Protection Controls for High Power Accelerators

J. Wenninger

CERN

AB Department / Operations Group

Acknowledgments : V. Kain, R. Schmidt, M. Zerlauth, J. Uythoven and other CERN colleagues, A. Dress (BNL), M. Staak, M. Lomperski (DESY), K. White (ORNL) , M. Böge (SLS), E. McCrory (FNAL)

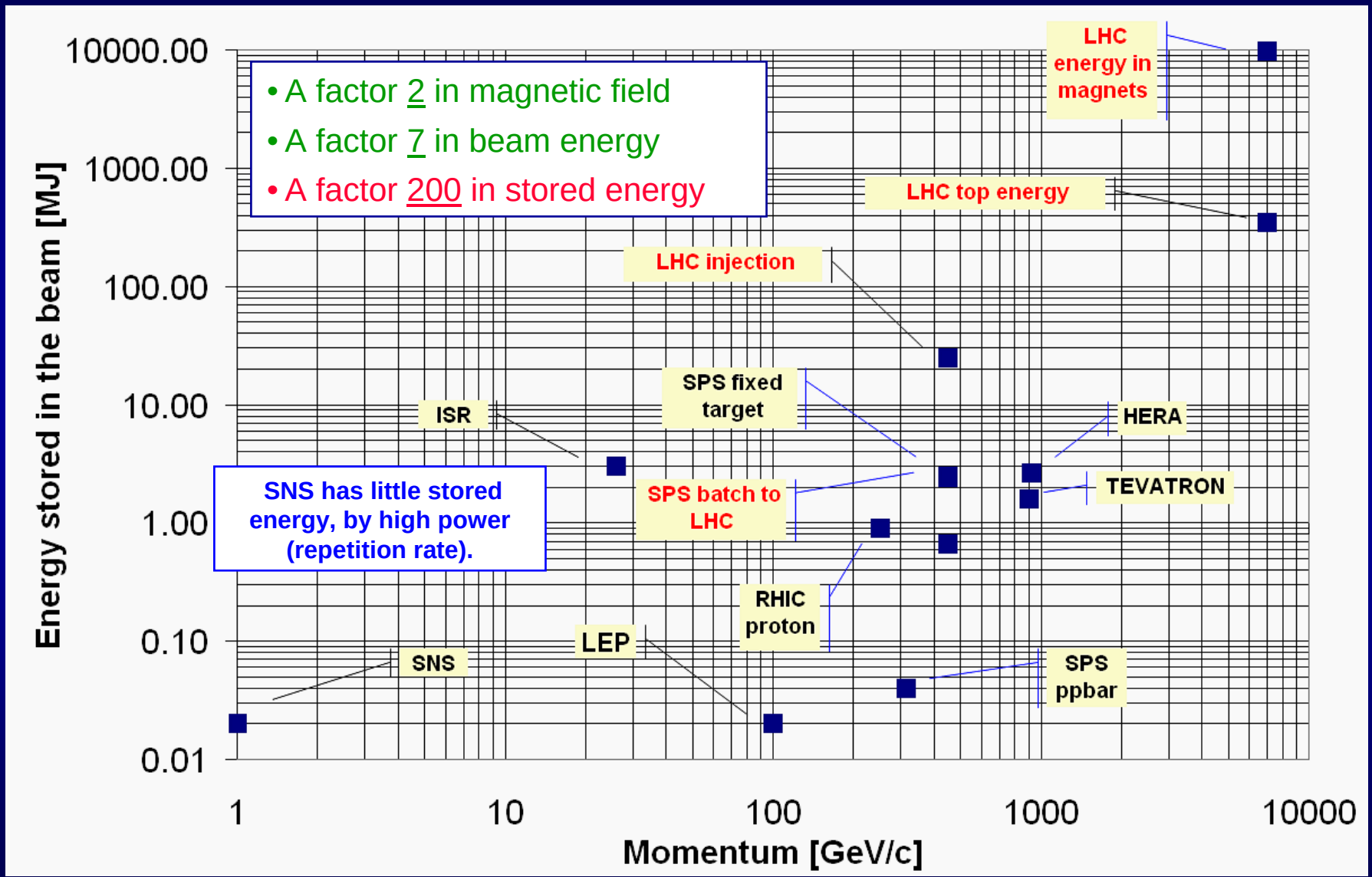
Motivation

- The latest generation of hadron machines reach stored energy and power levels where components may be easily damaged by beam loss of even a small part of the beam. And synchrotron light facilities follow closely…
  - **Multi MW beam power : PSI, SNS, JPARC, IFMIF,…**
  - **Multi 100's MJ stored beam energy : LHC**

- Such machines are designed with machine protection (MPS) as an important design constraint and all are equipment with fast interlock systems based on 'Hardware':
  - Nowadays even 'Hardware' interlock systems contain 'embedded software'.
  - The desire to keep the MPS system 'flexible' implies the introduction of 'parameters' within the MPS, and access possibility to potentially critical settings.

