Review of Reliability Concepts Applied to Beam Loss Monitoring Systems

Bernd Dehning

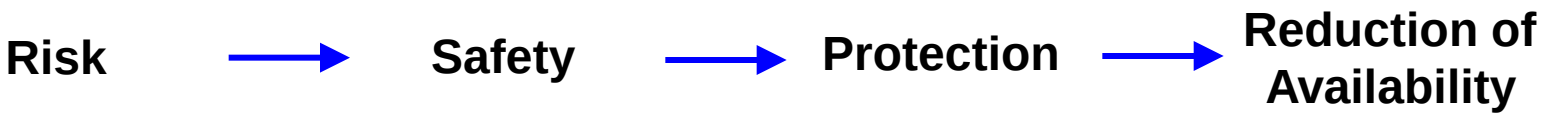
CERN BE/BI

Content

- Risk – Safety – Protection – Availability
- Failure probability and failure rate of systems
- System overview
- Reliability software
- Failsafe system, human errors
- Firmware updates
- Functional tests
- Data path
- Preventive actions

Reliability: Safety System Design Approach

Reliability: Safety System Design Approach



Reliability: Safety System Design Approach

Risk → **Safety** → **Protection** → **Reduction of Availability**

Scaling:

frequency of events
x
consequence

Damage
(system integrity)

Quench
(operational Efficiency)

Reliability: Safety System Design Approach

Risk → **Safety** → **Protection** → **Reduction of Availability**

Scaling:

frequency of events x consequence → Mean time between failures

SIL ALARP

$1\ 10^{-8}$ to $1\ 10^{-7}$ 1/h

Damage (system integrity)

Quench (operational Efficiency)

Failsafe
Redundancy
Survey
Functional Check

Reliability: Safety System Design Approach

Risk → **Safety** → **Protection** → **Reduction of Availability**

Scaling:

frequency of events x consequence → Mean time between failures

SIL ALARP

$1\ 10^{-8}$ to $1\ 10^{-7}$ 1/h

Methods:

Stop of next injection

Extraction of beam

Systems:

Beam loss Monitors

Quench protection system

Interlock system

Dump system

Damage (system integrity)

Quench (operational Efficiency)

Failsafe
Redundancy
Survey
Functional Check

Reliability: Safety System Design Approach

Risk → **Safety** → **Protection** → **Reduction of Availability**

Scaling:

frequency of events x consequence → Mean time between failures

SIL ALARP

$1\ 10^{-8}$ to $1\ 10^{-7}$ 1/h

Methods:

Stop of next injection

Extraction of beam

Reduction of operational efficiency

Damage (system integrity)

Quench (operational Efficiency)

Failsafe
Redundancy
Survey
Functional Check

Systems:

Beam loss Monitors

Quench protection system

Interlock system

Dump system

Solutions:

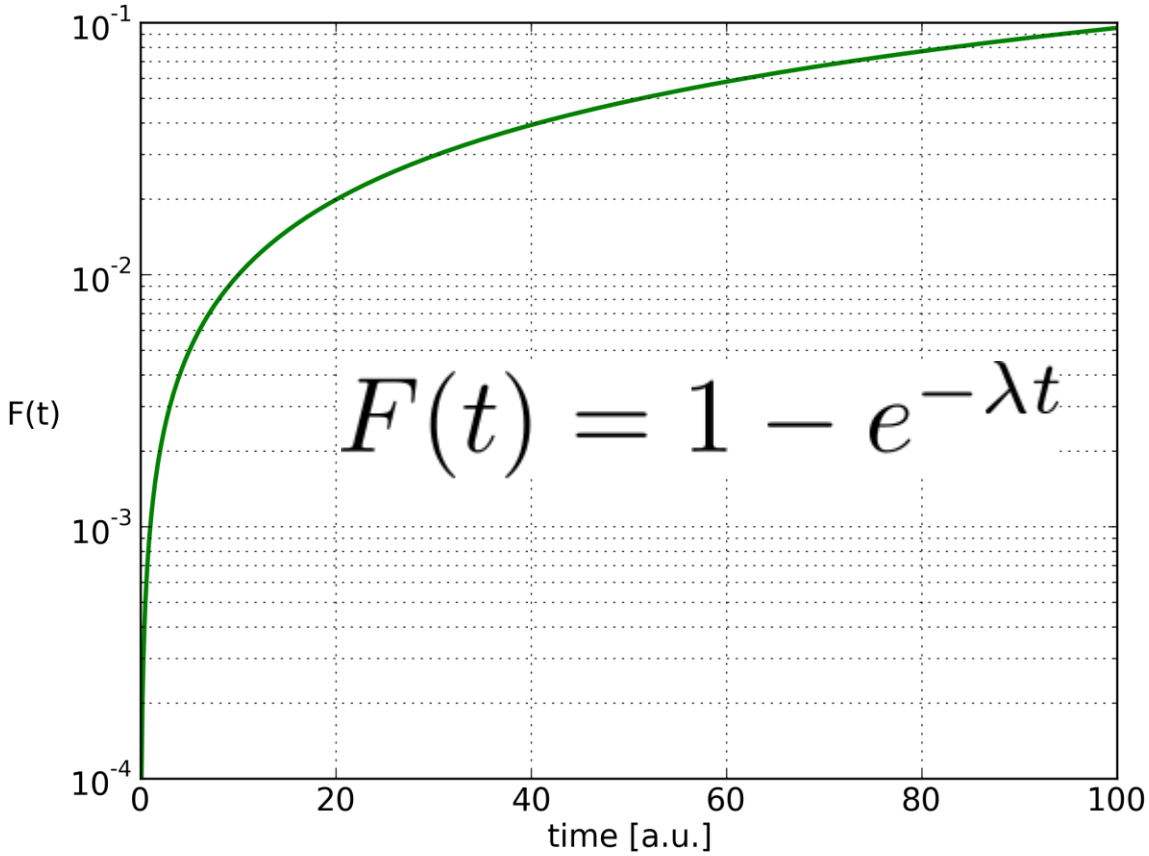
Reliable components

Redundancy voting

Monitoring of drifts

Redundancy - Survey - Functional Check I

F (t) Probability that a failure occurs in the time 0 to t



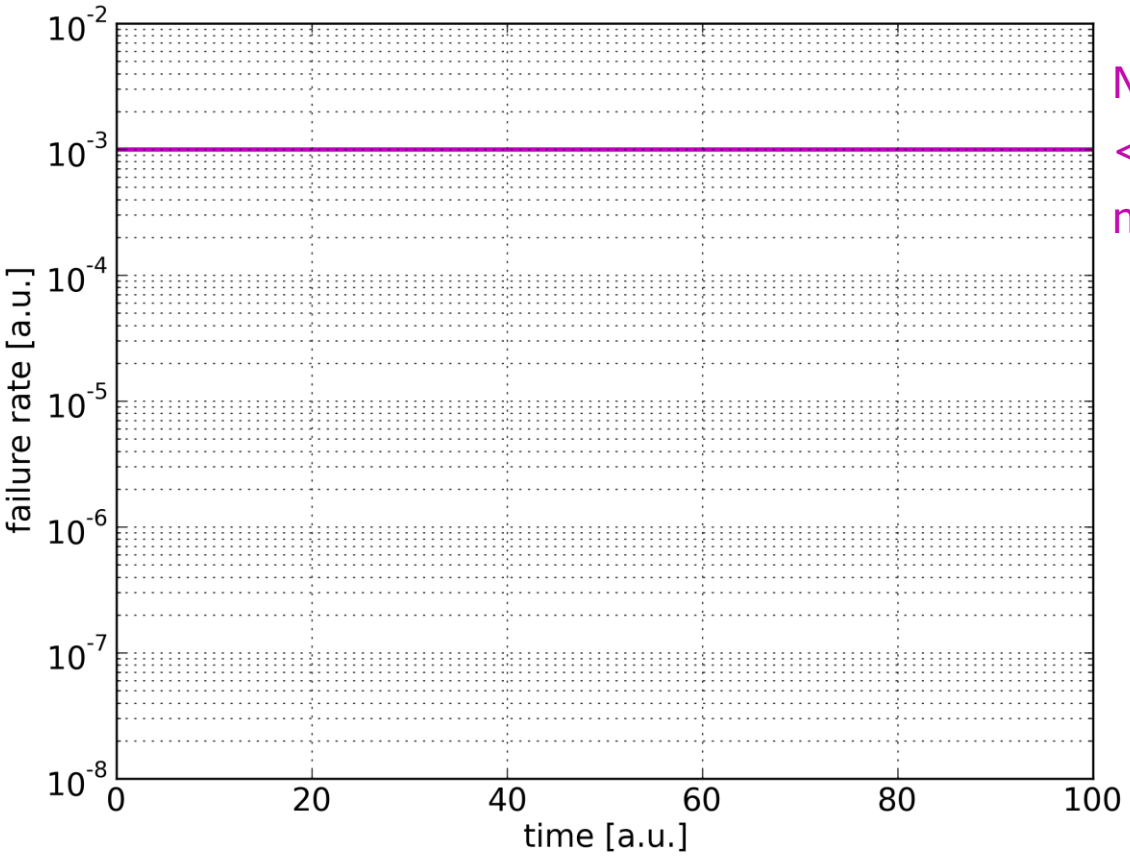
The exponential failure probability leads to a constant failure rate

$$Failurerate = \lambda$$

Redundancy - Survey - Functional Check II

failure rate: Probability that a failure occurs at the time t, given that the system was operating before

Single system



No time dependence

<=>

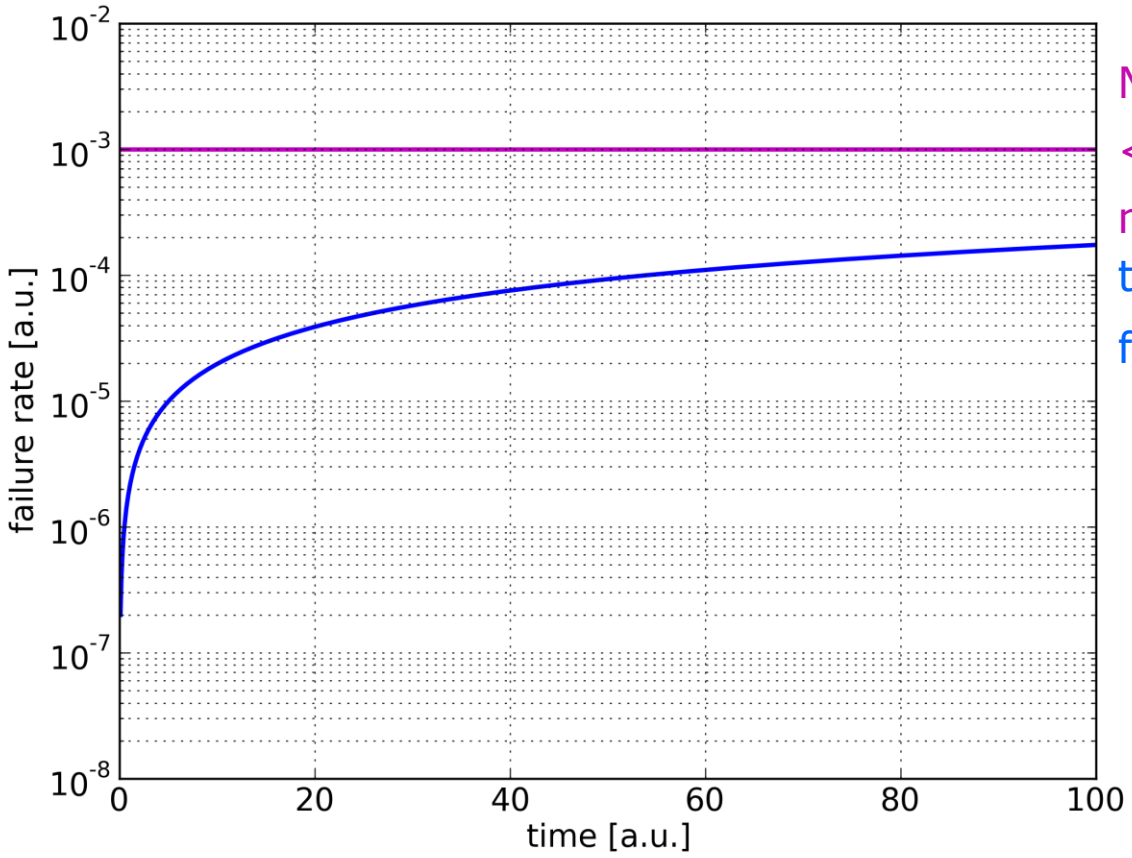
no memory effect

Redundancy - Survey - Functional Check II

failure rate: Probability that a failure occurs at the time t, given that the system was operating before

Single system

Two Systems parallel



No time dependence

<=>

no memory effect

time dependent

failure rate

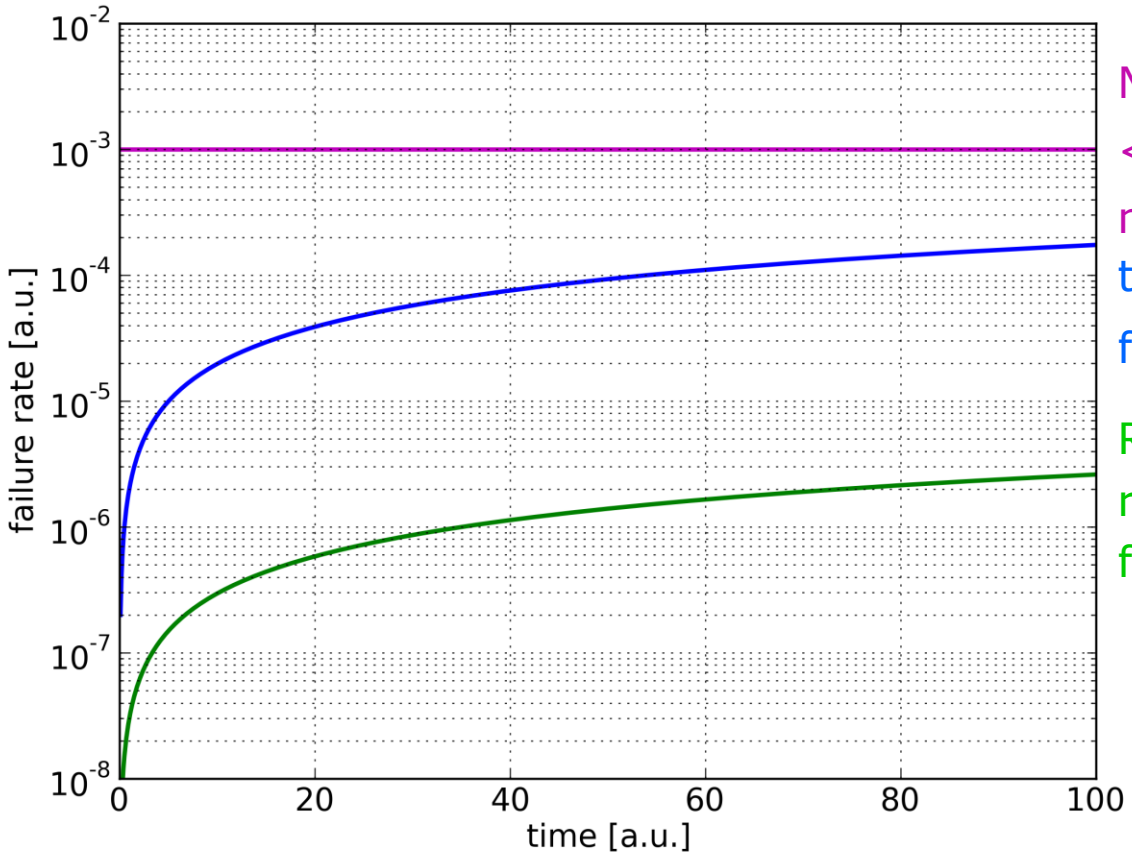
Redundancy - Survey - Functional Check II

failure rate: Probability that a failure occurs at the time t, given that the system was operating before

