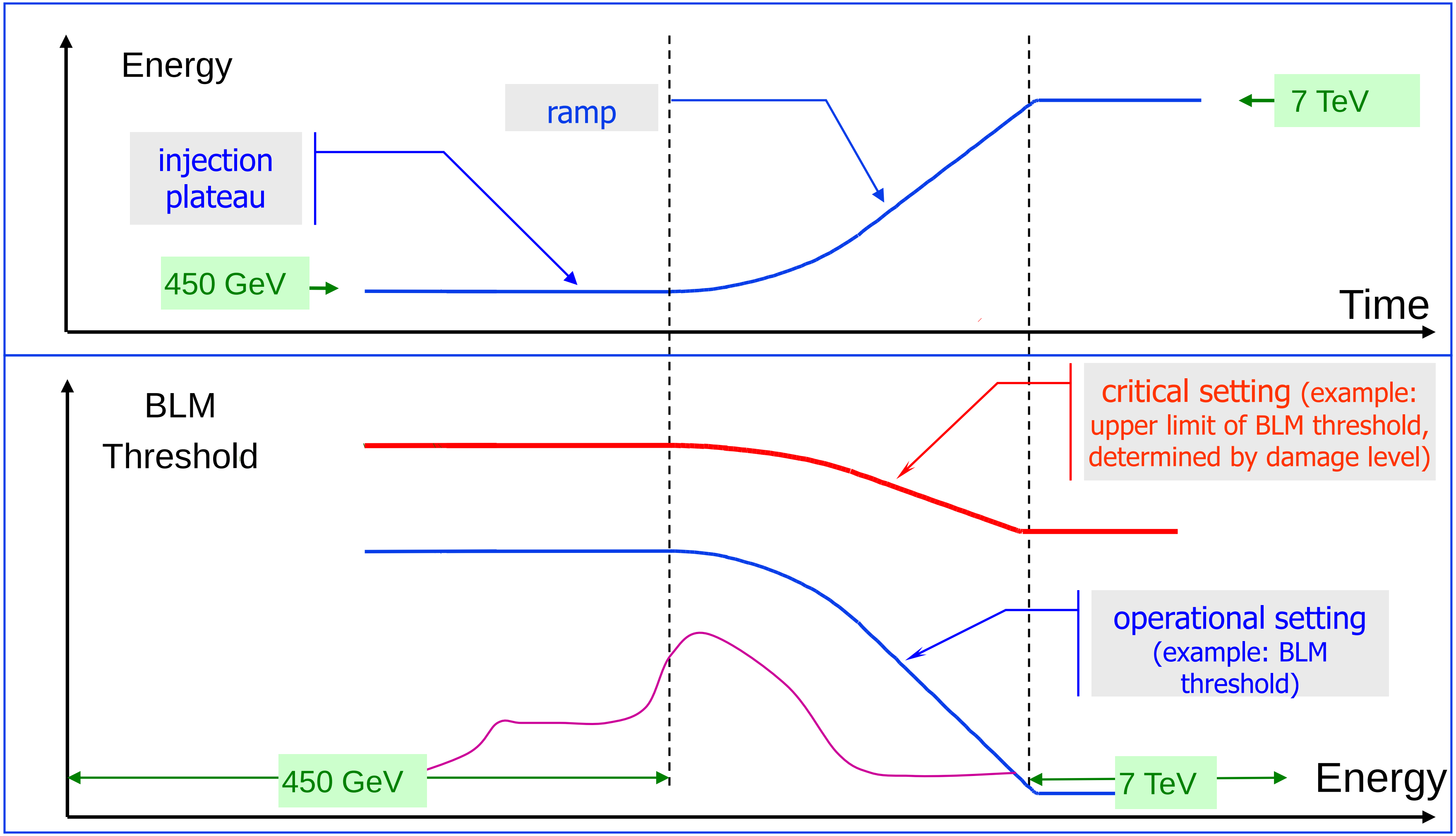

Critical settings
User system detects failure
BLMs
BPMs
FMCM
PIC
QPS
WIC
dIb/dt
Collimators
Vacuum
Experiments
Movable Elements
some systems have critical settings
Beam dump request to BIC
Safe Beam Flag
critical settings
Beam Interlock System
Unmaskable
Maskable (with Safe Beam Flag)
Disabled (only by hardware)
critical settings
Beam dump request to BDS
Verify Energy tracking - by hardware
Beam Dumping System
Energy function
critical settings
Fire kicker magnets
dump beam
Circulating beam and beam dump

LHC energy ramp – example for operational setting and critical setting



- general philosophy: operation settings and window around the setting defining safe limits
- critical settings defined for BDS in hardware, not possible to change it remotely
- critical settings can be read, and compared with settings in data base (for checks)
- task of the HW: if operational setting outside window => dump beam

Beam Loss Monitor Thresholds during energy ramp



- BLM thresholds are a function of energy, and defined for 11 integration windows
- There is an operational threshold and a limit for such threshold (maximum threshold)
- The operational threshold should never exceed the maximum threshold
- Task of the BLM HW: if BLM reading > BLM threshold => dump beam