Balance of flexibility versus safety

The LHC challenge



Where the WEB was born…

- **Equipment access through a WEB browser becomes ever more common:**
  At CERN without separation of networks, almost every accelerator device would be open to the internet world !!!

- **More public focus:**
  Very large (and expensive) projects receive a lot of ‘publicity’ which in turn may make them interesting for ‘software attacks’.

And some become famous for (mini) black holes !!!

>> new type of risk for high power machines

Outline

Selected controls issues for Machine Protection

- **Access Control**

  Who is allowed do something

- **Configuration Issues**

  Masking and parameter changes

- **System Validation**

Interlock testing and commissioning

- **Diagnostics**

  Post-mortem and logging

Access Control

- Aim is to prevent:
  - A well meaning person from doing the wrong thing at the wrong moment.
  - Ignorant persons from doing anything at any moment.
  - 'Intruders' from entering the control system.

… and at the same time:

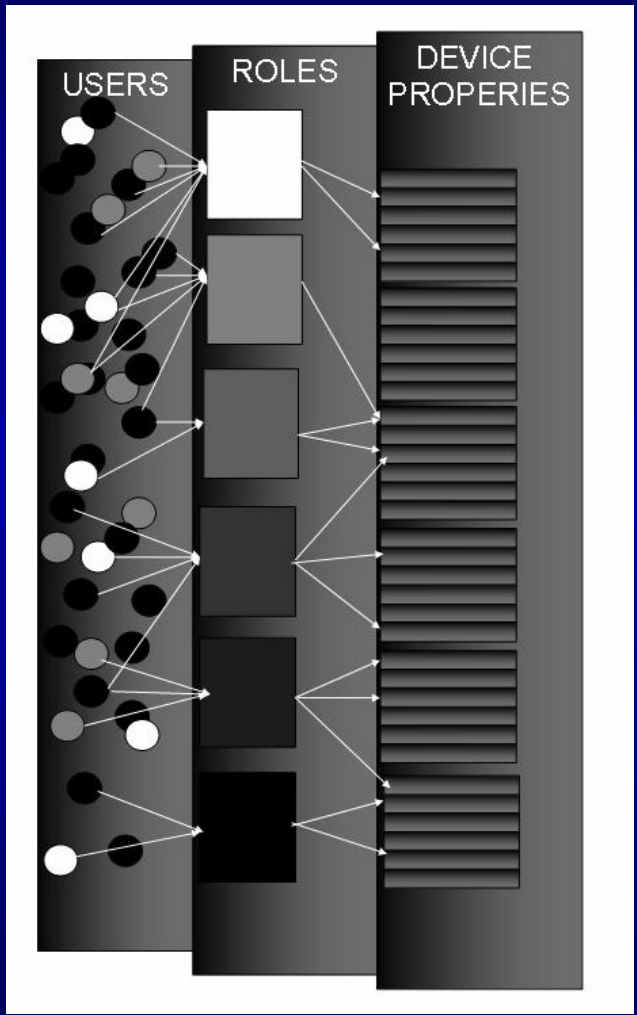
  - Avoid un-necessary overheads for operation crews.
  - Provide access for (software) engineers.
  - Provide remote access possibilities for international partners.

- Standard solutions:
  - Accelerator network is 'isolated' from general (public) internet.
  - Password protections.
  - Computer location dependent access to devices – for example FNAL & CERN.

Role Based Access Control (RBAC) for LHC

Access control from within CERN and from FNAL to the LHC accelerator complex.

- Collaboration CERN – FNAL.
- RBAC works by giving people ROLES and assigning roles PERMISSIONS to access device properties.
- RBAC is part of the CERN control system middleware.
- RBAC provides means for
  - AUTHENTICATION
    - Login with CERN central ID and password.
  - AUTHORISATION
    - Manage access maps between roles and accelerator devices.