Single system

Two Systems parallel

Surveyed System



No time dependence

<=>

no memory effect

time dependent

failure rate

Reduction of failure rate by excluding failure modes

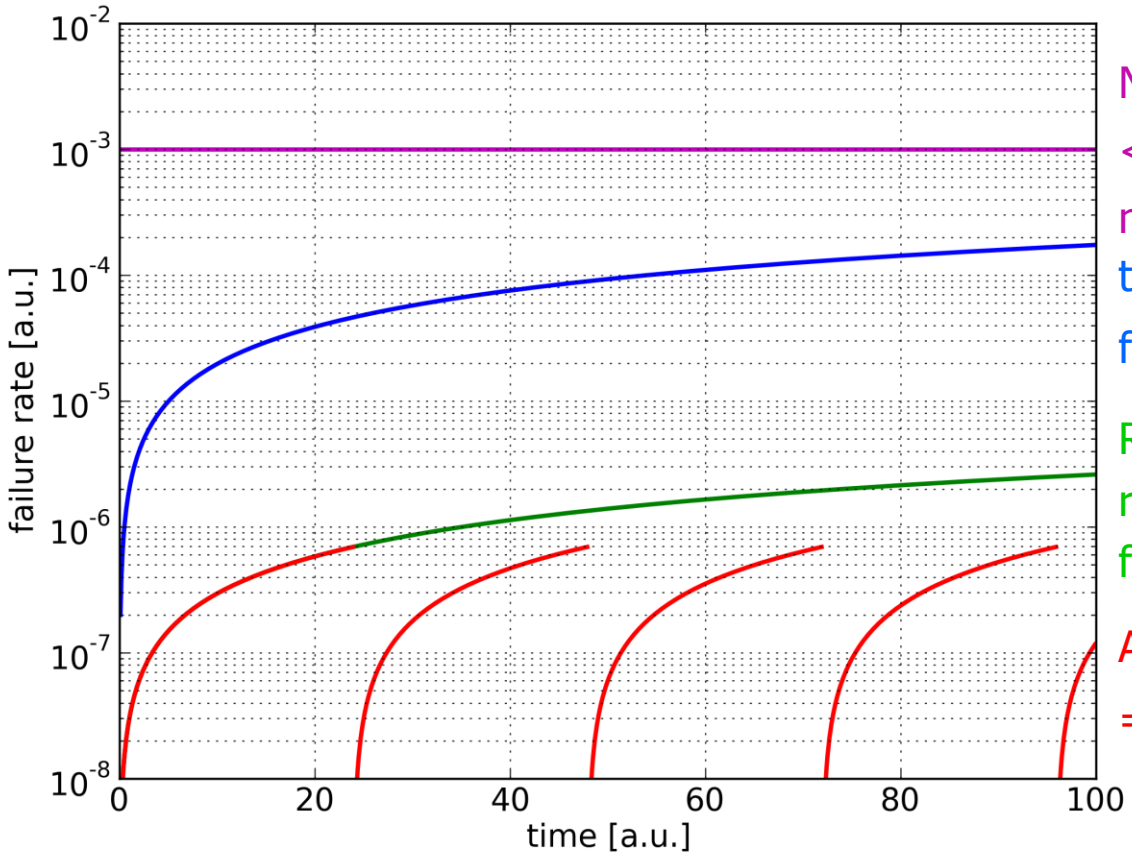
Redundancy - Survey - Functional Check II

failure rate: Probability that a failure occurs at the time t, given that the system was operating before

Single system

Two Systems parallel

Surveyed System



No time dependence

<=>

no memory effect

time dependent

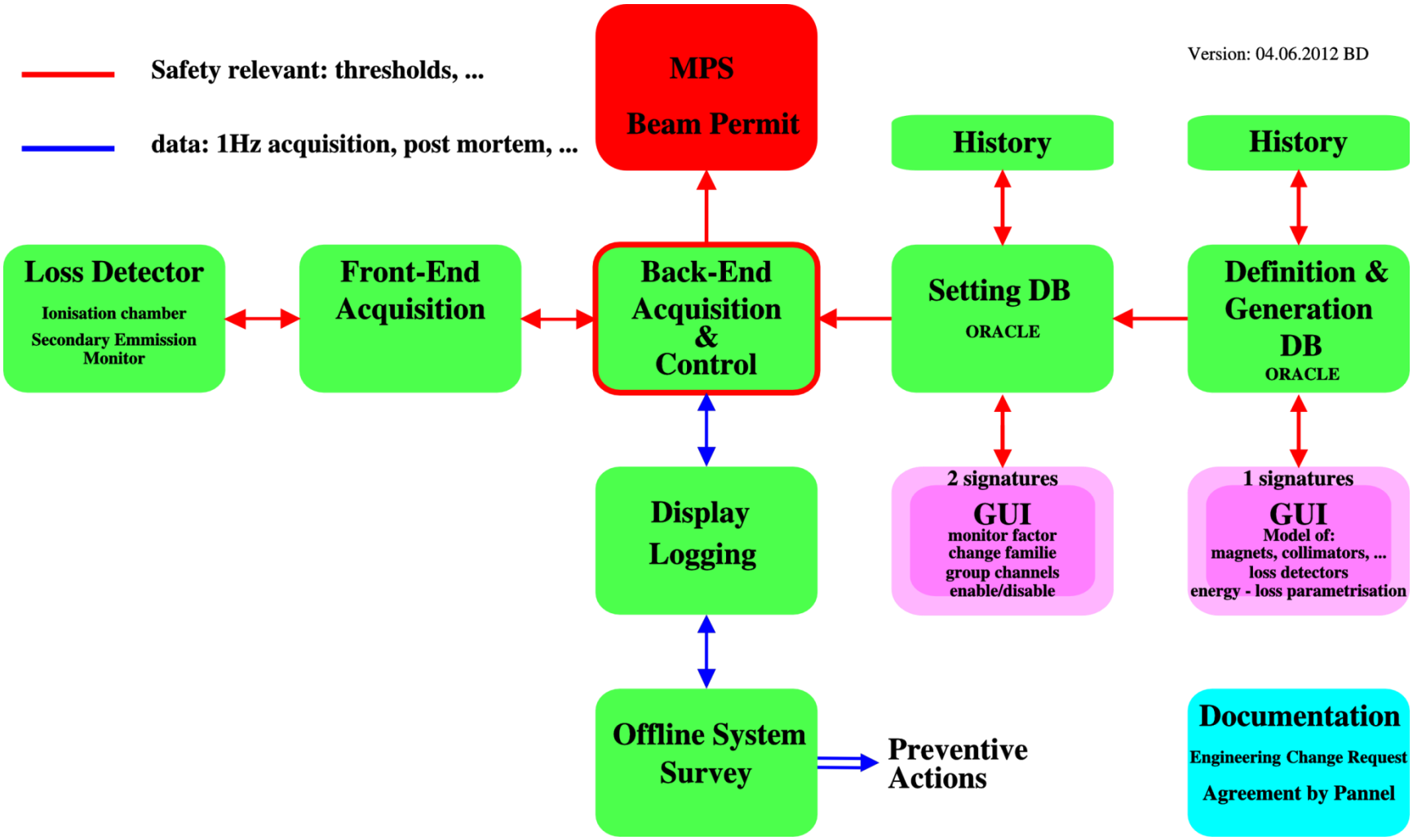
failure rate

Reduction of failure rate by excluding failure modes

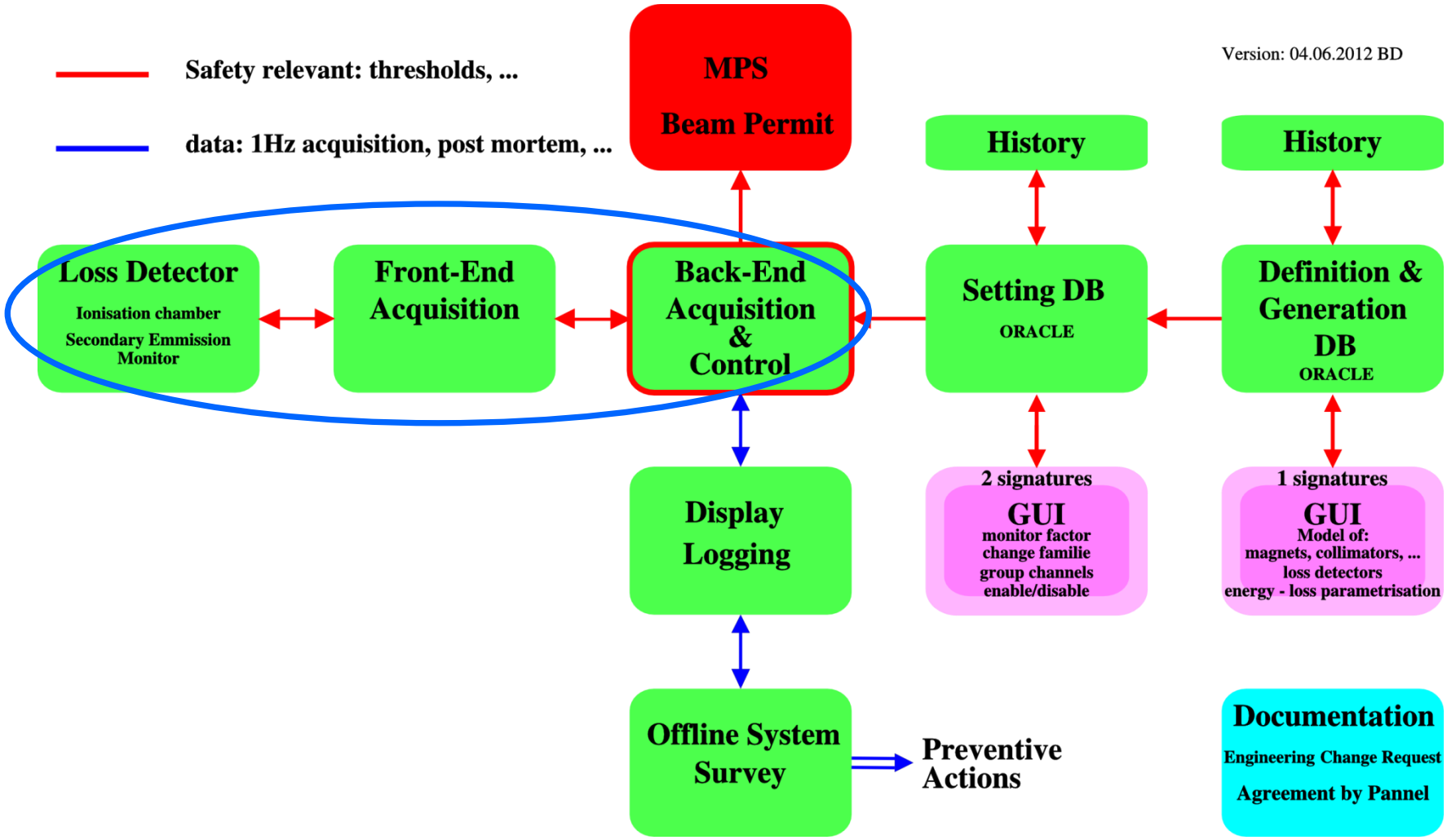
After **functional** test

=> **System new**

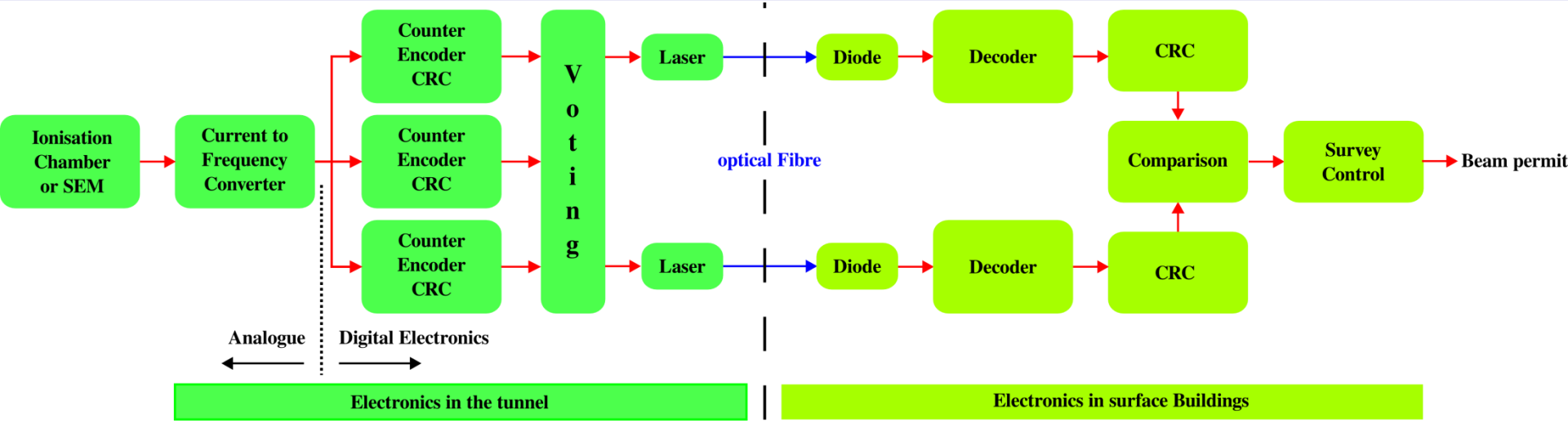
BLM System Information Flow

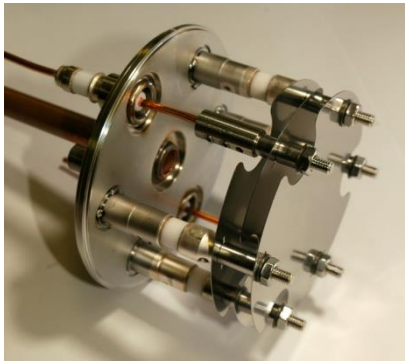


BLM System Information Flow



Beam Loss Measurement System Layouts



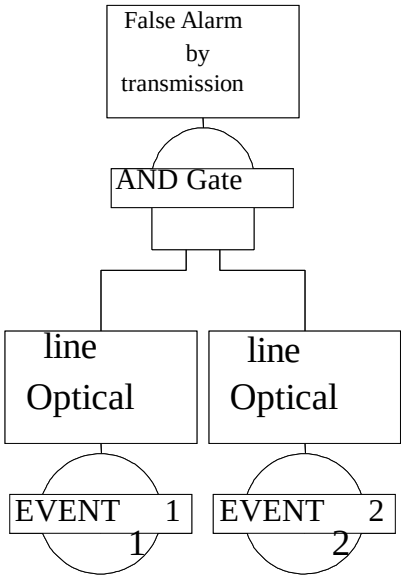


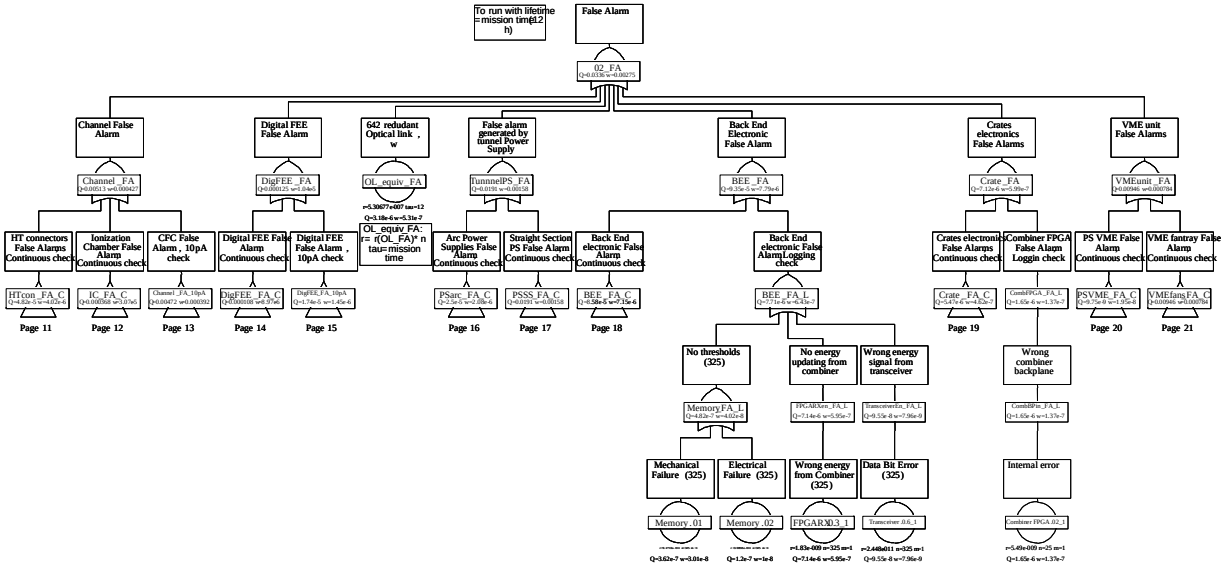
- Ionisation chamber
  - Function: observation and beam permit
  - 3700 installed
  - Over 90 % connected to MPS/dump system
- Secondary emission detector
  - Function: observation
  - 300 installed

	comment	Safety gain	Availably gain
Failsafe	active state = beam permit	yes	no
Voting		yes	yes
Redundancy		yes	yes
CRC	Cyclic redundancy check	yes	no

Reliability: Fault Tree Analysis

- Definitions of failure modes (LHC 160)
- Three end effects:
  - Damage risk: probability not to be ready in case of dangerous loss
  - False alarm: probability to generate a false alarm
  - Warning: probability generating a maintenance request due to a failure of a redundant component
- Probability of a failure mode is calculated given the failure rate, repair rate and the inspection rate