Critical settings

Critical settings are parameters related to machine protection systems

- interlock thresholds, flags for disabling interlocks, …

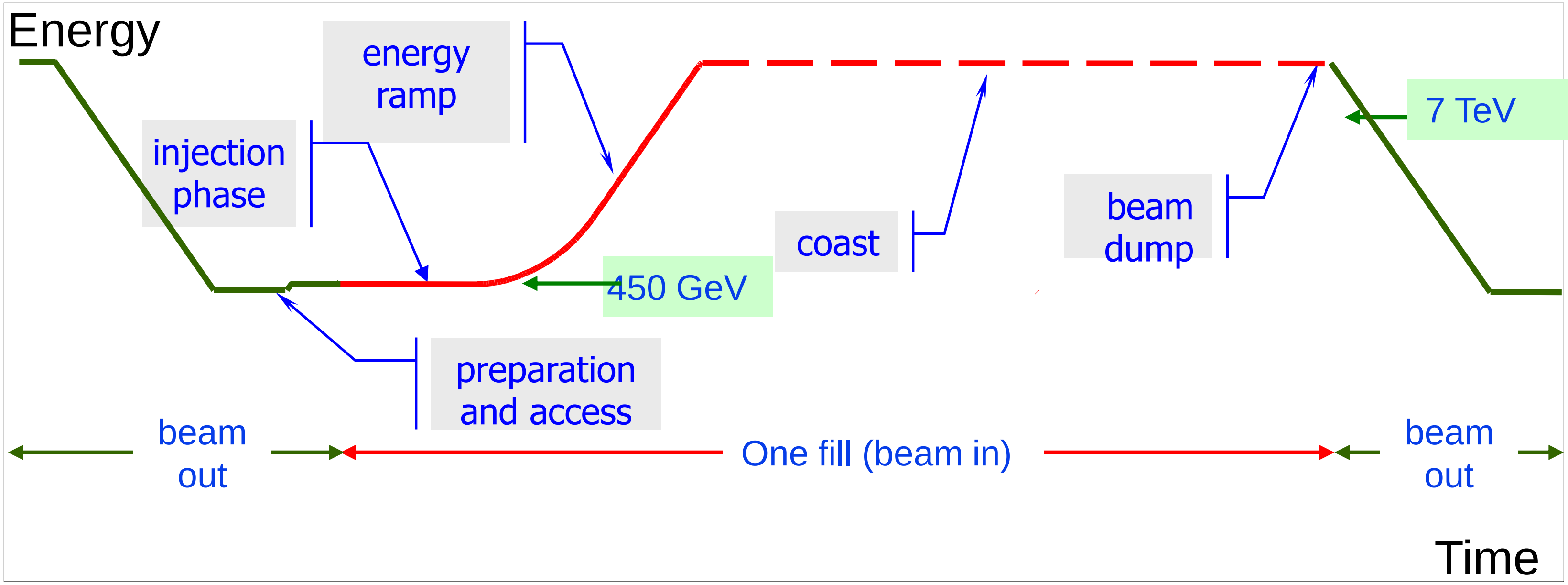
Critical setting can be constant during a fill (static critical settings)

- Boolean value (True / False)
  - Examples
    - Input to Beam Interlock System – disabled or enabled (HW)
    - Beam Loss Monitors – in the interlock chain: Yes or No
    - Collimator jaws - in the interlock chain: Yes or No
- Numeric value, constant during a fill
  - Examples
    - safe beam limit

Critical setting can change during a fill (dynamic critical settings)

- Numeric value, as a function of a parameter (for example energy)
  - Examples
    - limits for strengths of extraction kicker and septa magnets versus energy
    - beam loss monitor threshold versus energy
    - collimator position versus energy
    - collimator position versus beta squeezing factor

Terminology: configuration



LHC Configuration: a set of parameters that describe the LHC fill

- Parameters that are constant for one fill: static configuration parameters
  - ions or protons, totem operation, LHCb magnet polarity plus or minus
  - injection energy (normally 450 GeV) and physics energy (normally 7 TeV)
  - from one fill to the next fill, static configuration parameters might change
- Parameters that change during one fill: dynamic configuration parameters
  - energy (450 GeV $\rightarrow$ 7 TeV), beta squeeze, x-ing angle, … (numeric)
  - filling, ramping, stable beam, … (Boolean)
- Terminology….. to be agreed upon

Critical settings…… and LHC configuration parameters

- Some critical settings do not depend on configuration parameters
  - example: interlock channels for the BIC
- Some **critical settings** need to be updated when **static configuration parameters** (fill configuration) change:
  - example: limit for safe beam operation when changing from protons to ions
- Some **critical settings** change during one fill as function of **dynamic configuration parameters**
  - to be loaded into the hardware either for a fill, or for a run, or only once
  - the dynamic configuration parameter is distributed to the hardware
  - the interlock process uses the critical settings as a function of the dynamic configuration parameter (example: BLM threshold as function of energy)

Locking of critical settings: critical settings must not be changed in an uncontrolled way

- send the settings to hardware (possibly with some software key), and read them back to ensure that the correct settings are used by the hardware
- devise tests to ensure that the correct critical settings are used (see later)
- prevent changing parameters during beam operation (for example, only allow modifications at the pre-injection plateau)

Critical settings: for what ?

- Some critical settings are defined in hardware, and it is neither necessary nor possible to remotely modify such settings
  - this is the preferred strategy
  - it is required to read such settings, and an image should be stored in a DB
- Systems with settings defined in hardware
  - Beam Interlock System and Beam Dumping System
  - Quench Protection System + Energy Extraction Systems
  - Safe beam flag limit
  - FMCM (Fast Magnet Current change Monitor)