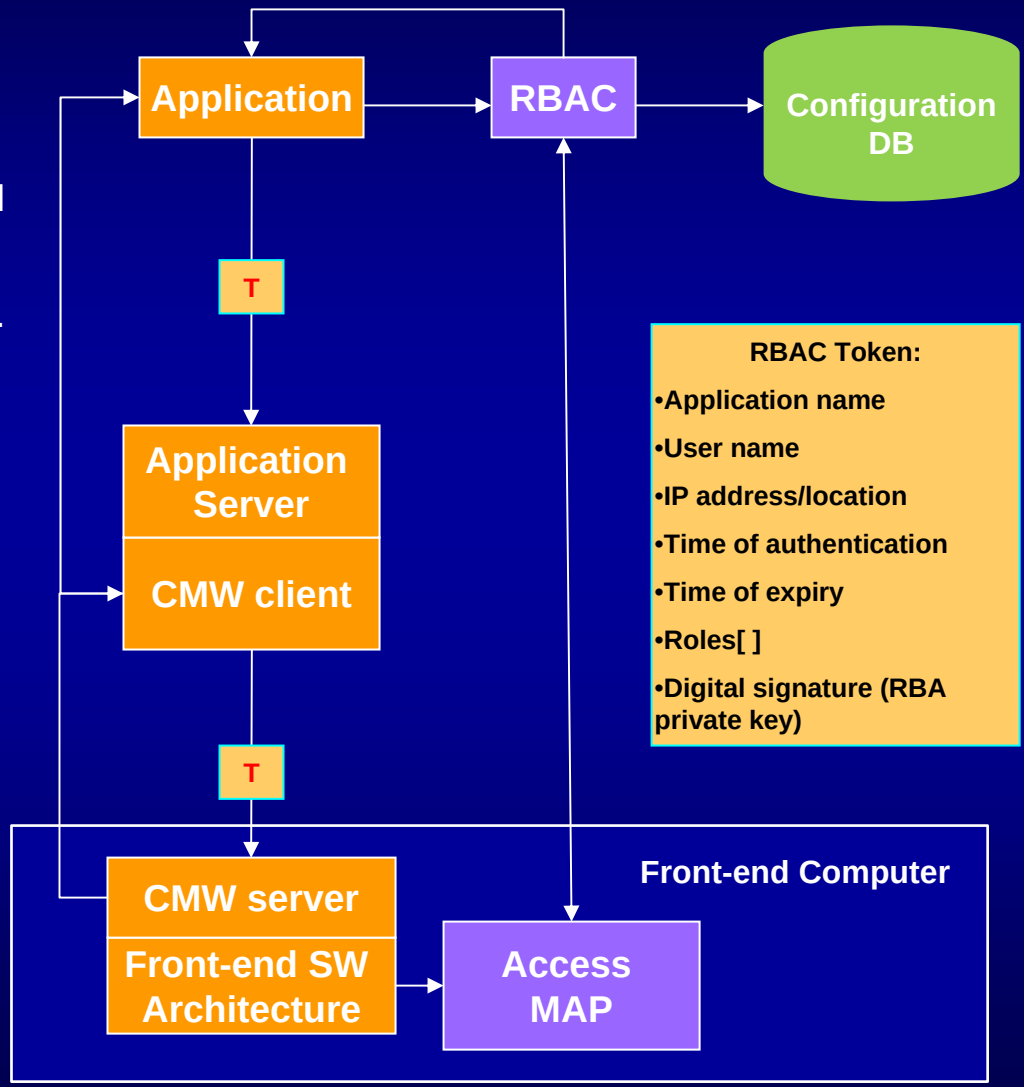
RBAC Overview

Authentication:

- User requests to be authenticated.
- RBAC authenticates user via CERN central user name and password.
- RBA returns an RBAC token to Application.

Authorization:

- Application sends token to Application Server.
- CMW client sends token to CMW server.
- CMW server (front-end) verifies token.
- CMW server checks Access Map for role, location, application…