Used program: Isograph, includes component catalogue

Comparison of Reliability Tools

Tool	Pros	Cons
Spreadsheet	Previously used by SNS, good source of data	Interface difficult to use, lack of visualization, error prone
AvailSim (free)	Previously used for ILC, many accelerator specific concepts	No GUI
Sapphire (semi-commercial)	Widely used by NASA and nuclear industries, developed by Idaho National Lab	Newest version (8) only US government organizations
ReliaSoft (commercial)	Good GUI, widely used, SNS uses it	File format is proprietary
Isograph (commercial)	Good GUI, open file format	Lacks some GUI features

Lit: S. Bhattacharyya, IPAC12

Steps taken for a Failsafe System: Error-free Communication

The steps taken to ensure a reliable communication link:

- Double (redundant) optical link
- CRC-32 error check algorithm
  - All single-bit errors.
  - All double-bit errors.
  - Any odd number of errors.
  - Any burst error with a length less than the length of CRC.
  - For longer bursts $Pr = 1.16415*10^{-10}$ probability of undetected error.
    - 224 bits of data plus 32 bits of CRC remainder = 256 bits
- 8b/10b encoding
  - Clock data recovery (CDR) - guarantees transition density.
  - DC-balanced serial stream - ones and zeros are equal/DC is zero.
  - Error detection – four times more characters.
  - Special characters used for control – sync, frame.
    - 256 bits of data are encoded in 320 bits = 64 extra bits

To avoid misplacement of electronic cards or threshold and masking tables

- Tunnel Card ID
  - Unique number embedded in the FPGA (16bit)
  - Included in every transmitted frame
  - Compared with the one stored in settings DB
- Surface Card Serial number
  - Unique number embedded in a IC (64bit)
  - Compared with the one stored in setting DB

Steps taken for a Failsafe System: System Failures

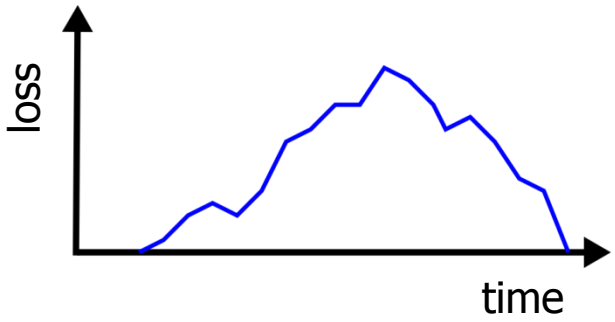
To avoid loss of data

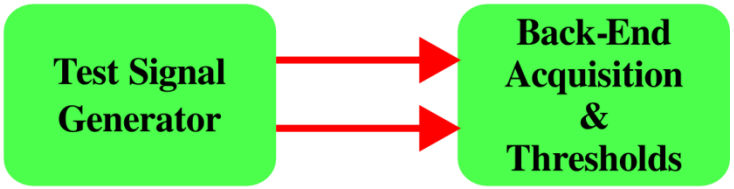
- Frame ID
  - Surface FPGA checks for missing frames
  - Incrementing number included at every transmission
- Optical link is always active
  - 8b/10b encoding sends "commas" when no data
  - Disconnection is detected in max 25ns

To ensure recognition of system failures and beam dump requests

- FPGA Outputs (Beam Dump signals) as frequency
  - At a dump request, reset, or failure the transmitted frequency will be altered
- Beam Permit lines are daisy-chained between cards
  - Custom VME backplane
  - Dummy cards on empty slots to close circuit

Verification using Emulator Module

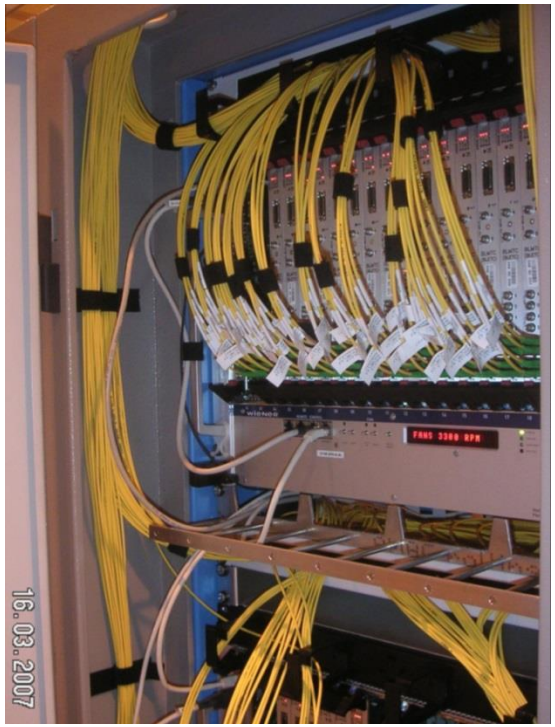




- In situ test of the TC in VME crate by emulation of output signals of CFC
  - Arbitrary Tx data
    - Comparison of different firmware versions
    - Playback of measured data for analysis
  - Tx errors
    - CRC, CID, FID
  - Wrong configuration
  - Errors in physical layer
  - Manual testing procedure
  - Results read out in Expert application

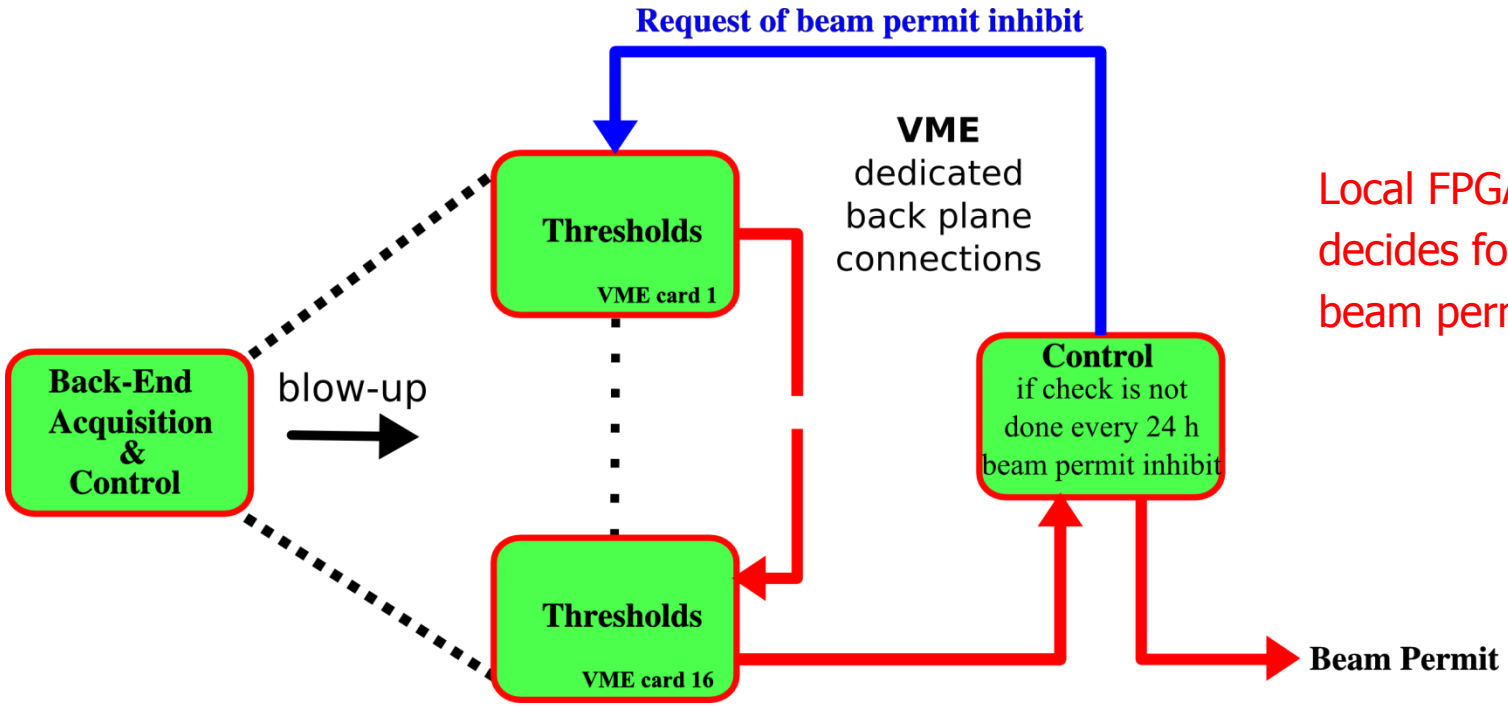
Verification of FPGA Functionality

- Exhaustive verification of the behavior of the Threshold Comparator block in FPGA
  - Check all permutations and their ability to trigger a beam dump request
  - Flash modified threshold table to FPGA targeting one table field at each iteration.
    - 16 cards/crate
    - 16 detectors/TC card
    - 12 integration windows/detector
    - 32 beam energy levels
    - 98'304 test cases/crate
- VME readout check
  - The same test case repeated 500'000 times
- Automatic procedure should ensure that beam permit inhibit could be issued by every channel and for every threshold



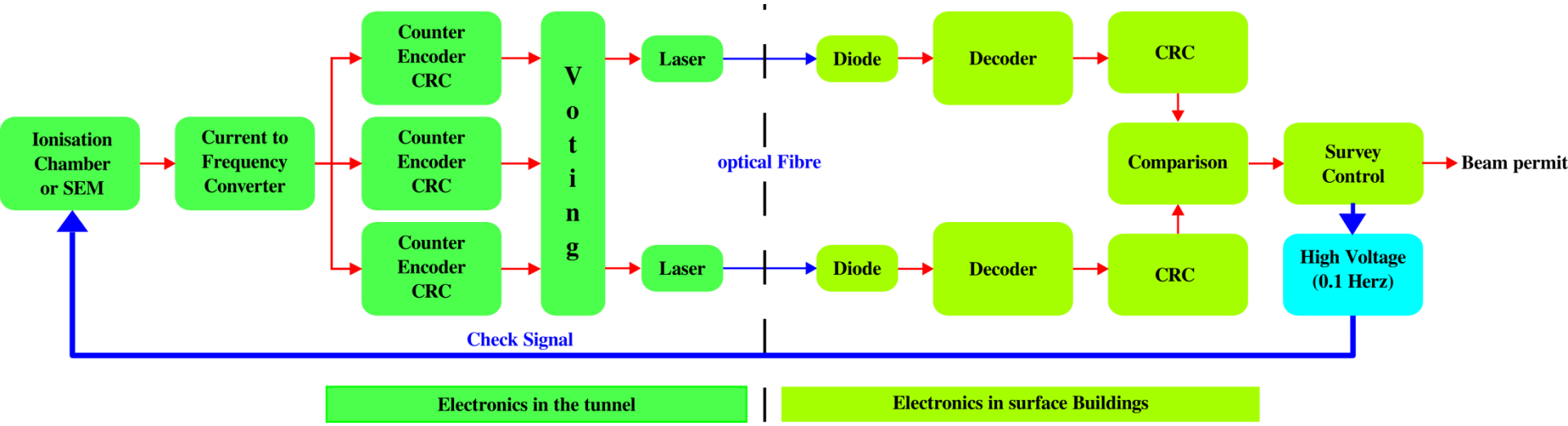
Beam Permit Line Checks

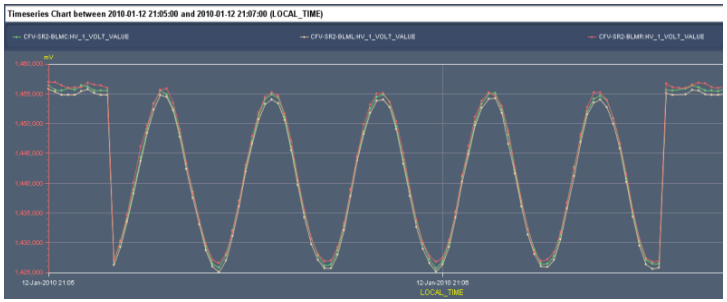
- Check the beam permit lines inside and between crates
- Check results are saved in the database
- Exhaustive test yearly for every threshold (beam energy and integration time dependent)

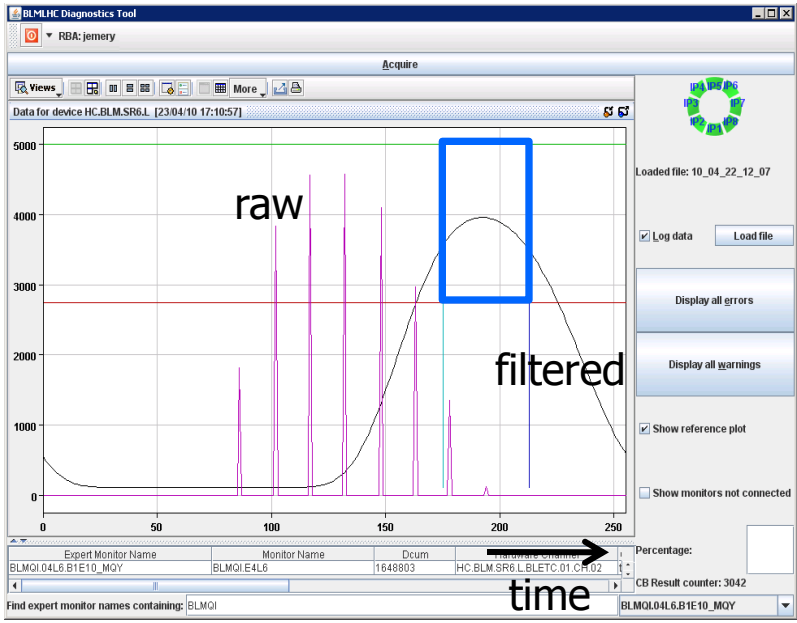


Local FPGA on VME card decides for all checks if beam permit is given

Check of Acquisition Chain (Modulation of HV)