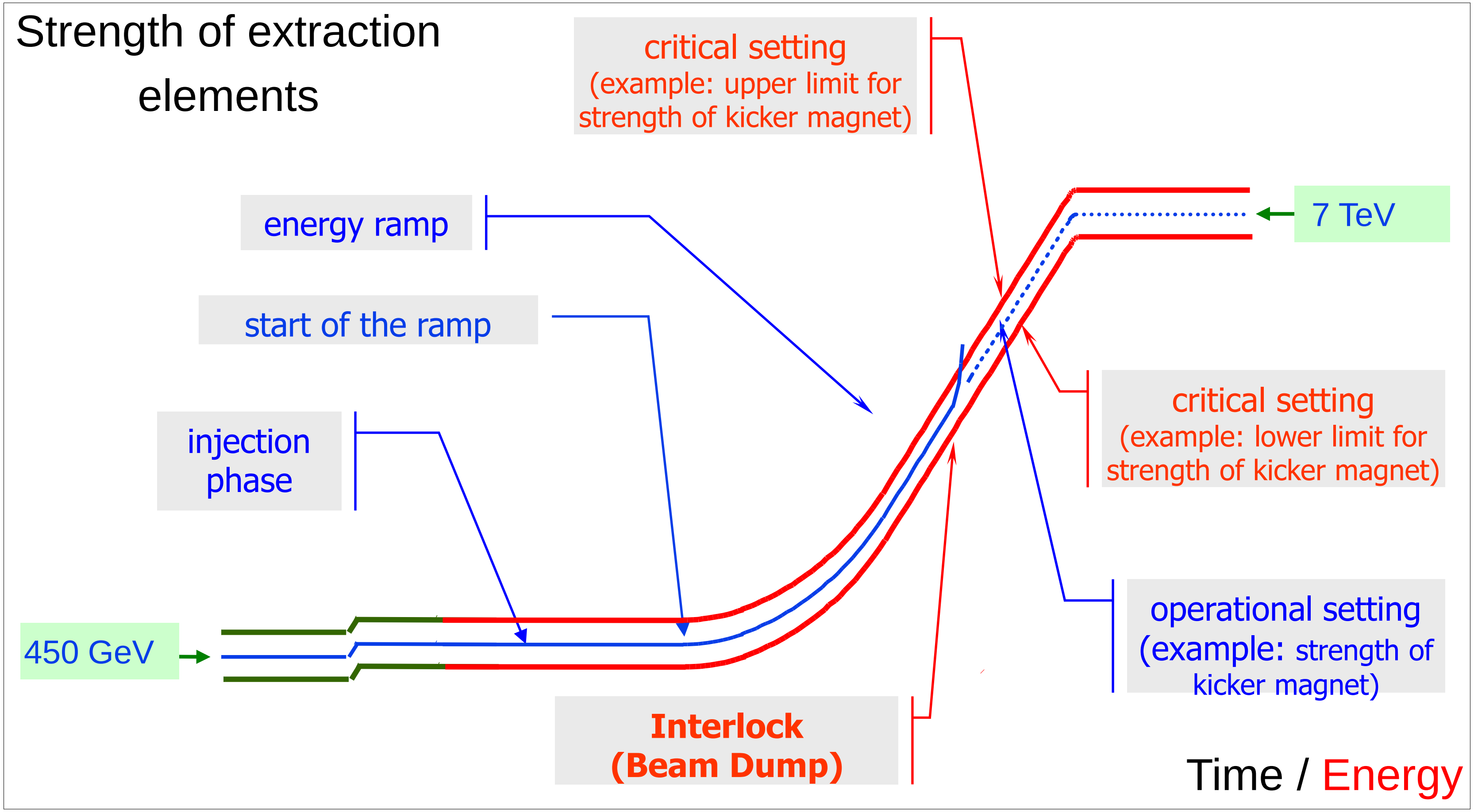
Examples

- Systems with critical settings that must be modified remotely
  - Thresholds of Beam Loss Monitors
  - Interlock position (window) of Collimators and Beam Absorbers
  - Current limits for transfer line magnets
  - Beam position in SPS at extraction

Examples

Level of criticality

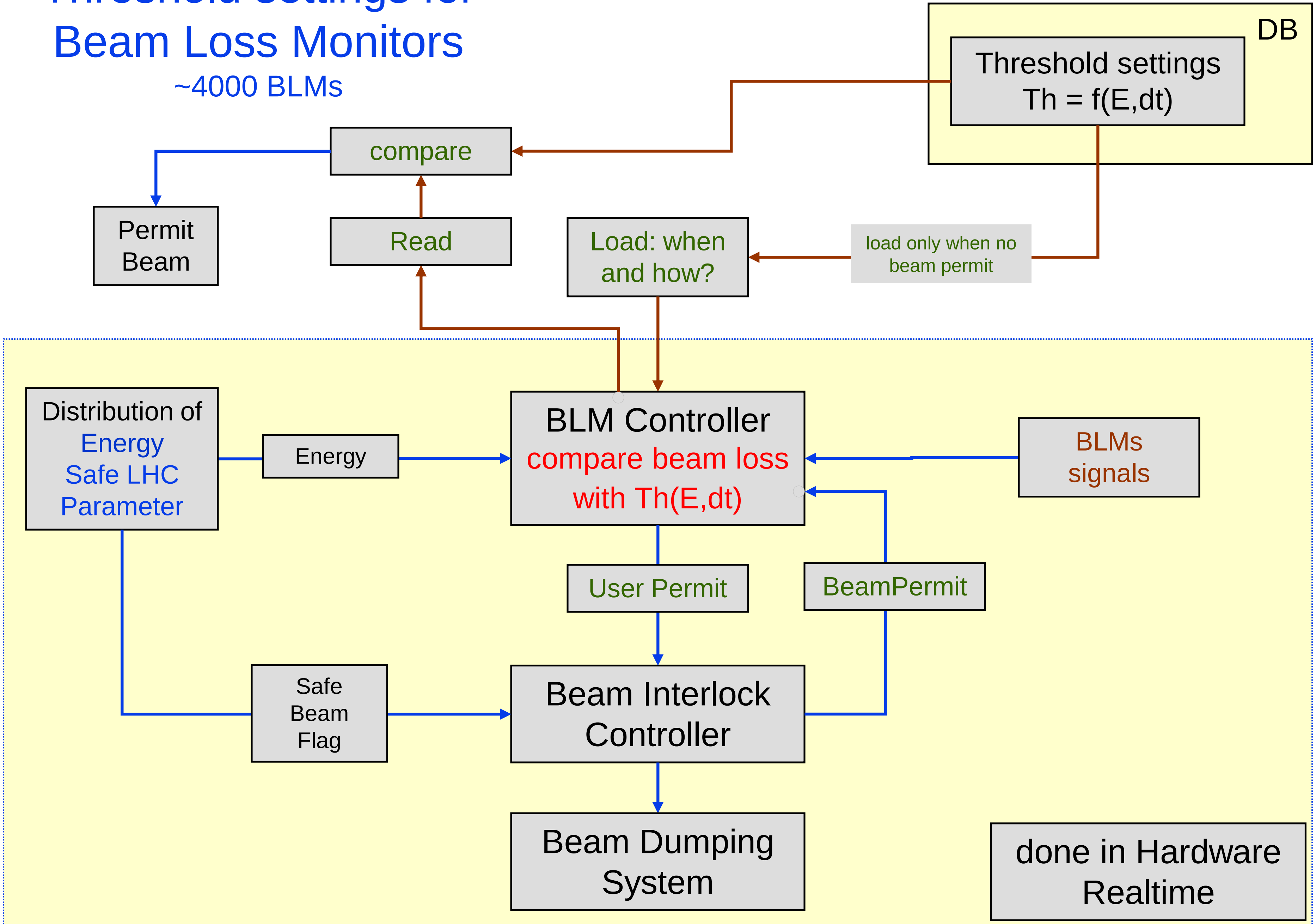
LHC energy ramp – example for test to verify that the critical settings are correct