RBAC Issues

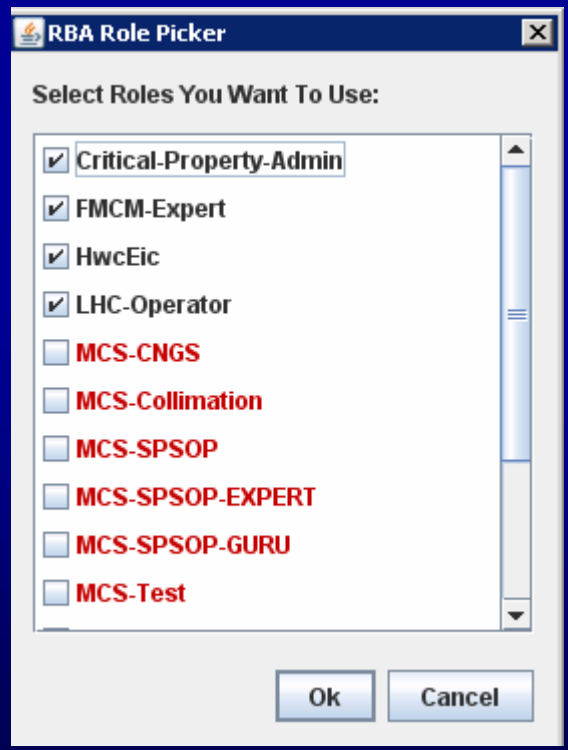
- Very complex design with access maps that can depend on :

  Device, role, location, application name, machine mode, etc
- Potential explosion of rules – must keep track !
- Need a DB … to store the roles and rules.

The system is progressively put in place for LHC.

Question : will this complex access logic work, or will it be (drastically) simplified within a few years ?

The LHC experiments also started with complex systems, and cut them down drastically…



Masking and Configuration Changes

1. **Masking** : ‘deactivation’ of selected interlocks.

   For example a complete bypass of all or part of the beam loss monitors, but without touching the monitor thresholds.

2. **Settings changes** : modification of MPS settings.

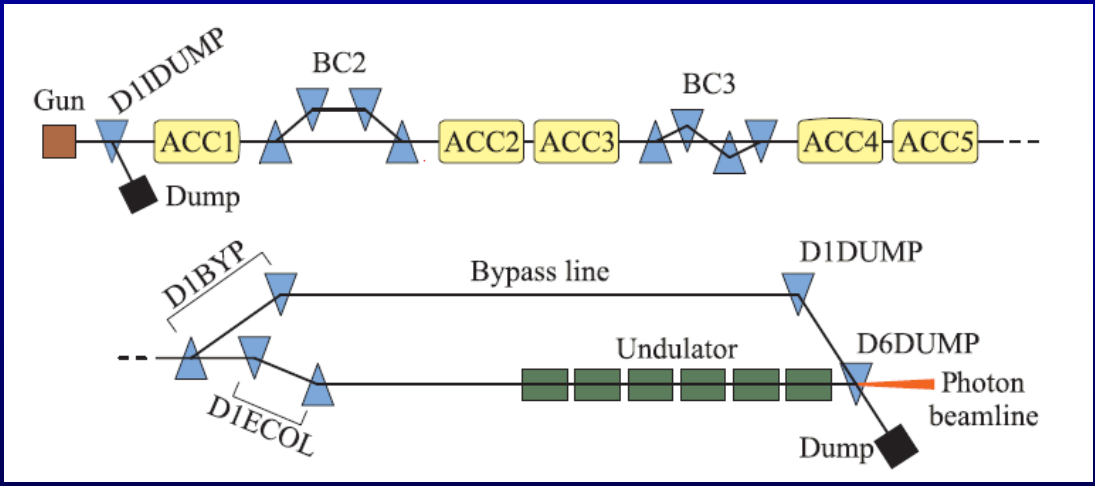
   Typically beam loss monitor thresholds etc

…for machine commissioning (low intensity), setting up, ‘experiments’ etc

Interlock Masking / Configuration changes

- Expert intervention:
  - Manual intervention by an expert.
  - Simple to implement, but only really practical for rare changes.
- Automatic beam & machine mode masks:
  - Automated configuration change based on the state of the machine or of the beam.
  - Active interlocks are (un-)masked depending on beam intensity (source state), on dumps or other essential element states.