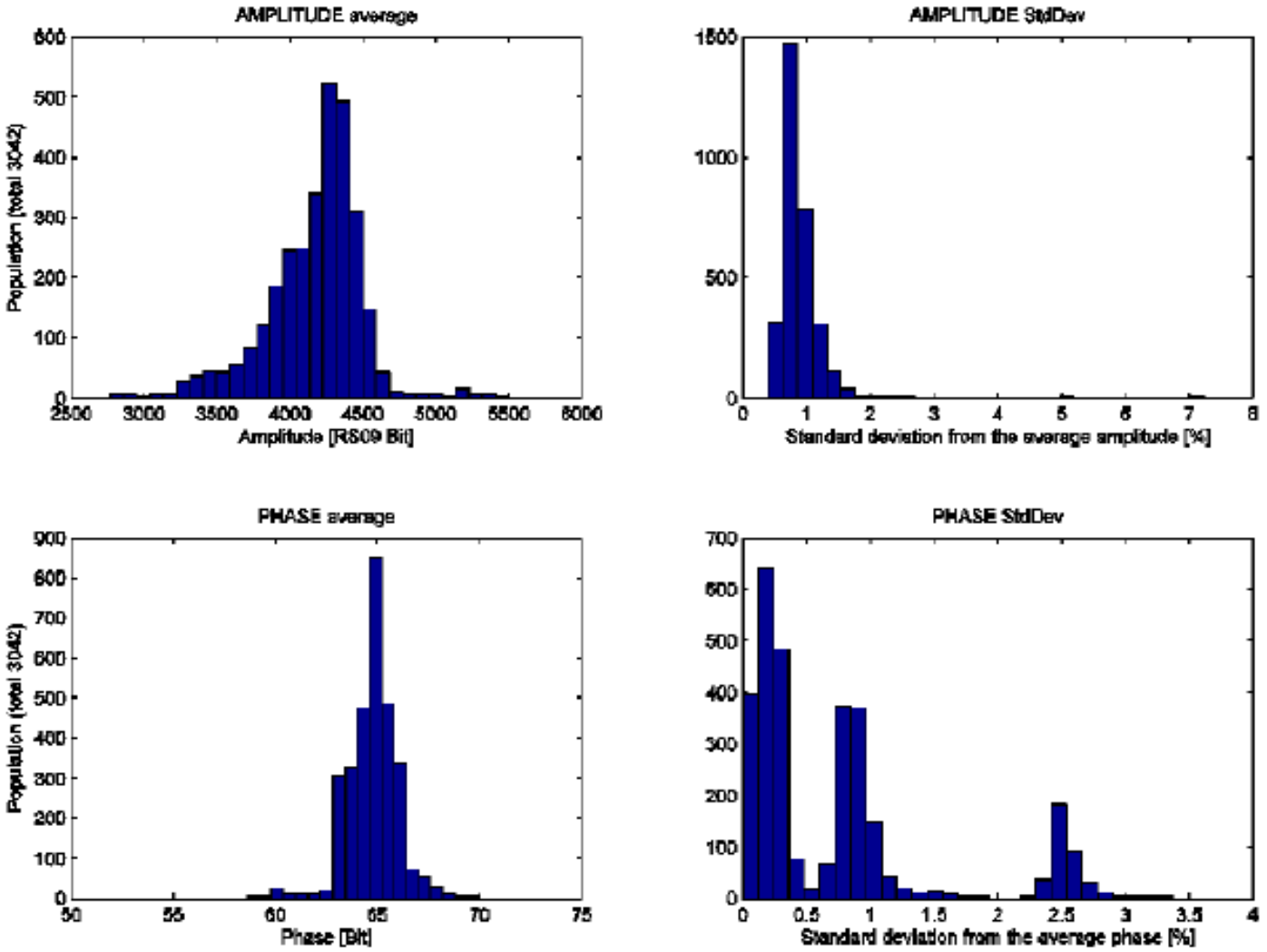




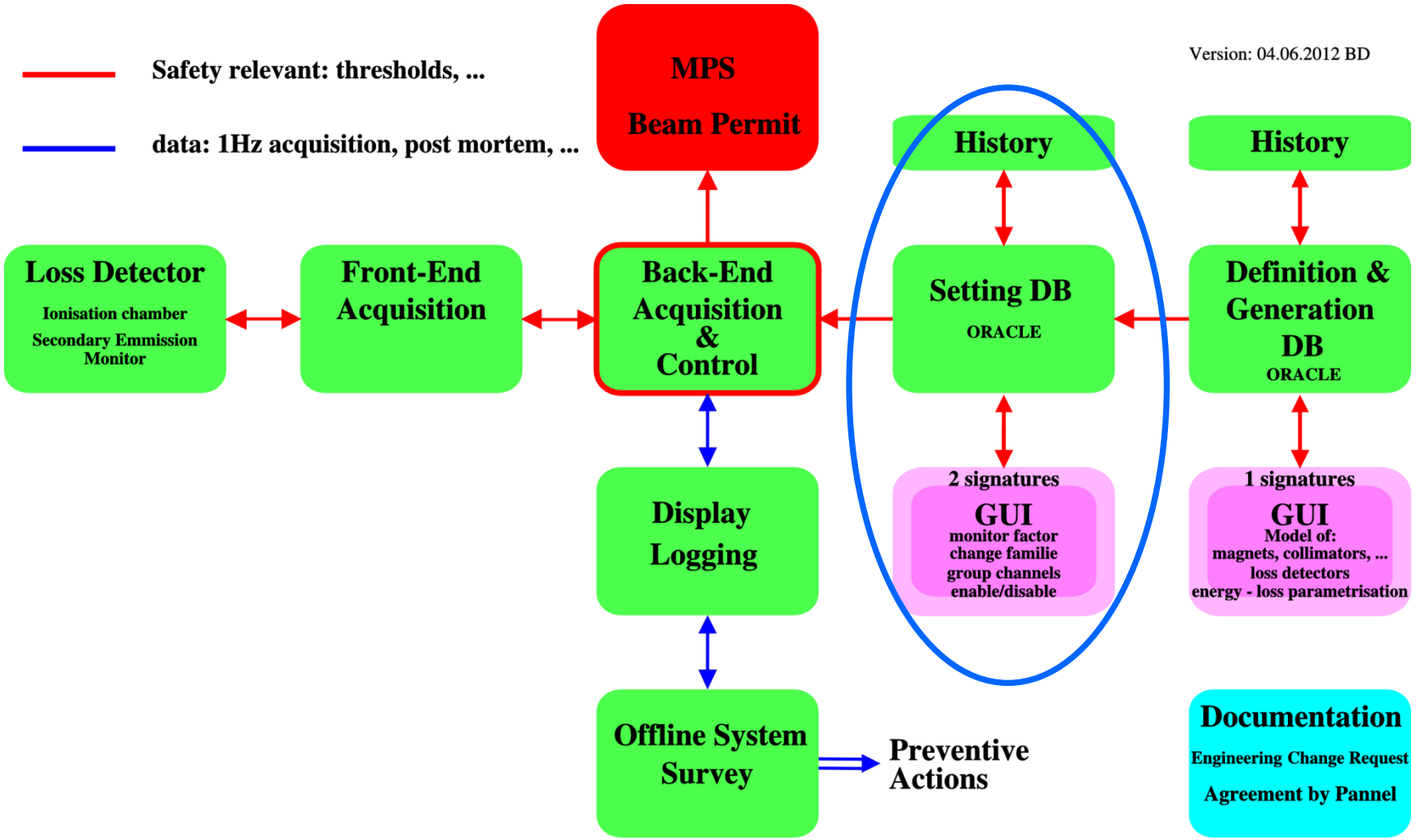
- Phase and amplitude are compared with thresholds
- Beam permit not given if not done every 24 h
- Local FPGA on VME card decides for all checks if beam permit is given

High Voltage Modulation Results

Connectivity check measurements (100x) on BLMQI monitors (Ionization chambers in the arcs)

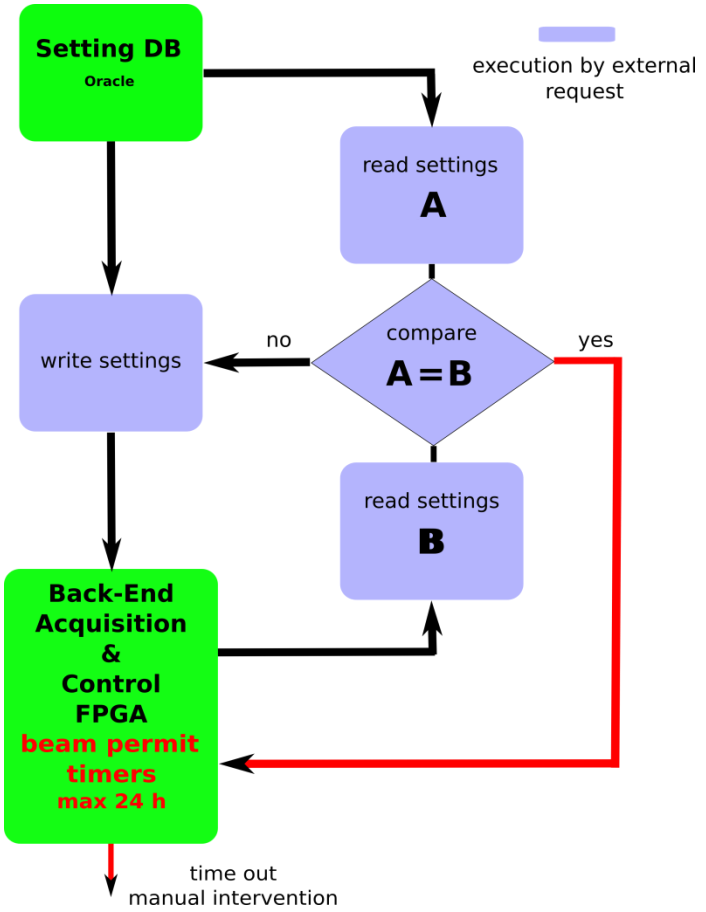


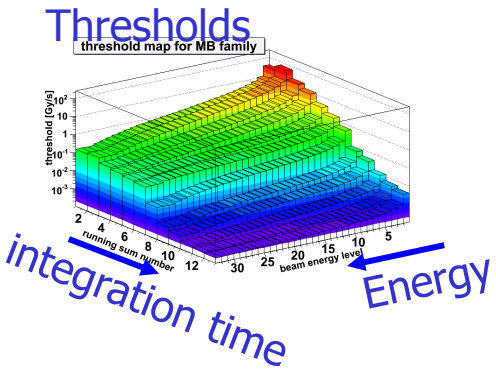
BLM System Information Flow



Reliability: Comparison of Back-End Settings with Database

Corruption in frontend are more likely as in reference database, therefore =>

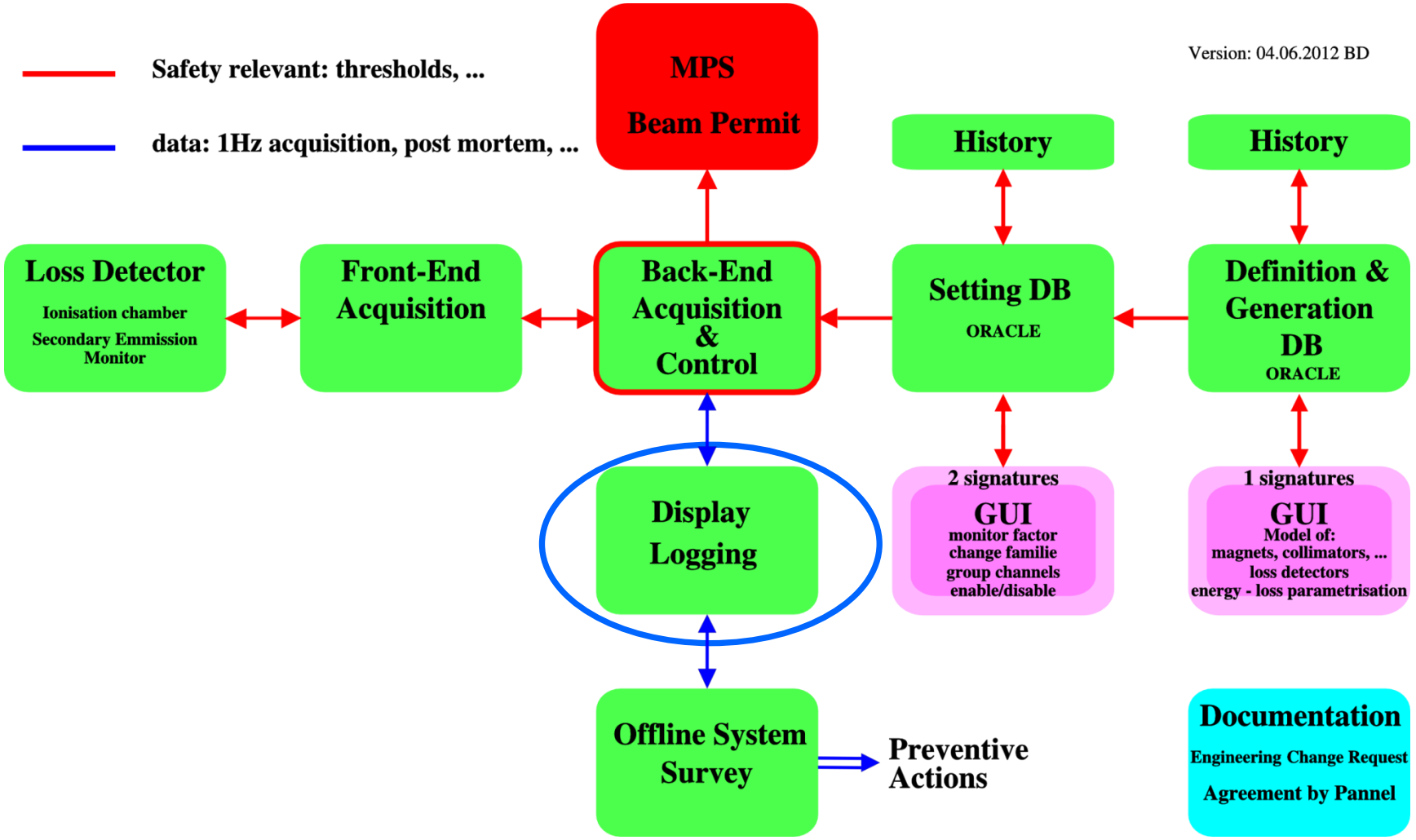




- Setting storage in Oracle database
- Settings:
  - Threshold values
  - Voltages, currents, phase limits
  - Serial numbers
  - Software version numbers
- If comparison negative and after retry, manual intervention (no beam permit)

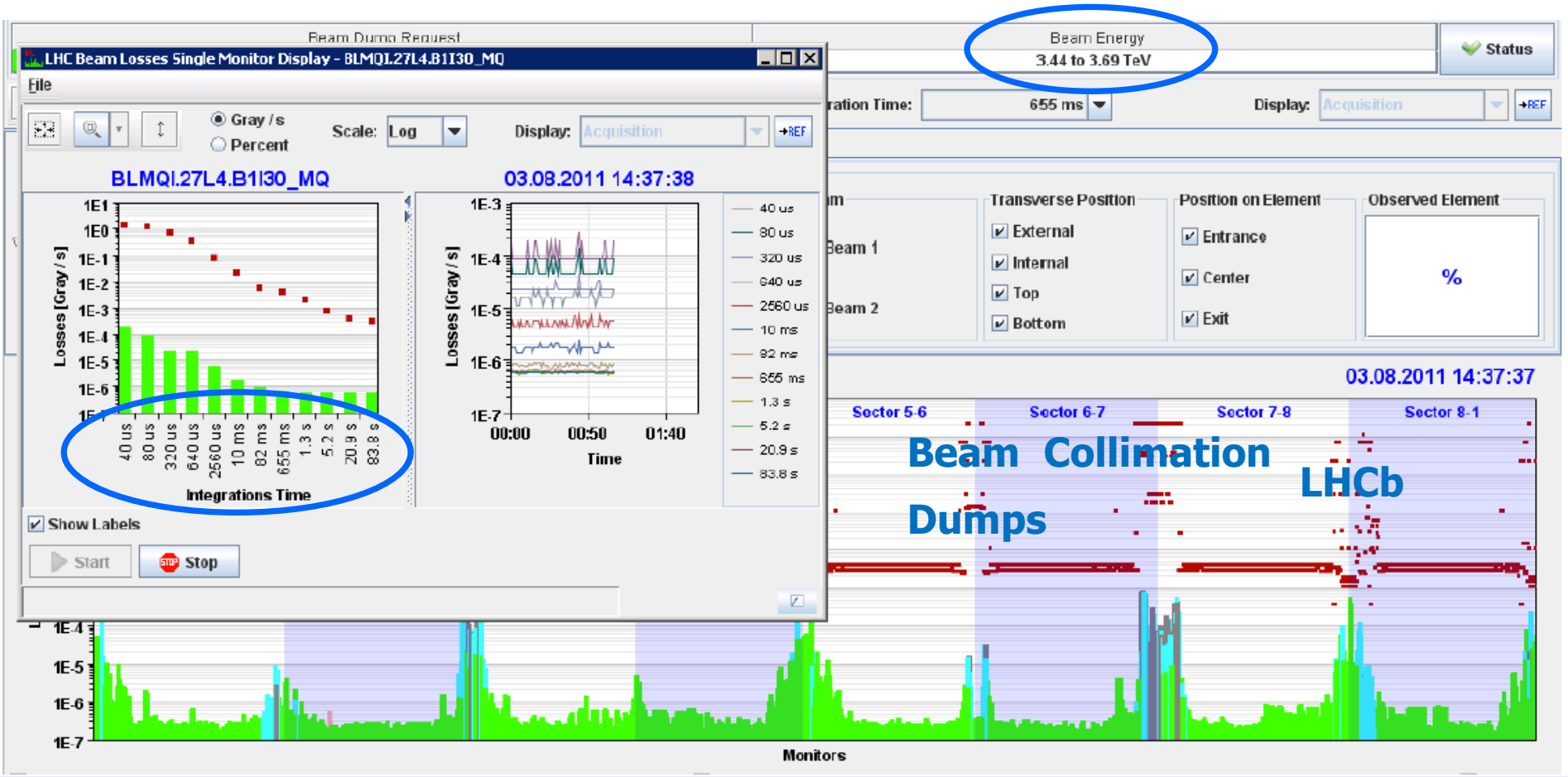
Request for comparison issued by Back-End Acquisition (counter), most reliable (no software layers in between)

BLM System Information Flow



BLM System – Online Display

- Extensively used for operation verification and machine tuning
- 1 Hz update and logging (12 integration times, 40 us to 83 s)
  - Integration times < 1s: maximum during the last second
    - short losses are recorded and loss duration can be reconstructed (20% accuracy