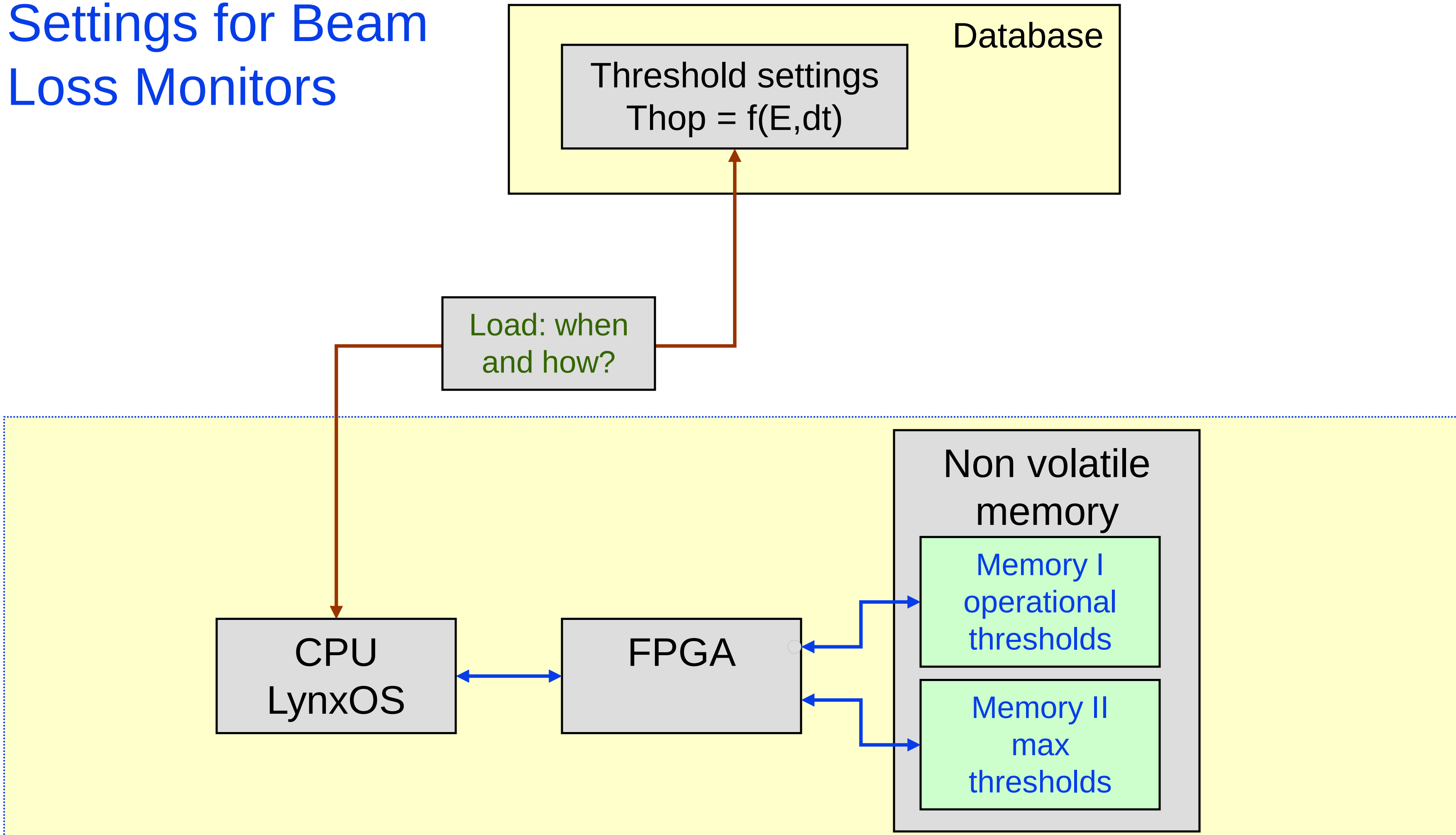
- trim the operational setting outside the allowed range
- should then cause an interlock

Threshold settings for Beam Loss Monitors

~4000 BLMs



Settings for Beam Loss Monitors



Questions:
How to be sure that the correct data is in the memory
Is it possible to inhibit loading of THmax via the network ?
How can we assure that the correct data is in THmax ?
Can we use techniques such as CRC and hash to ensure correct data ?
How to block the data when is has been loaded and successfully checked ?
The integration windows are sliding ?