>> used in many places



FLASH

MPS operation modes:
- Gun
- Analysis
- Bypass
- FEL

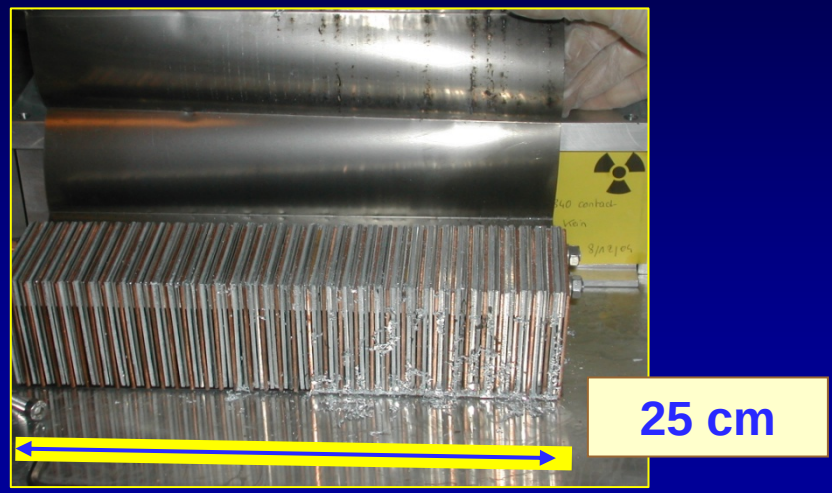
SPS & LHC : Safe Beam Flag

- Logical flag that indicates if the beam is considered to be ‘safe’ (i.e. below damage threshold) or not. The flag is distributed in a safe way to all elements of the beam interlock system.
- The Safe Beam Flag depends on the **beam energy** and **intensity**:
  - Energy information based on redundant sources (power converters).
  - Intensity based on redundant beam current transformers.
- Definition for LHC – based on a Copper ‘target’ :
  - Safe limit @ 450 GeV (injection) : 10^{12} protons
  - Energy scaling $\propto E^{-1.7}$

>> Limit defined from simulation & experiment @ the SPS

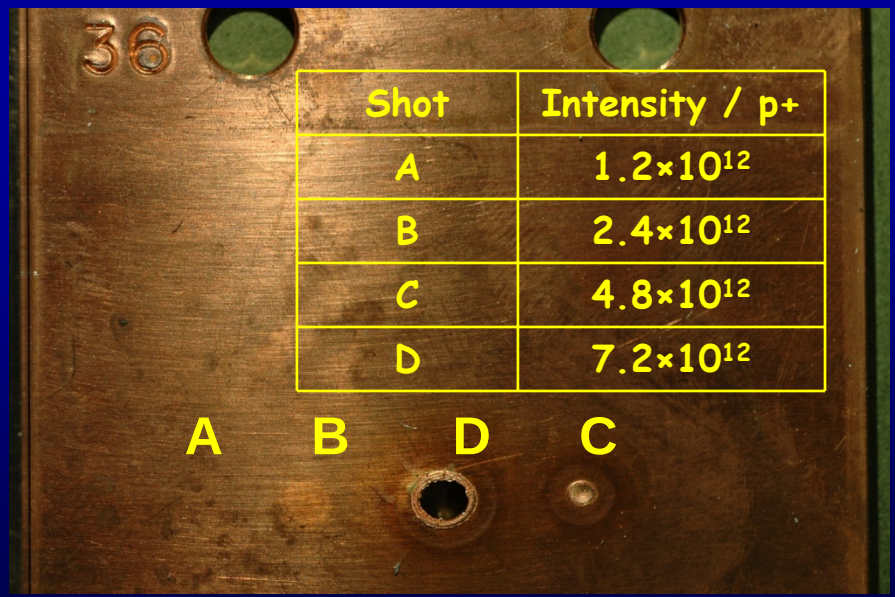
Safe Beam 'Test'

SPS Beam ➡



SPS damage test :

- Validated the simulation at 450 GeV.
- Confident that the interpolation to 7 TeV is reasonable.



Shot	Intensity / p+
A	1.2×10^{12}
B	2.4×10^{12}
C	4.8×10^{12}
D	7.2×10^{12}

Interlock Masking @ LHC

Interlocks at the LHC (and at the SPS) are split into 2 classes:

- Un-maskable channels : always taken into account.
- Maskable channels : mask is deactivated based on a the safe beam flag.

>> Proved to be very convenient and safe for commissioning of the high energy transfer lines (3 km long !) from the SPS to the LHC.

Fast extraction of a full HERA/TEVATRON beam !!

Possible issue : will the simple binary system (safe / not safe) provide enough flexibility / granularity for LHC operation ?