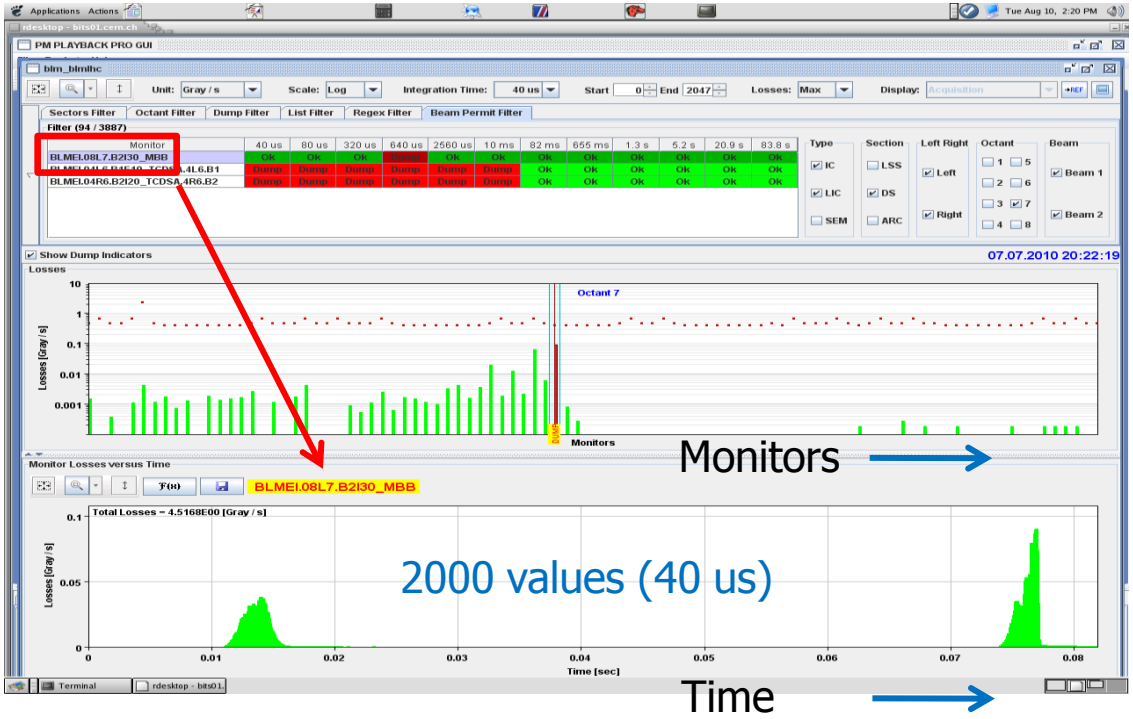


Post Mortem Data (some examples)

Loss in a bending magnet

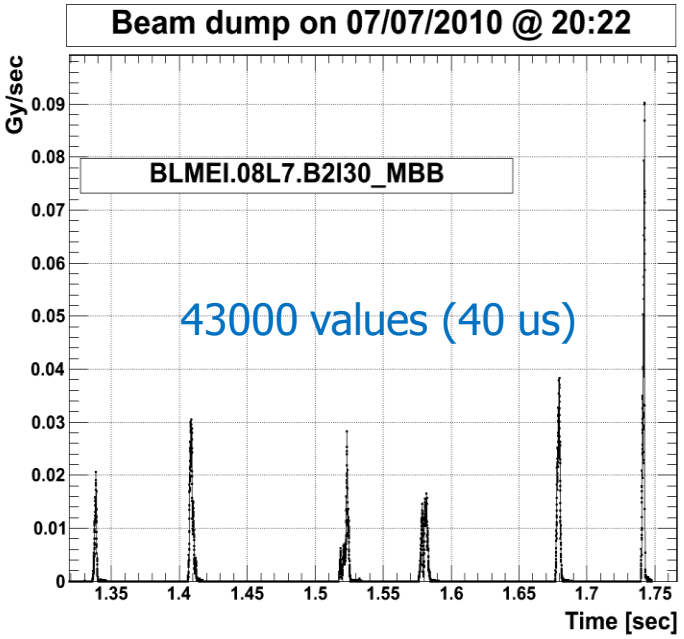
PM application: BLM data of 0.082 sec

online available

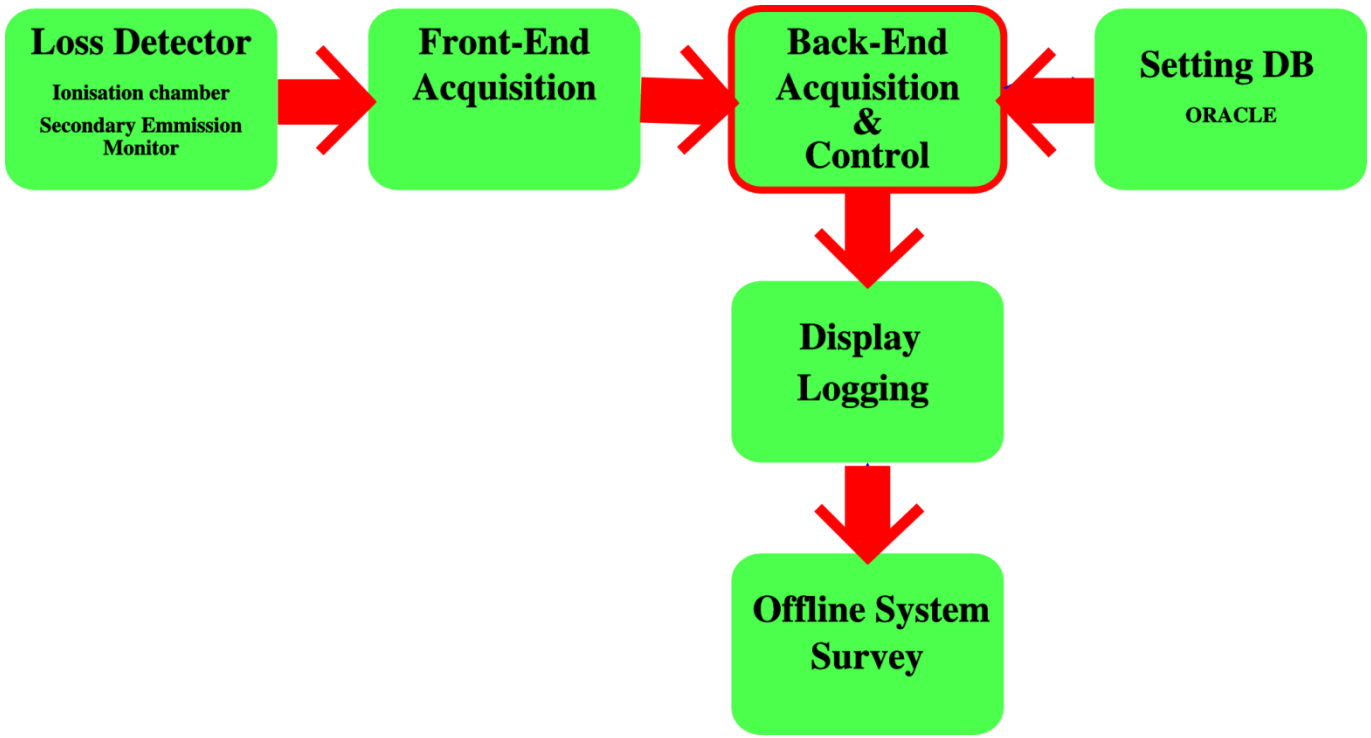


Longer PM buffer: BLM data of 1.72 sec

offine available



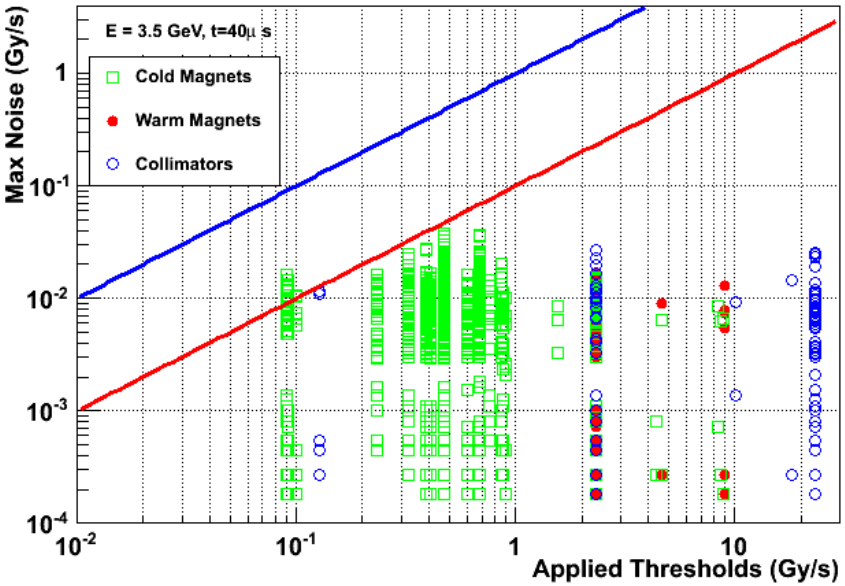
Combined Flow of Measurements and Settings

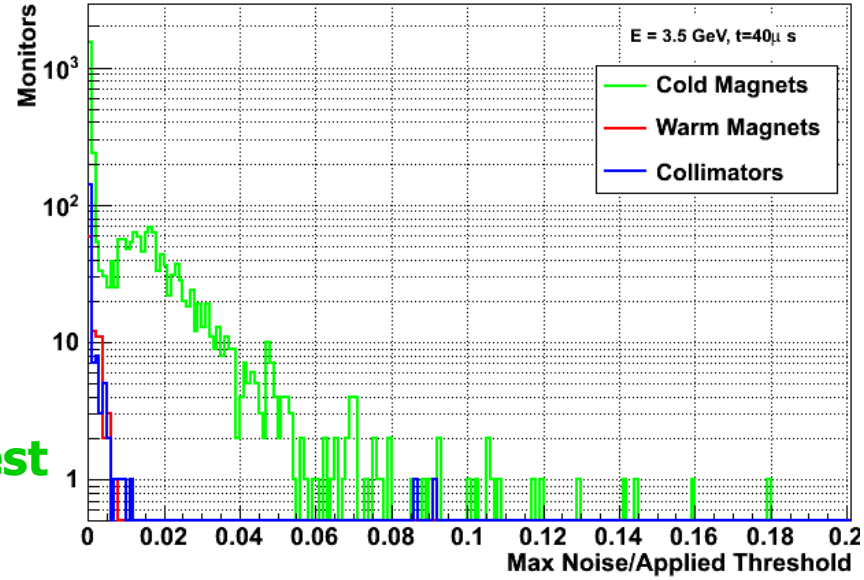


- Measurements and settings (thresholds, monitor names, …) are combined in VME crate (Back-End Acquisition & Control)
- Data flow path identical for both
- Display and logged data are coherent

Noise and Fast Database Access

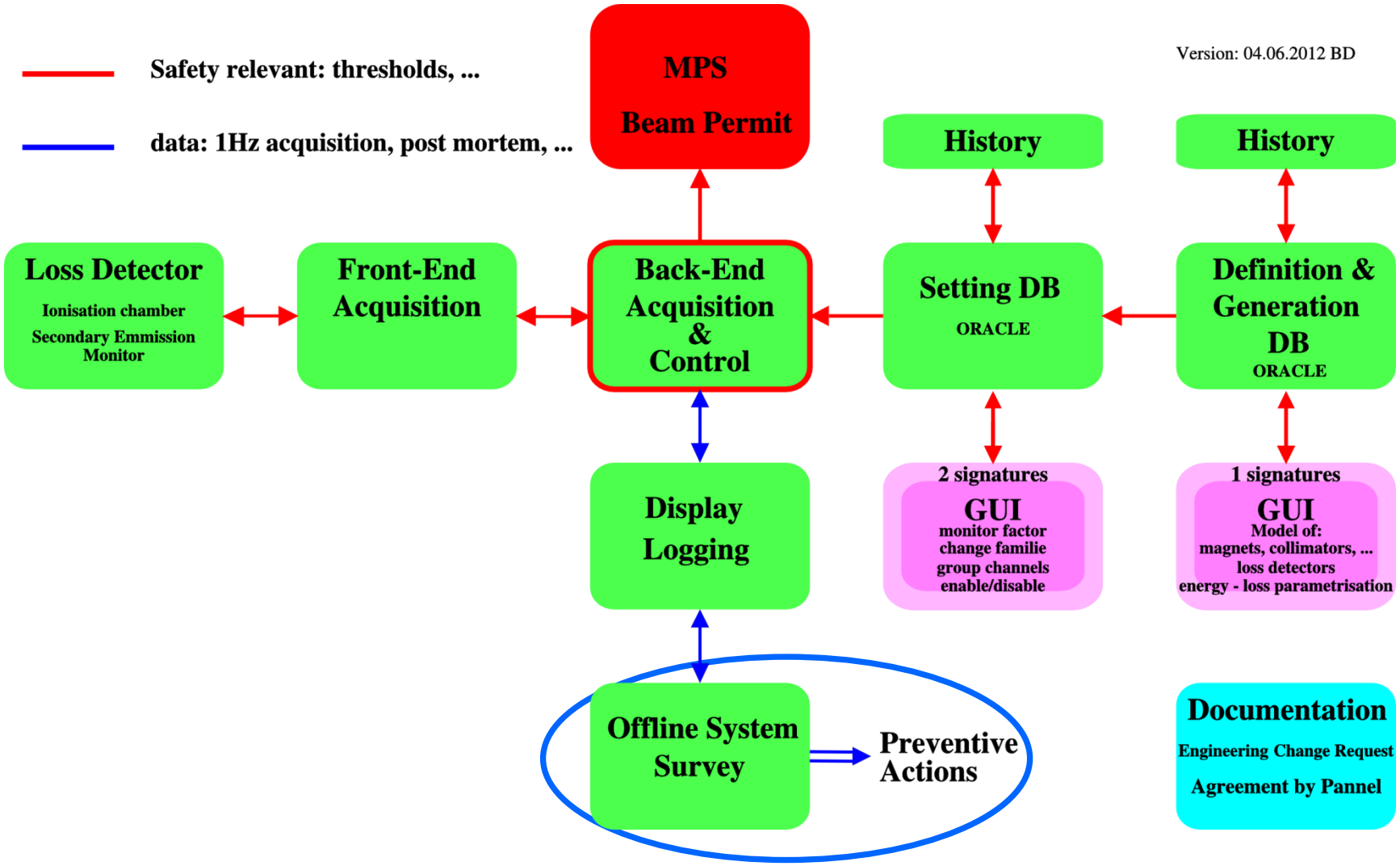
- Important for availability (false dumps) and dynamic range
- Main source of noise: long cables (up to 800 m in straight section)
- Aim: factor 10 between noise and threshold
- Thresholds decrease with increasing energy
- noise reduction before 7 TeV operation
  - Single pair shielded cables, noise reduction: > factor 5
  - **Development of kGy radiation hard readout to avoid long cables**





Noise estimate in design phase with test installations at comparable locations

BLM System Information Flow



Daily Checks

If >=10 errors/link within 24h, send warning and start monitoring this link in more detail

Cases:

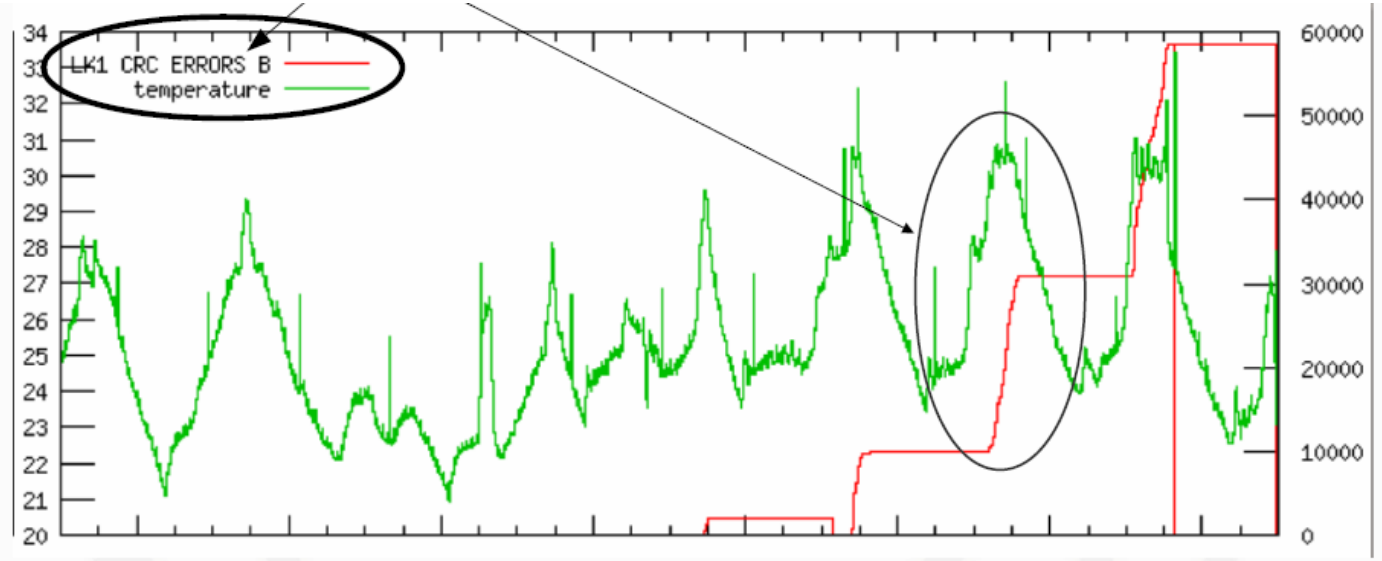
a) constantly low error rate

b) increasing error rate: critical, take action!