Example: critical settings for Beam Loss Monitors

In total, there are about 4000 BLMs in the LHC

When the threshold is exceeded for one BLM the beams will be dumped

The threshold depends on:

- type of BLM
- beam energy
- duration of beam loss
- particle type (to be verified)

For each BLM, ~300 numbers determine the thresholds (2-d array as a function of energy and loss duration)

There are BLMs that have identical thresholds, and are defined as a group

There are N groups of BLMs (N ~ expected 10…20, but could also be much larger)

One BLM belongs to <u>one and only one</u> group

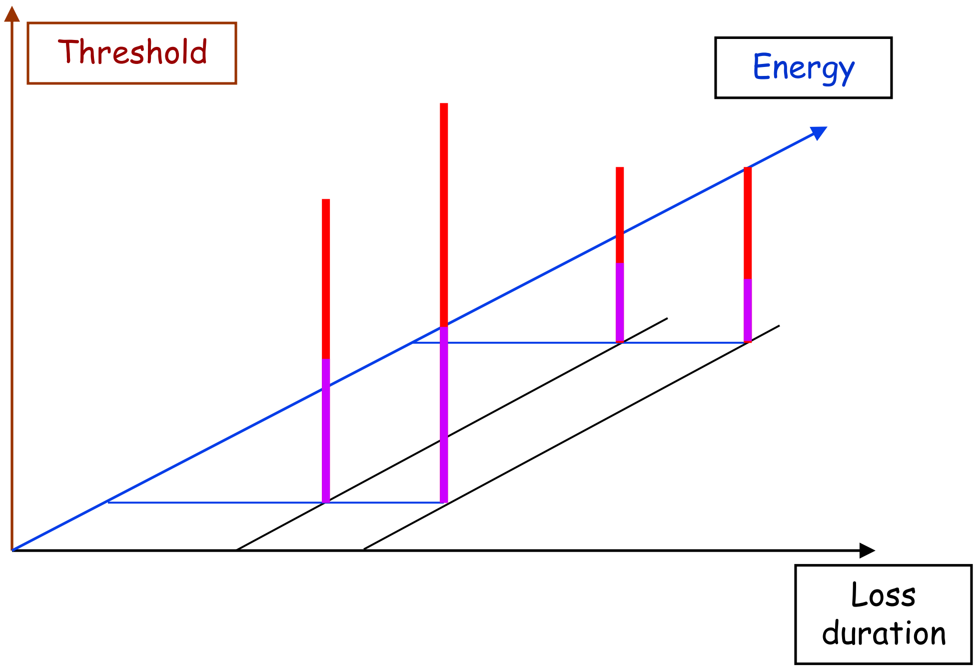
For each group, there is an upper limit of threshold values defined that cannot be exceeded (safety level)

The thresholds could be defined by group, or for individual BLM (operational level)

Example: Critical settings for Beam Loss Monitors

Group 1 - thresholds -					
	Time [ms]				
Energy [GeV]	1	10	100	1000	10000
450	1	9	17	25	33
1000	2	10	18	26	34
2000	3	11	19	27	35
3000	4	12	20	28	36
4000	5	13	21	29	37
5000	6	14	22	30	38
6000	7	15	23	31	39
7000	8	16	24	32	40

Group 1 - limits -					
	Time [ms]				
Energy [GeV]	1	10	100	1000	10000
450	50	58	66	74	82
1000	51	59	67	75	83
2000	52	60	68	76	84
3000	53	61	69	77	85
4000	54	62	70	78	86
5000	55	63	71	79	87
6000	56	64	72	80	88
7000	57	65	73	81	89



- For each group there are two tables
  - table with operational thresholds
  - table with maximum thresholds
- For each BLM, there is a table defining the group for this BLM
- An operator can edit the table with the operational thresholds, but not with the maximum thresholds
- A specialist can edit the table with the maximum thresholds

Modifying thresholds ….

Operations on the data that are required

- Change the operational thresholds for one group / BLM
- Attribute one BLM to one group
- Change the attribution of one BLM to from one group to another group
- Add one group
- Copy the operational thresholds from one group to another group
- Copy the maximum thresholds from one group to another group
- Change the maximum threshold for one group

Verifications required

- Compare the operational settings of the BLMs

Conclusion

- Functional specification for “Management of critical settings being written”
- see Verena …

Progress

- Management of critical settings
  - started, Draft of a Functional Specification has been written, prototype should work for CNGS operation with high intensity beam in summer 2006
- Post Mortem
  - work ongoing for hardware commissioning, not powering of sc magnets will be possible without such system
  - system to be extended for 2007 beam commissioning
- Software interlock system – new system being developed for the SPS run in 2006, also to be used for LHC
- Sequencer
  - work started for hardware commissioning and a sequencer was already used
  - can this be extended to beam commissioning? The concepts certainly yes, the code … needs to be seen

Strategy for protection for scheduled events

If potentially dangerous actions are planned: injection, starting the ramp, starting beta squeeze, beam dump at end of fill, …

- Sequencing of actions by procedures based on software processes
  - check if all elements are in the correct state allow for injection
  - process that is required to give “green light” for injection

Software interlock system: Hardware surveillance by software that can stop beam operation

- as discussed above for some parameters
- general software interlock system that reads equipment states, and produces software interlocks (existing SPS system – being upgraded for future SPS, CNGS and LHC operation)

Hardware protection has been discussed already

- avoid dangerous situations by applying procedures based on hardware inject into empty LHC only with low intensity beam
- only if beam is circulating, inject high intensity beam
- protect in case of failure
- beam absorbers for single turn failures