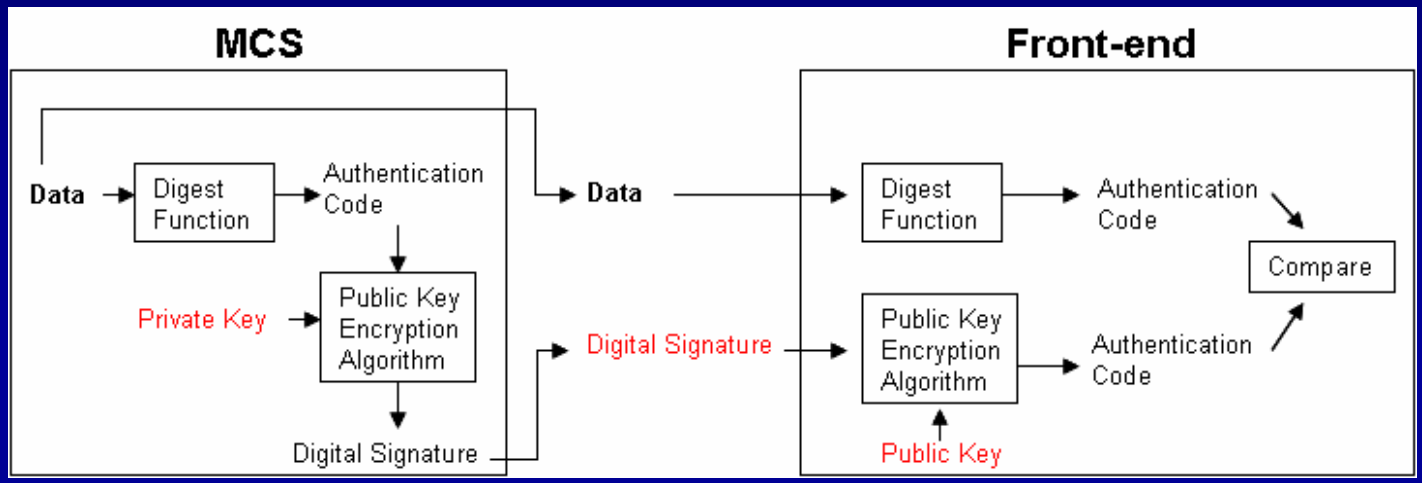
Critical Settings Control

- A Critical Settings Management (MCS) system has been developed for the LHC (and for CERN in general) to be able to control MPS settings through the central controls database without loss of security.

- MCS provides:
  - Critical parameters that can only be changed by an authorized groups of persons.
  - Parameters are visible to everyone that has access to the control system.
  - Authentication and Authorization of the user via RBAC.
  - Verification that values of critical parameters have not changed since the authorized person has updated them:
    - Data transfer errors.
    - 'Hacking'.
    - Data corruption – radiation, data loss during reboots…

Critical Settings Control

Based on the concept of **public** & **private** key.



- User logs in with RBAC that manages the public and private keys.
- The critical data receives a digital signature.
- Data and digital signature are:
  - Send to the front-end system which verifies the data validity.
  - Stored together in the DB - avoid direct DB access, reference for checks.

Monitoring – Software Interlocking

- In very large accelerators it is not always possible to cover all failure mechanisms with a hardware system: needs something more flexible.

  Example : At the LHC the integrated bending field of horizontal steering magnets may bias the beam energy and cause problems during beam aborts.

- Provide flexibility to quickly add new interlocks (provided they are not too time critical).
- Need to survey the integrity of the settings even with a MCS system:

  Comparison of data and digital signatures between front end computers and DB.

>> **Software Interlock System** to survey the control system components relevant for machine protection as additional protection layer, with possibility to abort beam if necessary.

Software Interlocking in Practice

- A large scale software interlock system is in place at the SPS and the SPS-LHC high energy transfer lines:
  - More than 1000 surveyed components or (interlock) settings.
  - High availability, despite the fact that it depends on many control system components!
- The same system is put in place for the LHC.
  - Initially mostly for alarms and injection protection.
  - As appropriate also for beam abort – watch the reliability !!

‘Big brother’ is watching you !

Very effective at the SPS, will play an important role at the LHC.