Daily Optical Link Check Results — from 2011-05-08 12:00:00 to 2011-05-09 12:00:00 (local time)

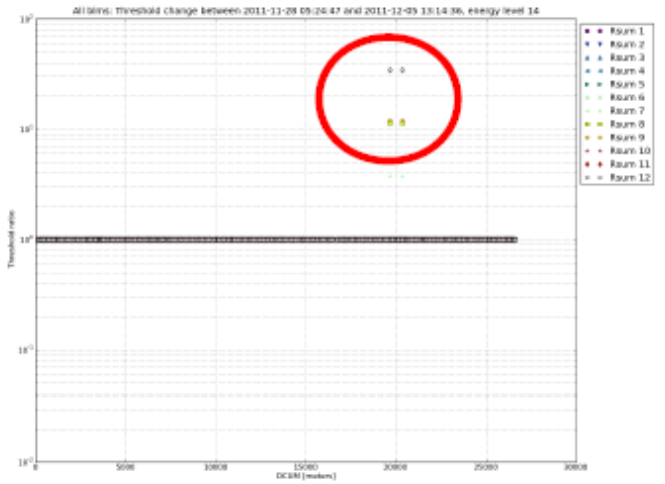
Card	Card-Serial numbers: BLECF Serial	BLETC Serial	BLECS Serial	CRC COMP A	CRC COMP B	LK1 ERRORS A	LK1 ERRORS B	LK2 ERRORS A	LK2 ERRORS B	LK1 LOST A	LK1 LOST B	LK2 LOST A	LK2 LOST B	FID COMP A	FID COMP B
SR1-L 12	0282 0241	9511602473975246337	12177733450726613761	71	0	71	0	0	0	0	0	0	0	0	0
SX4-R 14	0040 0230	857485375148303795 3	11096869540207459585	224	0	225	0	0	0	0	0	0	0	0	0
SR7-L 14	0580 0426	10952754354734524417	16429131499061498881	18	0	18	0	0	0	0	0	0	0	0	0
SR8-C 12	0278 0267	4899916455551403009	4755801264793850881	0	571	0	27762	0	0	0	999999	0	0	0	1

Temperature and failure rate

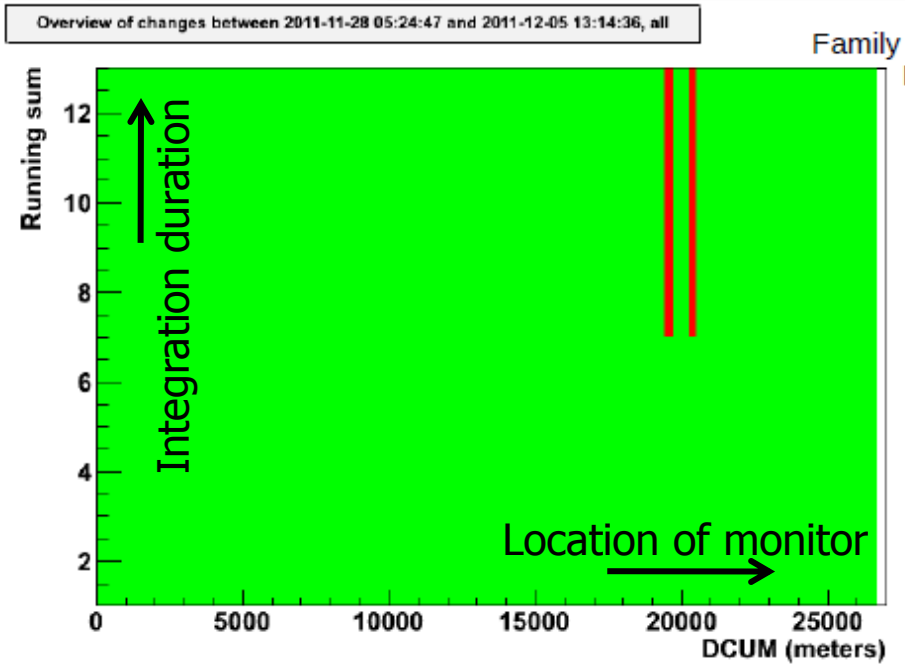


Survey of BLM thresholds

Purpose:
- Detect unwanted/unknown changes
- Detect changes done by EICs



Example of weekly report:



Family THRI.DS.B1.1_MQ:
BLMQI.09R7.B1E10_MQ, crate CFV-SR7-BLMR, dcum 20335:
Change between 2011-11-28 05:24:47 and 2011-12-05 13:14:36:
Energy level 14:
Running sums [7] changed with ratio 3.75
Running sums [8] changed with ratio 11.3527
Running sums [9] changed with ratio 12.0038
Running sums [10, 11, 12] changed with ratio 34.6335

Detailed Analysis of Modulation Result – Preventive Action

Example: Connectivity Check – Results from Shape Analysis

from 2010-10-21 00:00 to 2010-10-22 00:00

Expert Name	Hardware Channel	Cable conn.	BIS conn.	$\frac{\chi^2}{NDF}$	Gain min	Gain meas.	Gain max	Phase min	Phase meas.	Phase max
BLMQI.04R6.B1E10_MQY	6.R.01.02	True	True	73	2628	3772	4880	46	66	84
BLMQI.18R6.B2I30_MQ	6.R.07.01	True	True	87	2823	3973	5241	45	63	81
BLMQI.18R6.B1E10_MQ	6.R.07.02	True	True	92	2881	4052	5351	45	63	81

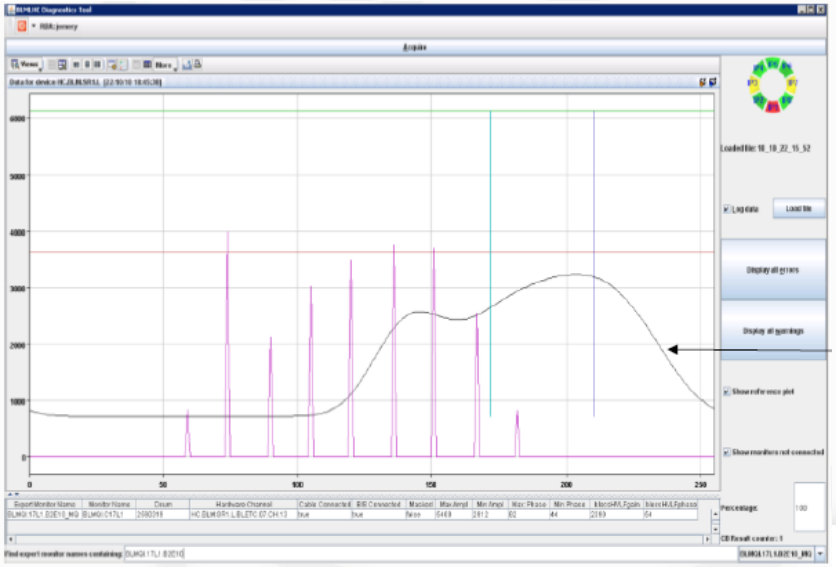
Connectivity check on 2010-10-21 19:00:27

Connectivity Check Results (High Voltage Modulation) from 2010-10-21 00:00 to 2010-10-22 00:00 (1 tests run)

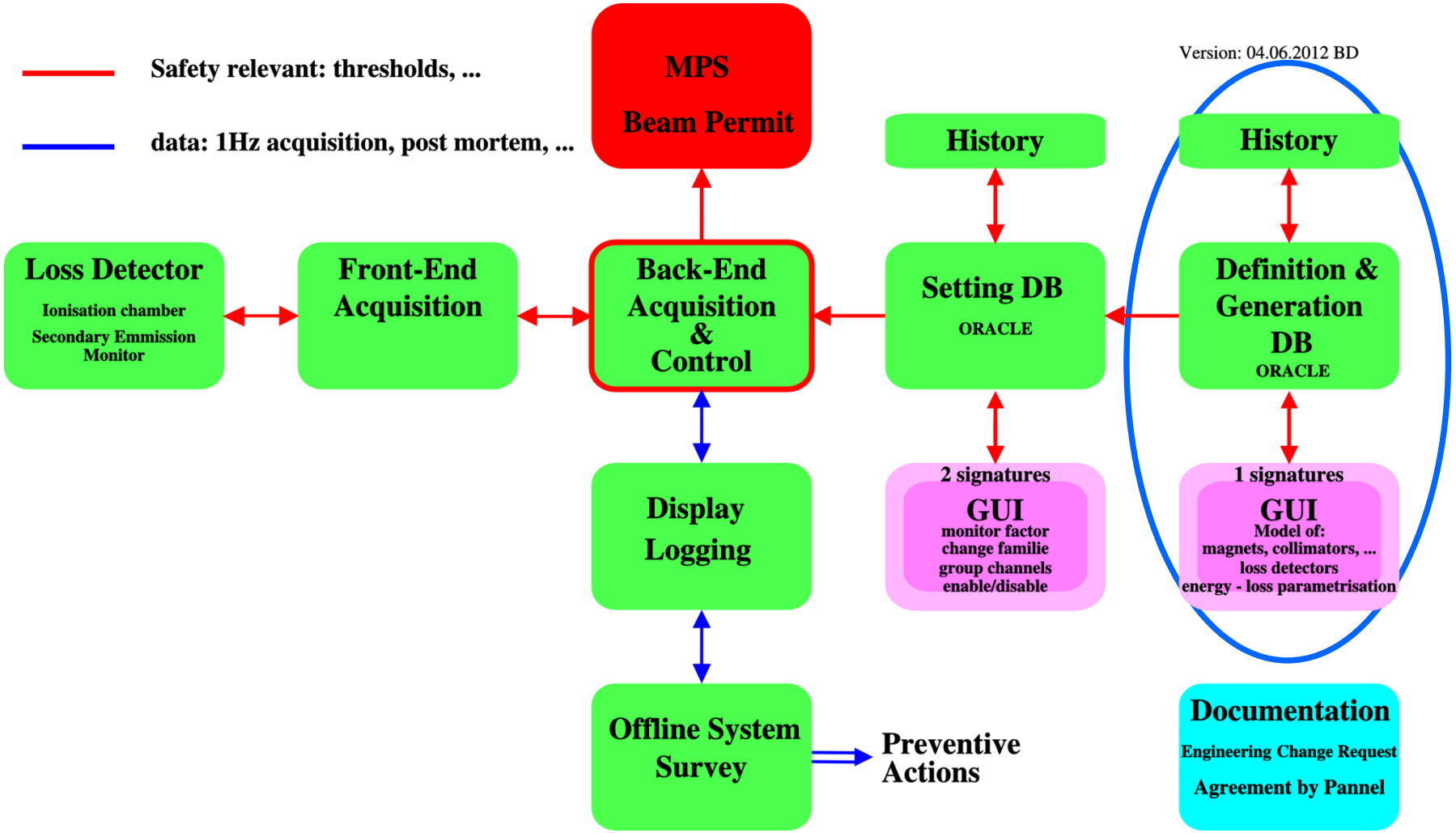
Example: Summary on Connectivity Check Measurement Results

Expert name	Gain min	Gain max	Phase min	Phase max	spare channel
Failures					
BLMQI.10R1.B2I10_MQML	1	0	0	0	0
BLMEL.06R7.B2I20_TCSG.A6R7.B2	1	0	0	0	0
BLMEL.06R7.B2I21_TCSG.A6R7.B2	1	0	0	1	0
BLMEL.06R7.B2I22_TCSG.A6R7.B2	0	1	0	1	0
Warnings					
BLMCC.08R3.A8R3_BATT	1	0	0	0	—
BLMCC.06R3.A6R3_BATT	1	0	0	0	—
BLMCC.06R3.A6R3_HV	1	0	0	0	—
BLMES.06R3.B2E10_TCAPA.6R3.B2	1	0	0	0	—

Summary table

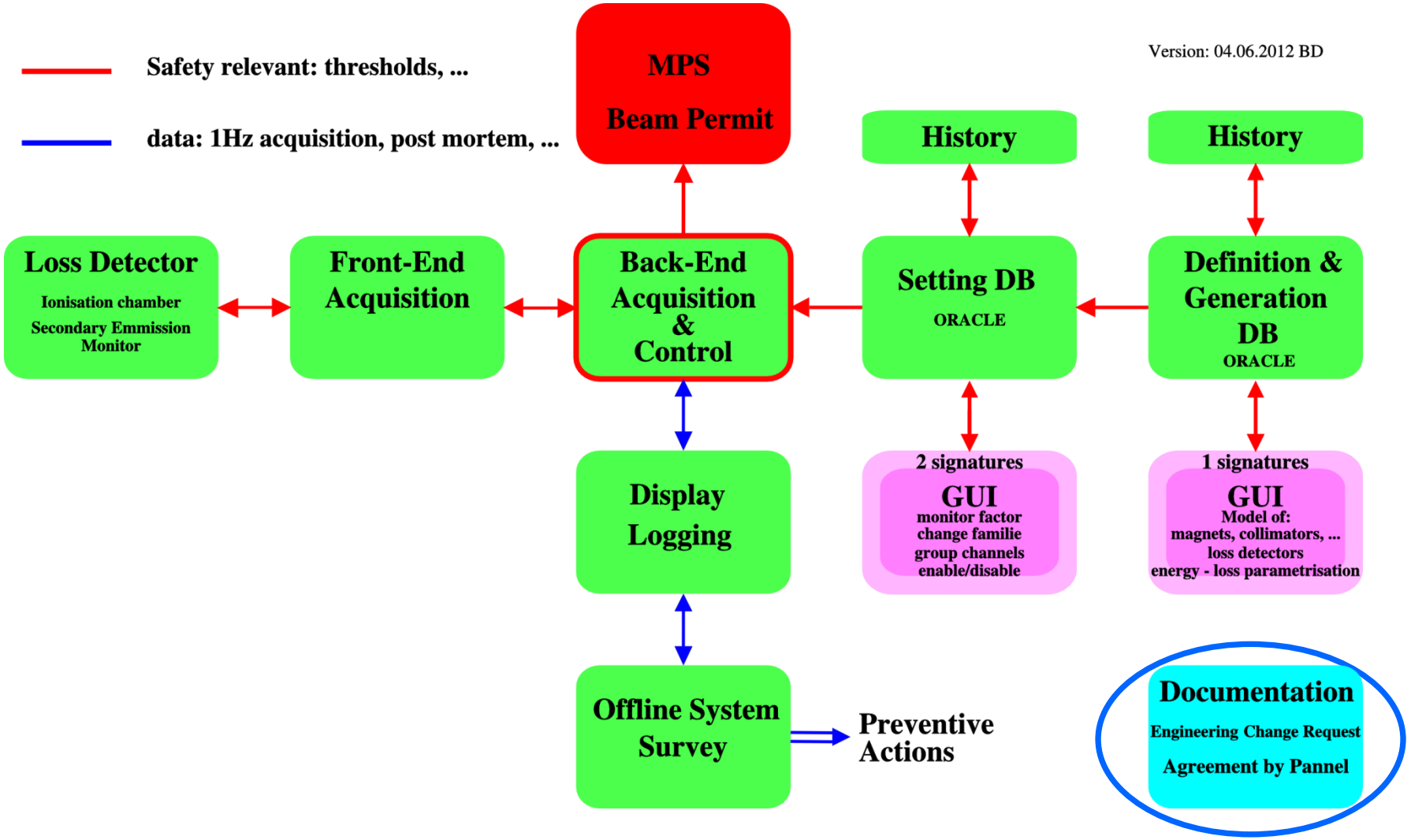


BLM System Information Flow



Now: C++ program and SVN storage Future: all values and functional dependence in ORACLE

BLM System Information Flow



Reliability Feature Implementations

- Detectors connection test:
  - ionisation chambers, constant current over resistor: Los Alamos; modulation of HV: CERN
  - Scintillators and PM: LED at scintillator (DESY, ...)
- HV check: J-PARC, Los Alamos
- Electronics check, offset current: Los Alamos, CERN
- Optical link, CRC: DESY, Jefferson Lab, J-PARC
- Redundant optical link: DESY Petra3
- Survey of status information: PowerPC core in FPGA (Linux+EPICS)
- Use of reliability software: SNS, Fermi Lab project X, ILC

Concluding Remarks

- Key issue to high reliability and availability, survey, parallel system and functional tests
- Reliability and availability needs to be considered from the beginning of a design
  - LHC: PhD thesis on reliability (path has been followed during project)
- System reliability and availability is strongly depending on management of settings, creation of settings and preventive action

- Issue of LHC design: protection and measurement functionality are implemented in same FPGA
  - Critical, because of upgrades are more often needed for the measurement functionality compared to protection functionality
  - New: modular FPGA design and locking of critical parts