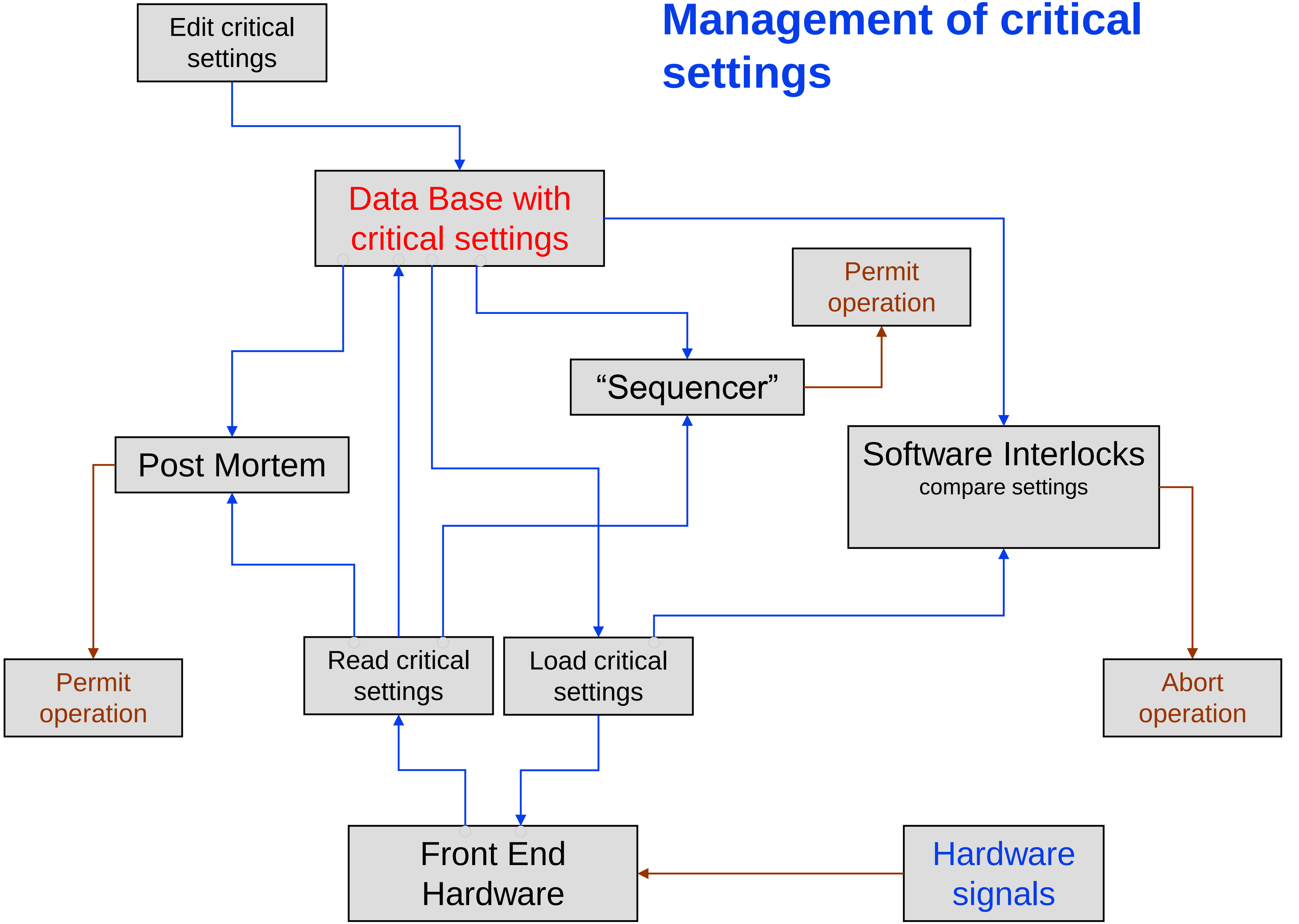
Example: Beam interlock system – configuration data

- A beam dump is performed if at least ONE connected system requests to dump
- This channel must be enabled
  - verified during commissioning
  - not possible to disable a channel remotely
  - the state of all channels (enabled – disabled) is known
- For channels that are maskable
  - masking only present with low intensity (“safe”) beam
  - the status of all masks is known, and will be compared with the data in a database
- Example: an electronics module needs to be changed
  - only done by a specialist
  - only one card that needs to be configured (channels are enabled / disabled on the PCB by switches)
  - the specialist configures the new card as the old card – the system should be operational
  - before “giving green” light for beam operation, the configuration of the new module is compared with the data in the database, only if consistent, beam permit is given