Testing & Validation

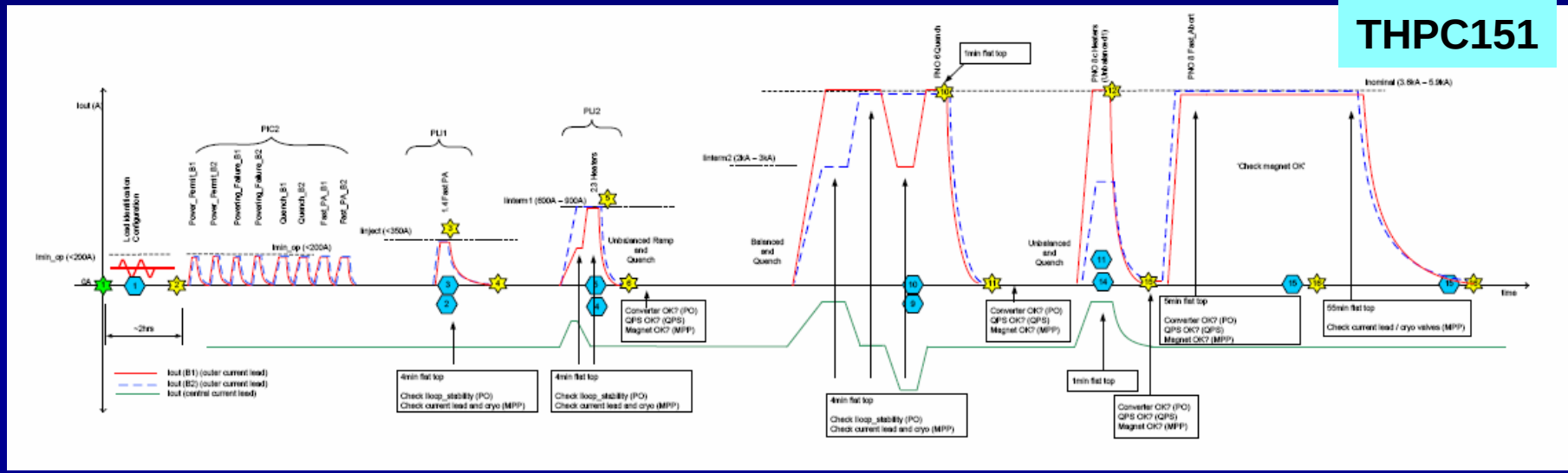
- The size of the MPS and the number of interlocks (many hundreds to thousands of channels) pose a challenge for MPS testing:
  - Tedious and long testing – lengthy (re)commissioning.
  - Risk of mistakes & reduced concentration due to repetitive nature of tests if performed 'manually'.

- (Possible) solutions:
  - Test by 'sampling': only a random selection of channels is tested systematically.
    - Not applicable for super-conducting magnets !
  - Automated testing with 'sequencers' that run pre-defined test procedures:
    - Well adapted to systems with large number of identical tests.
    - Direct logging of the results to file or DB.
    - Gain in time.
    - Test sequences can easily be rerun after interventions etc.
    - Requires careful specification and testing of the sequence.

Test Sequences for LHC Hardware Commissioning

- During LHC HWC, each magnet circuit is following a pre-defined set of current cycles to validate functionality of powering equipment and protection systems.

THPC150
THPC151



- A sequencer is executing the tests and collecting the Post-morten data before sending the data to a database :

  >> absolutely essential for quality and efficiency of the LHC commissioning.

- Similar scheme will be uses for the commissioning of the LHC MPS – to start soon.

Post-Mortem… Lux

- Post-mortem data recording following a beam abort is widely used at colliders and other facilities:
  - Diagnose the cause of beam aborts.
  - Provide data for optimization of operation.

- A good PM system must be carefully designed from the start:
  - Data ‘completeness’ : circular data buffers must be foreseen at an early stage for EVERY system.
  - Accurate time-stamps for correlation to microseconds or better.
  - Coherent trigger signal to freeze data buffers.

- Other facilities (linacs, beam transfer lines) frequently rely on data logging of every ‘shot’:
  - High rep-rate logging.

Post-mortem Data Volumes

Machine	PM Data Volume	Comment
HERA	5 MB	
RHIC	130 MB	
LHC	**2-5 GB**	Estimate !
CNGS (SPS)	0.1 MB/s	‘Shot by shot’
FLASH	5 MB/s	‘Shot by shot’

At the LHC the data volumes will be so large that the data analysis and data presentation (to the operation crews) is essential to make sense out of the PM event !!!

No manual browsing of the data….

Post-operational checks - POCs

S. Wagner THPC145

- At the LHC certain systems are so critical for safe operation that one must ensure that the systems are 'as good as new' before every machine filling.
- The systems use redundancy to achieve very high safety standards, but the redundancy must be verified after every mission (beam dump).
  - Requires a detailed analysis of the PM data for the system. A successful analysis is MANDATORY to resume beam operation.