Acknoledgements

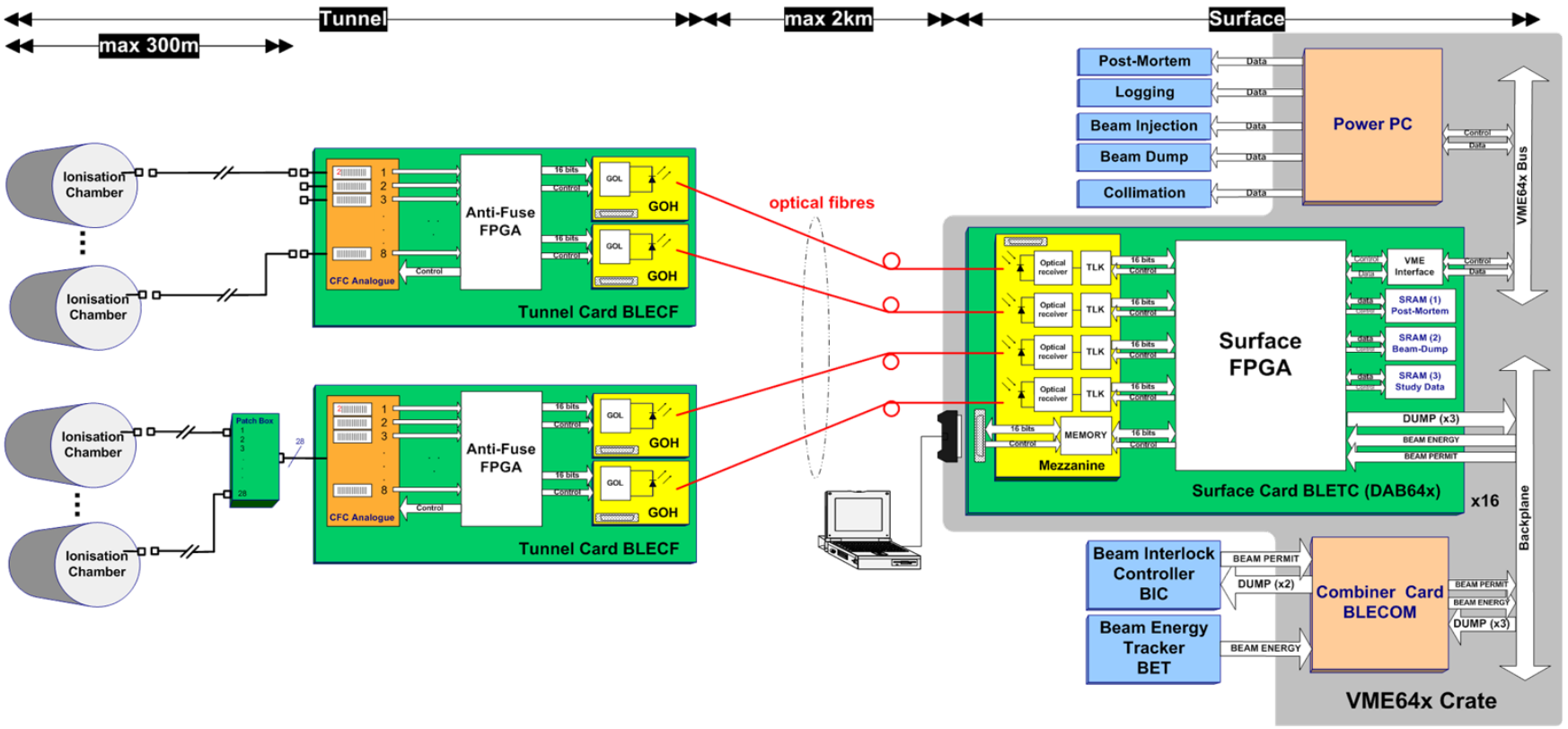
- T.J. Lensch, M. Werner, K. Wittenburg (DESY)
- K. Jordan (Jefferson Lab)
- H. Ikeda, T. Naito, T. Mitsuhashi, A. Nakagava, K. Satou, T. Suwada, H. Tanaka, T. Toyama, K.Yamamoto (KEK)
- A. Zhukov, A. Aleksandrov (SNS)

Reserve Slides

Literature

- http://cern.ch/blm
- LHC
  - Reliability issues, thesis, G. Guaglio
  - Reliability issues, R. Filippini et al., PAC 05
  - Front end electronics, analog, thesis, W. Friesenbichler
  - Front end electronics, analog-digital, E. Effinger et al.
  - Digital signal treatment, thesis, C. Zamantzas
  - Balancing Safety and Availability for an Electronic Protection System, S. Wagner et al., to be published, ESREL 2008

The BLM Acquisition System



Analog front-end FEE

- **Current to Frequency Converters (CFCs)**
- **Analogue to Digital Converters (ADCs)**
- **Tunnel FPGAs:**
  Actel's 54SX/A radiation tolerant.
- **Communication links:**
  Gigabit Optical Links.

Real-Time Processing BEE

- **FPGA Altera's Stratix EP1S40 (**medium size, SRAM based**)**
- **Mezzanine card for the optical links**
- **3 x 2 MB SRAMs for temporary data storage**
- **NV-RAM for system settings and threshold table storage**

Hardware Failures (since Feb. 2010)

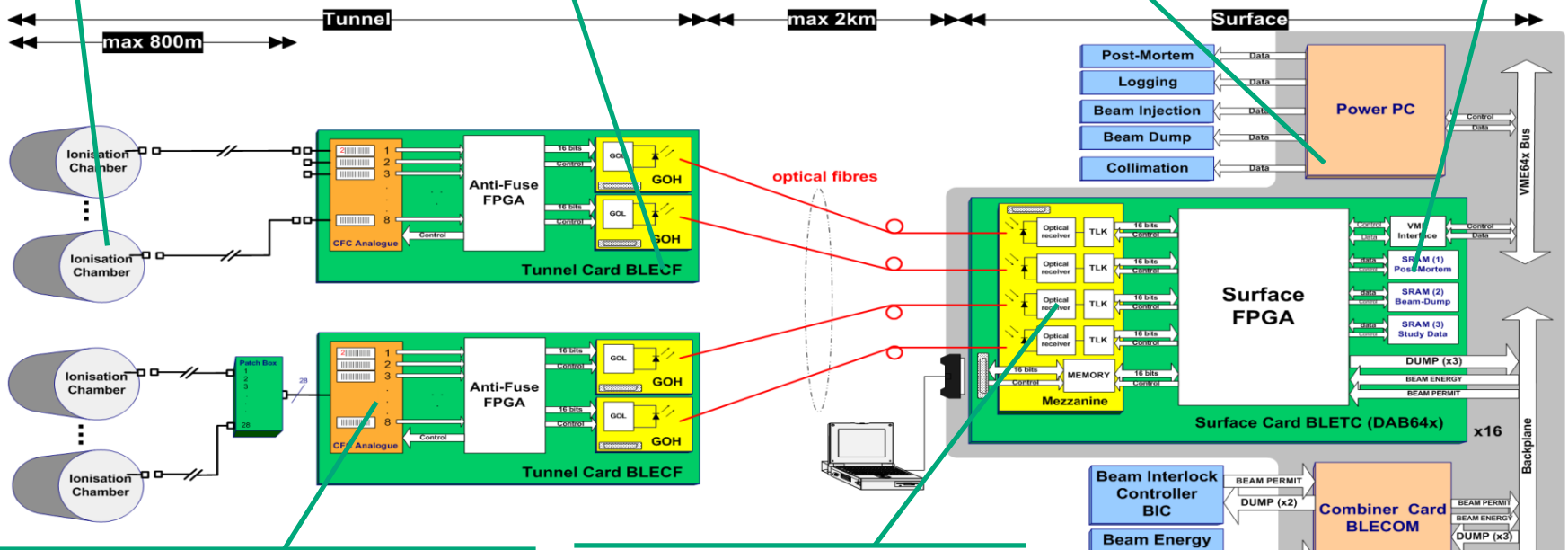
- Mostly, onset of system degradation detected by regular offline checks before malfunction
- Number of failures regarded manageable (no availability issue)

12 IC with bad soldering (out of 3600)

9 GOH with low power
1 damaged connector
out of 1500

3 failed CPU RIO3 out of 25

2 with failed SRAM out of 350



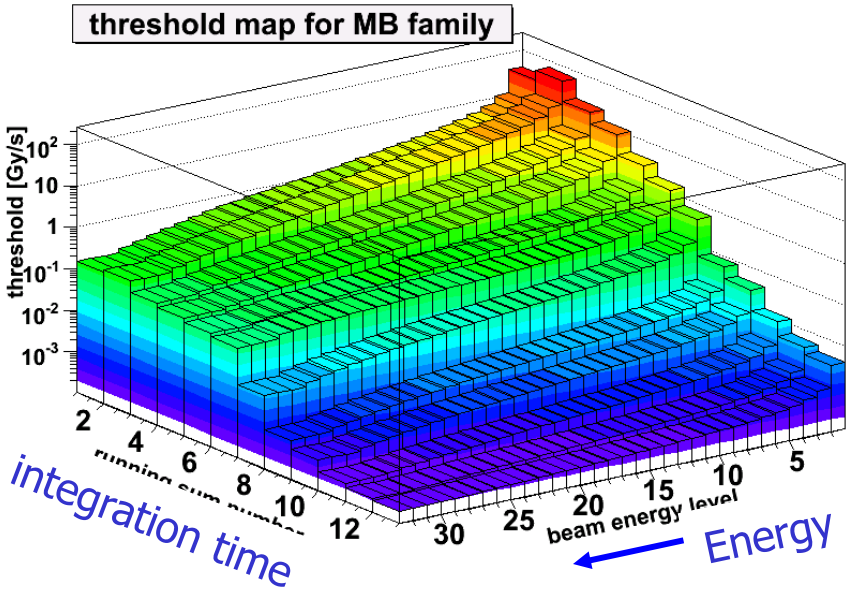
7 CFC with 'noisy' components
2 cards with bad soldering
out of 750

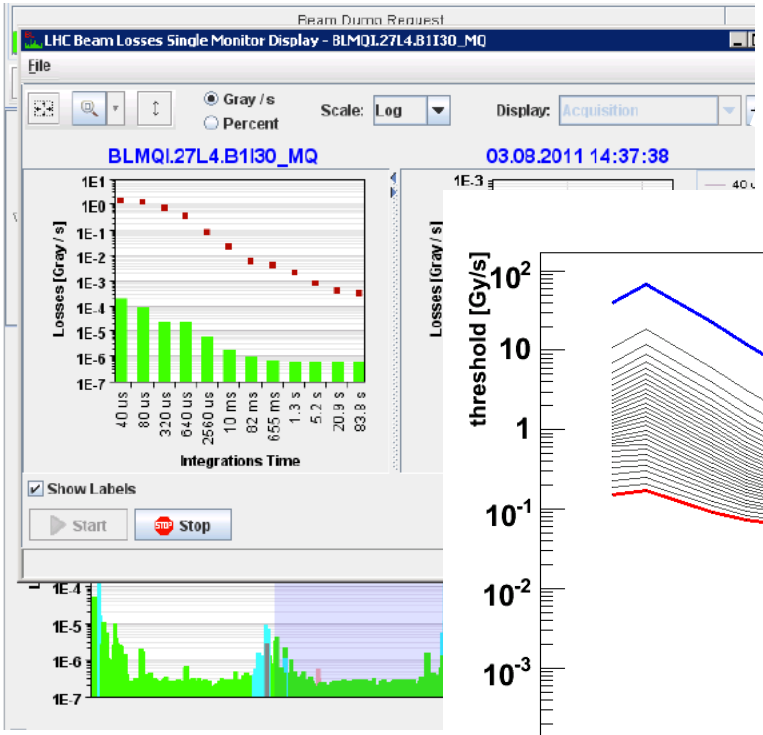
12 with 'weak' receivers
out of 1500

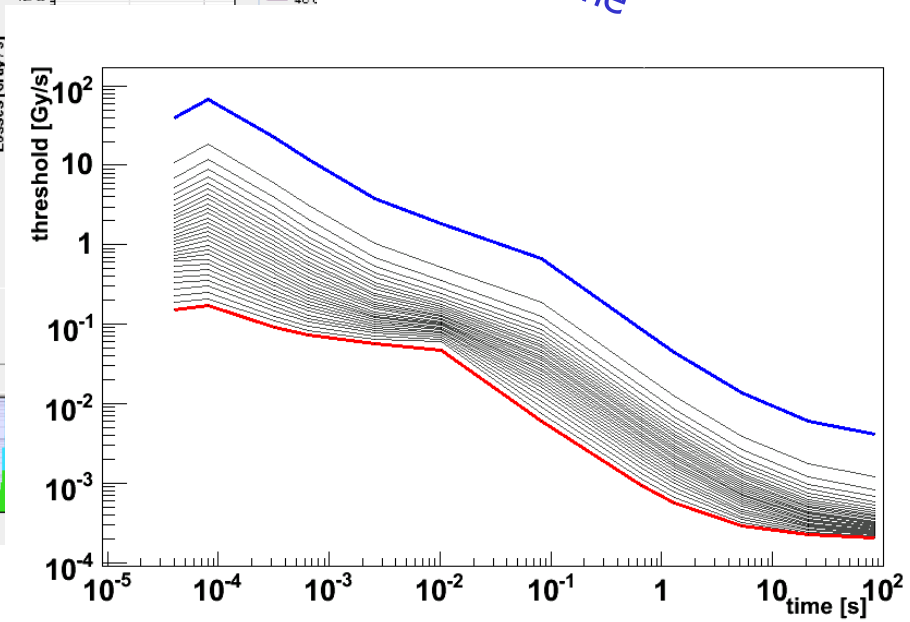
1 VME Power Supply, out of 25

BLM Published Data – Logging Data – Online Display

- Change of the thresholds:
  - As function of loss duration
  - As function of beam energy
- Will also be implemented for warm magnet and equipment protection