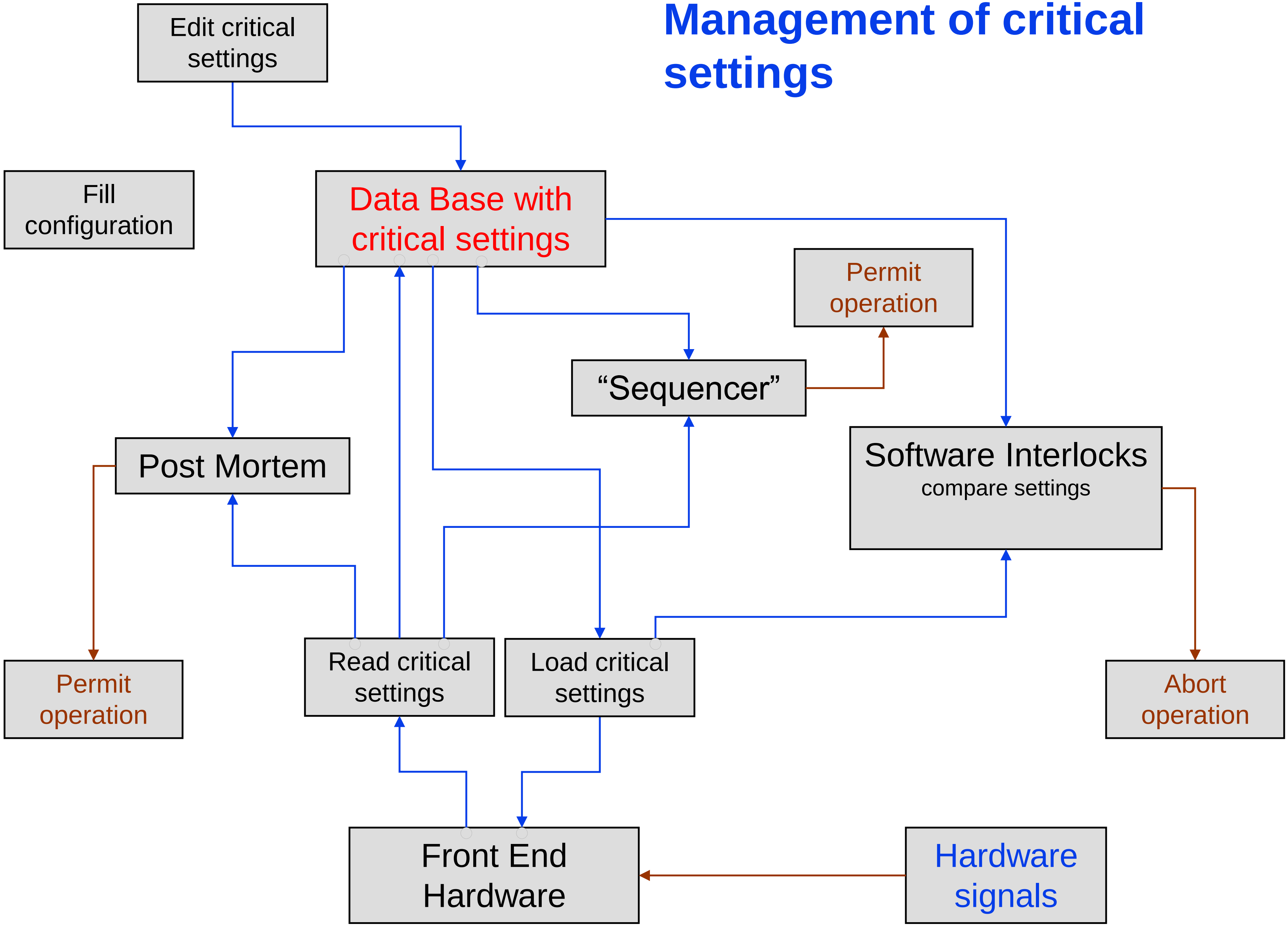
LHC cycle


Energy
energy
ramp
coast
beam
dump
start of the
ramp
7 TeV
injection
phase
beta
squeeze
start
injection
450 GeV
preparation
and access
Time
beam
out
One fill (beam in)
beam
out

Management of critical settings



Management of critical settings



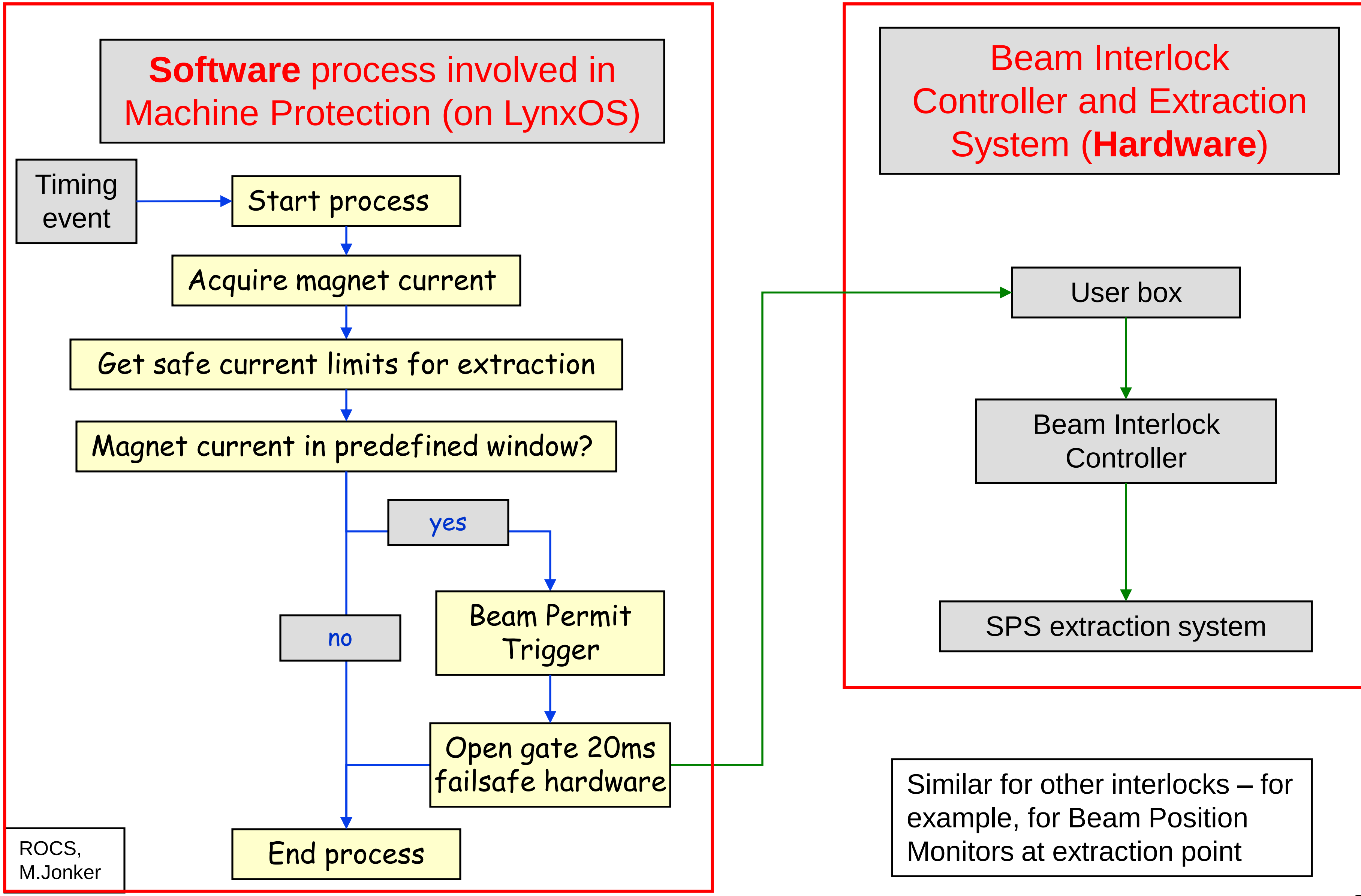
Conclusions

- there is a lot to do
- we have to operate the other accelerators, and therefore some software will be deployed already in 2006, as a prototype for 2007
- for each domain, we start to have some competence, and people who feel responsible