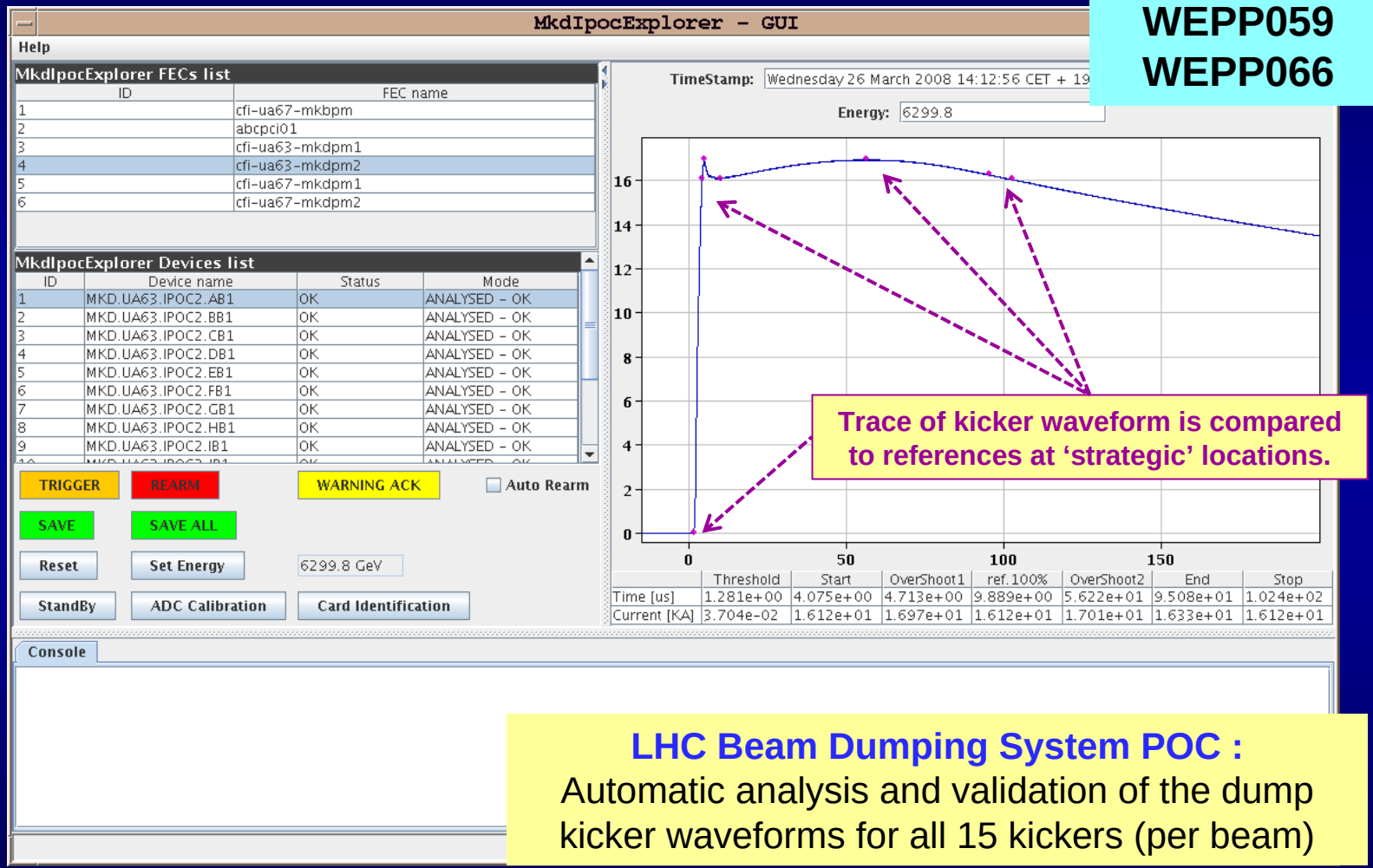
>> Post Operation Check (POC)

Concerned systems:

- After a beam dump : Beam Dumping System, Interlock System.
- Before a run/fill : BLM system.
- Periodically : Quench Protection System.
- List may extend with time and experience…

POC example

J. Uythoven, WEPP059 WEPP066



Trace of kicker waveform is compared to references at 'strategic' locations.

LHC Beam Dumping System POC :
Automatic analysis and validation of the dump kicker waveforms for all 15 kickers (per beam)

Summary

- Controlling access to critical control system devices is essential for high power/stored energy machines.
  - Various access control schemes, up to very sophisticated role-based systems.
  - Digital signatures to protect the authenticity of data.
- Masking interlocks is a delicate topic, yet it can be important for setup and commissioning:
  - Accelerator mode based.
  - For the LHC safe / unsafe beam concept.
- MPS testing can be very time consuming, and well prepared and tested automated sequences are essential to ensure that the systems is properly (re-)commissioned.
- Post-mortem (or logging) data is evolving from ‘nice to have’ to ‘absolutely essential’ for machine safety. PM data is used to ensure that critical systems are ‘as good as new’.