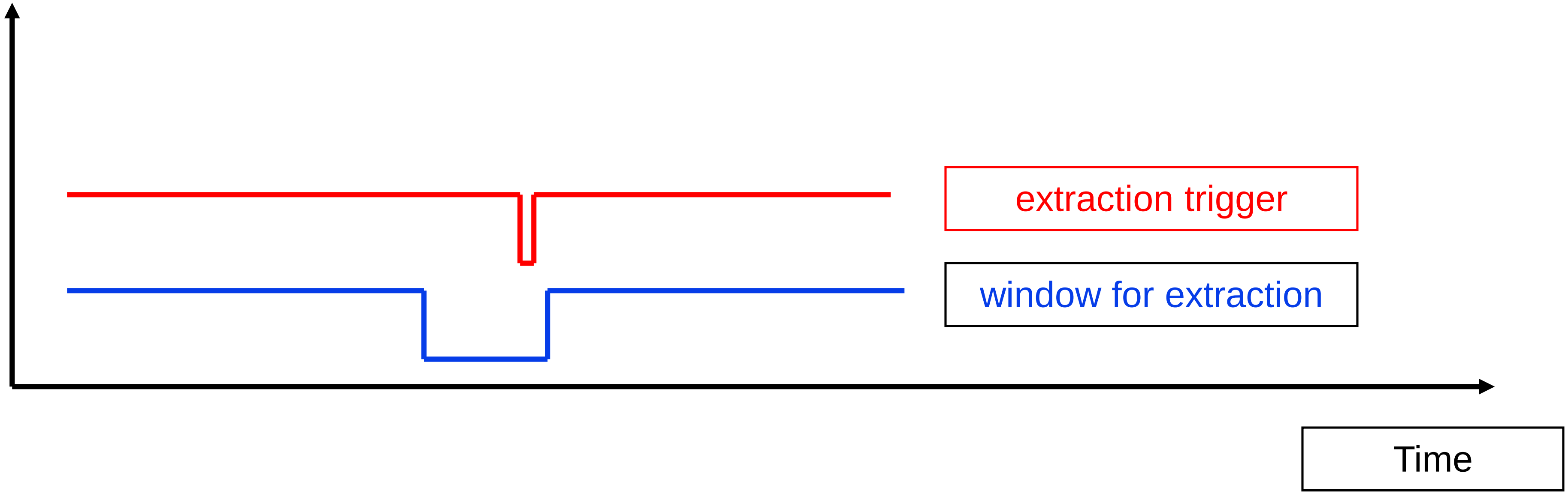
Questions:

- *what is the relation of LSA and MCS* ?

Example: Verify correct magnet current before extracting beam from SPS



Software failure modes



Failures that lead to non-extracted beam

- Software does start
- Software does not work correctly until end

Failures that could lead to damage

- Wrong value for magnet current AND wrong values for safe current limits (example: 900 A instead of 1000 A, and a window from 100 A …. 2000 A)

How to ensure that the current limits are correct ? Management of critical settings

Real-time systems versus non Real-time systems

Real-time – bound response time

- hardware

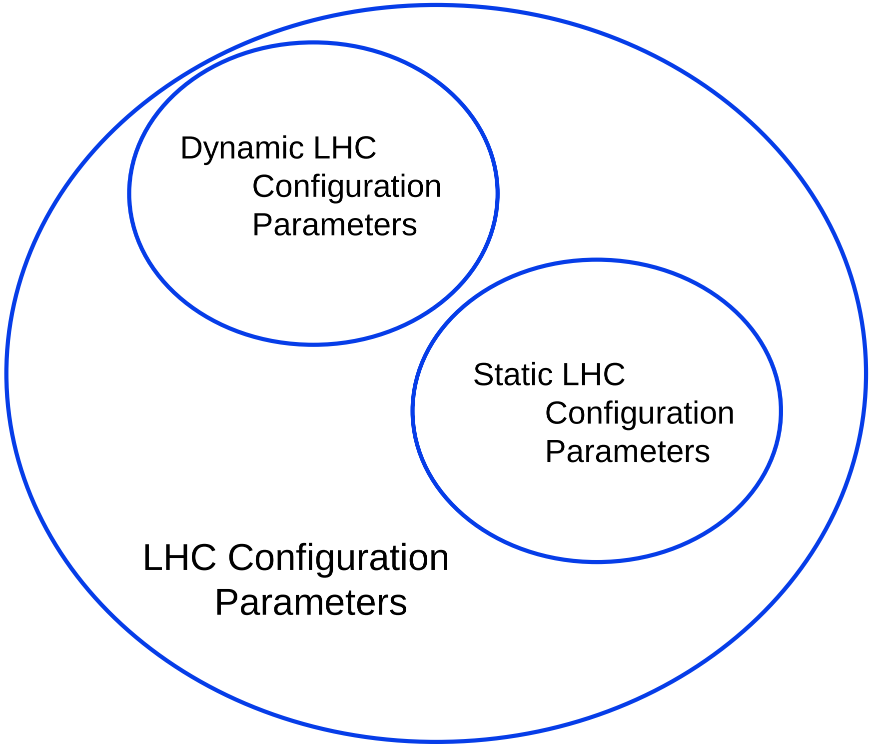
Non Real-time – not bound response time

- sequencer

LHC machine protection does not rely on “safe software”

- what is safe software ? Deterministic and predictable….

Critical settings: for what ?



Configuration parameters

Examples for static configuration parameters that do not change during a fill

- ions or protons, totem operation, …
- LHCb magnet polarity plus or minus
- injection energy (normally 450 GeV) and physics energy (normally 7 TeV)

…should be taken care of before injection of beam

Examples for dynamic configuration parameters that change during a fill

- filling: Yes / No
- energy (450 GeV $\rightarrow$ 7 TeV)
- squeezing factor
- stable beam for physics: Yes / No

... change during the fill

Questions

- useful approach ?
- better names ?