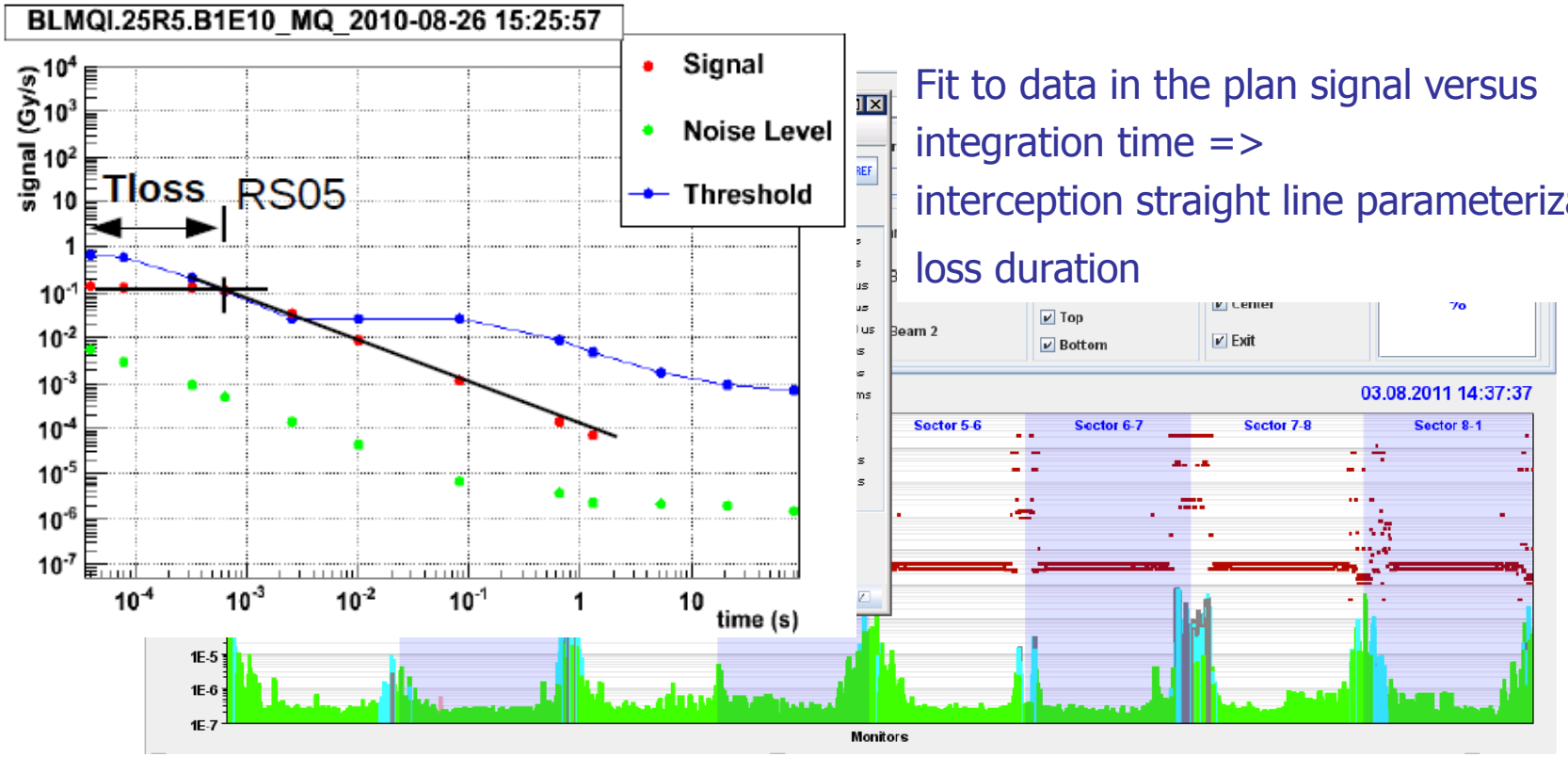






BLM Published Data – Logging Data – Online Display

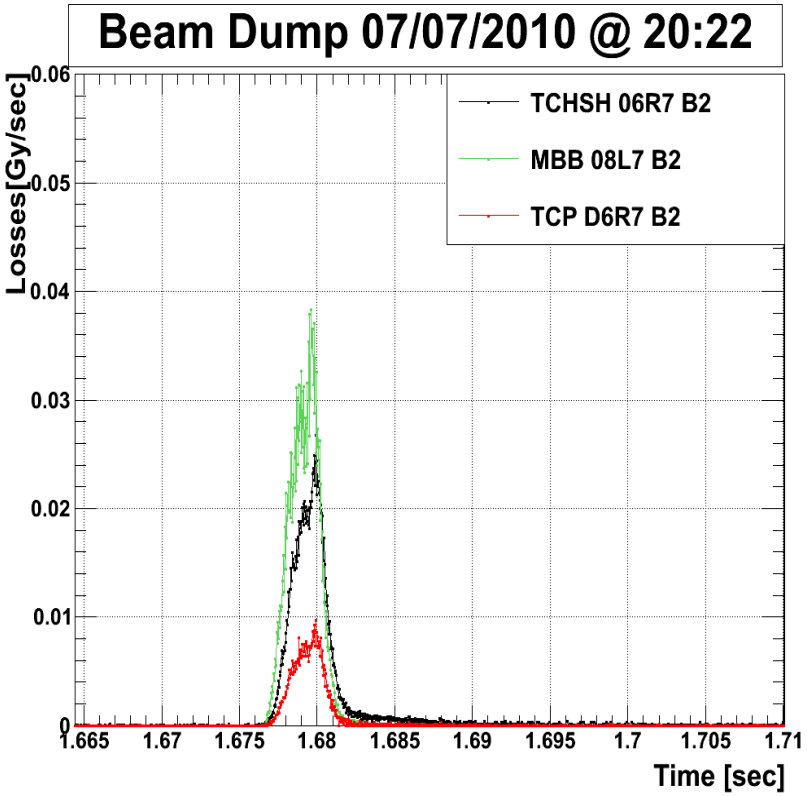
- Extensively used for operation verification and machine tuning
- 1 Hz Logging (12 integration times)
  - Integration times < 1s: maximum during the last second is logged
    → short losses are recorded and loss duration can be reconstructed (20% accuracy)
  - Also used for Online Display



Fit to data in the plan signal versus integration time =>
interception straight line parameterization =>
loss duration

Storage of several running sums allows reconstruction of duration of loss event (reduction of network traffic and data storage place)

Post Mortem Data (some examples), Zoom



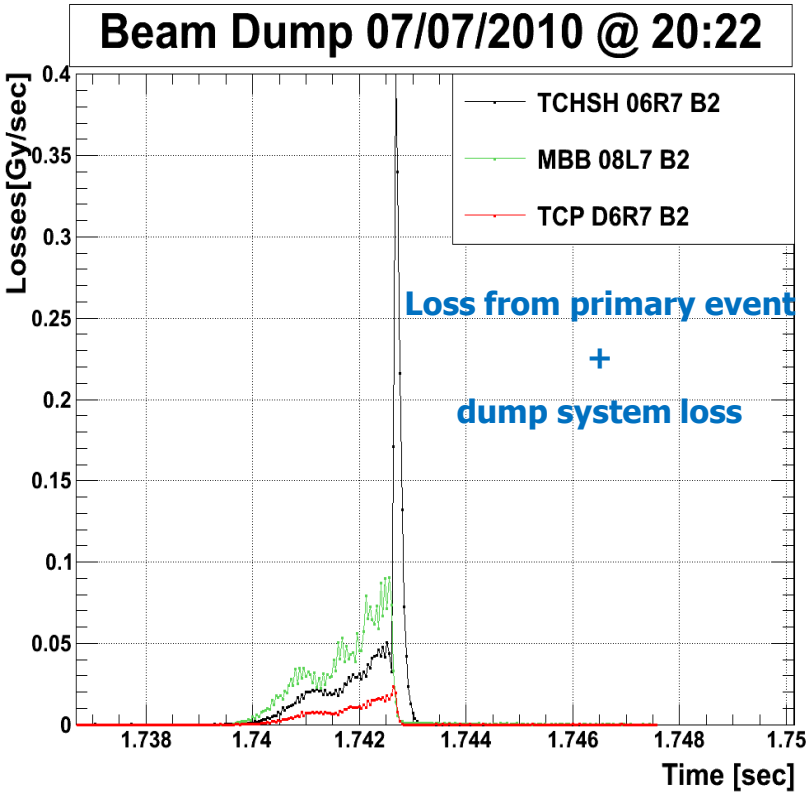
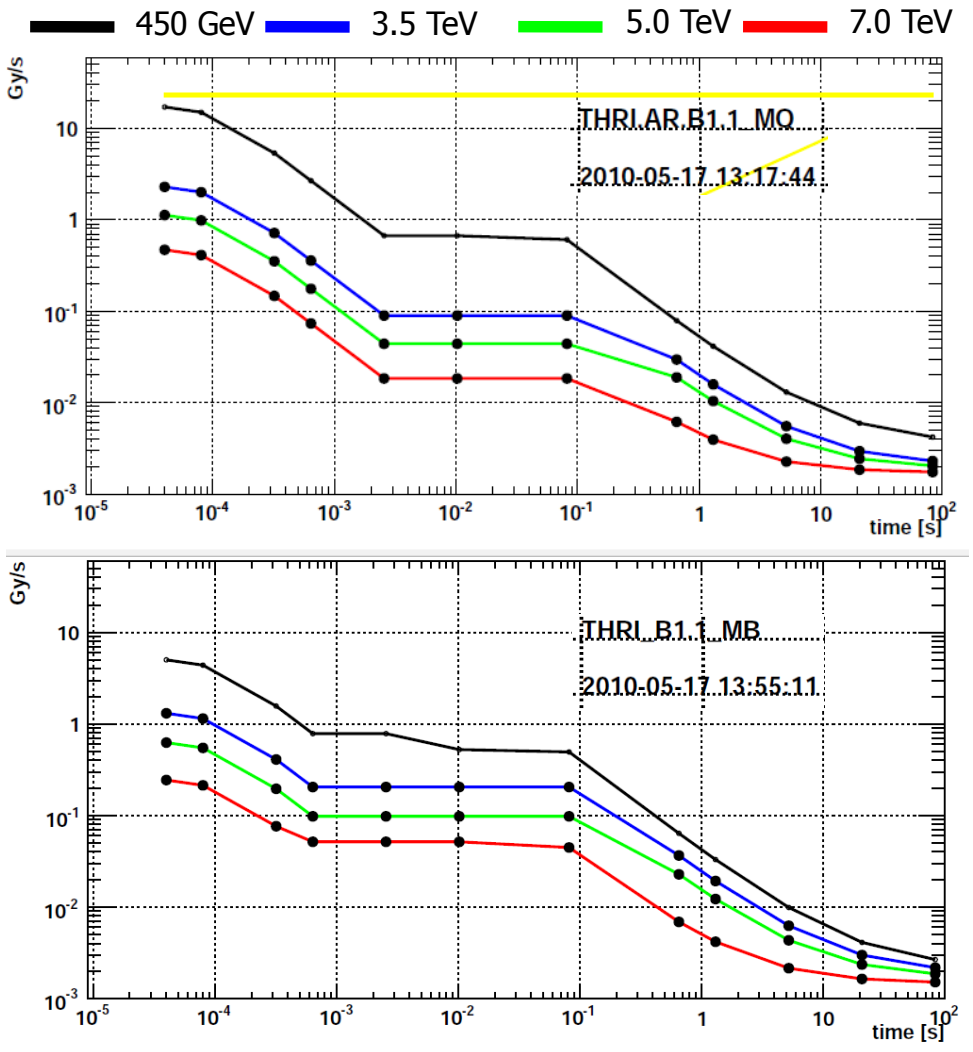


Table 4: Hardware interventions due to channel degradation or failure since february 2010

Element	Details	Number	Out of total installed
IC	bad soldering	12	3600
tunnel electronics	noisy analogue component (CFC)	7	359
tunnel electronics	bad soldering	2	720
tunnel electronics	low power optical transmitter (GOH)	9	1500
tunnel electronics	damaged connector	1	1500
surface electronics	weak optical receiver	12	1500
surface electronics	failed SRAM	2	350
VME64x Crate	failed CPU RIO3	3	25
VME64x Crate	failed power supply	1	25

Quench and Damage Levels

Quadrupole and bending magnet thresholds

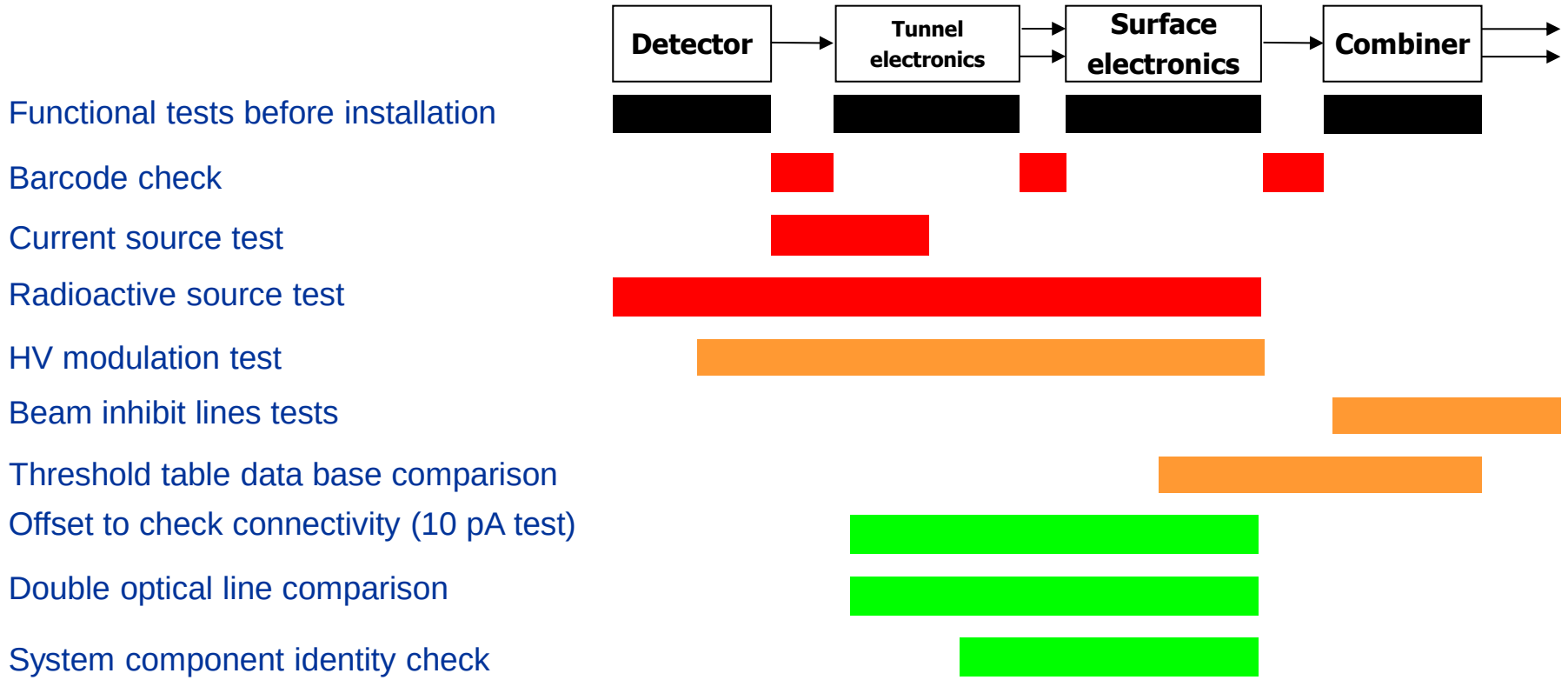


Specifications

- Time resolution ½ turn, 40 us
- Average calculation loss:
  - 12 values, 40 us to 83 s
- Max amplitude 23 Gy/s
- Min amplitude
  - 1E-4 Gy/s @ 40 us
  - 3E-7 Gy/s @ 1.3 s
- Dynamic
  - 2E5 @ 40 us
  - ~ 1E8 @ 1.3 s
- Damage level
  - 2000 Gy/s @ 1 ms
- All channels could be connected to the interlock system
- Thresholds
  - Loss duration dependent, 12 values
  - Energy dependent, 32 values
  - About 1.5 E6 thresholds

Functional Tests Overview

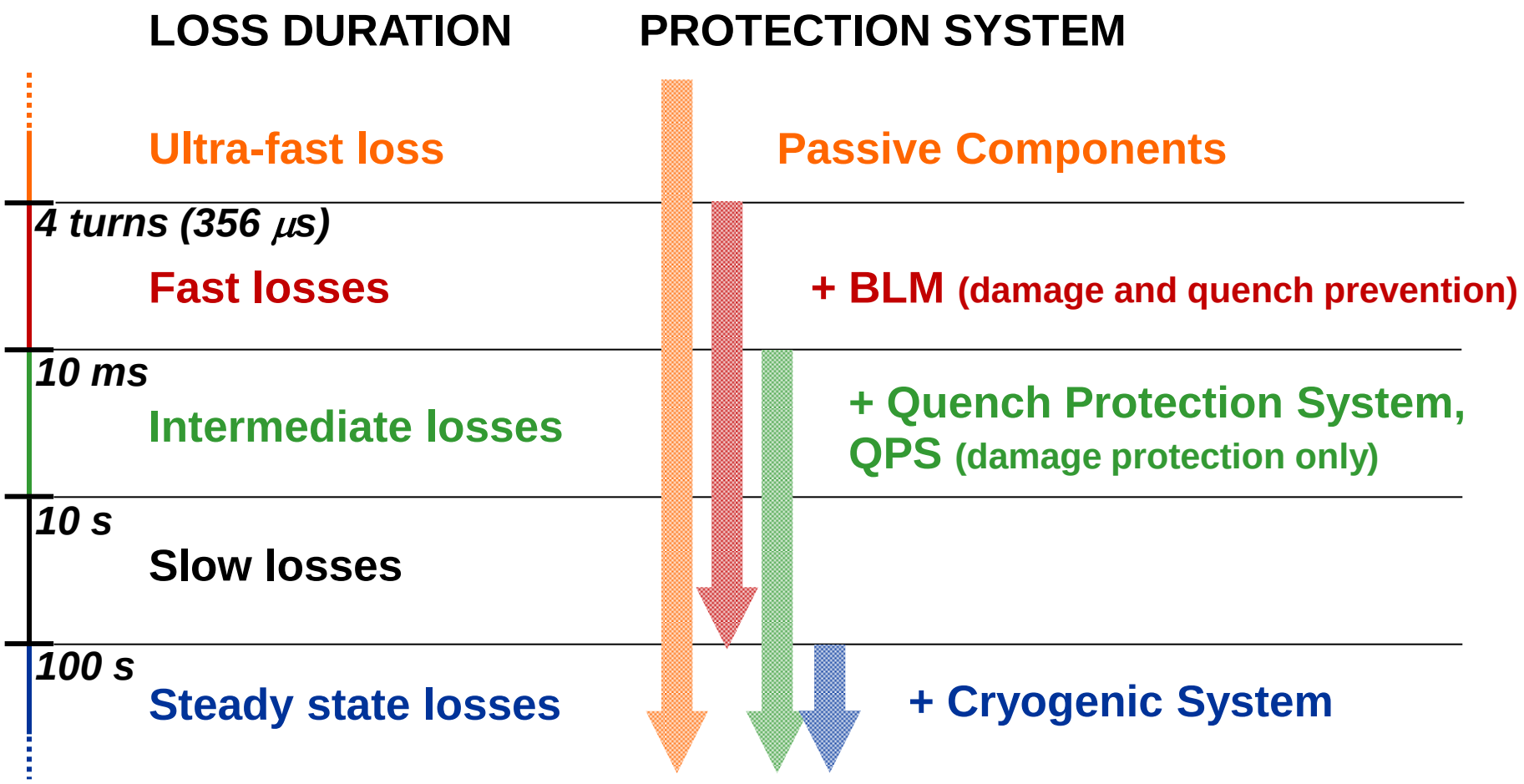
PhD thesis G. Guaglio



Inspection frequency:

Reception | Installation and yearly maintenance | Before (each) fill | Parallel with beam

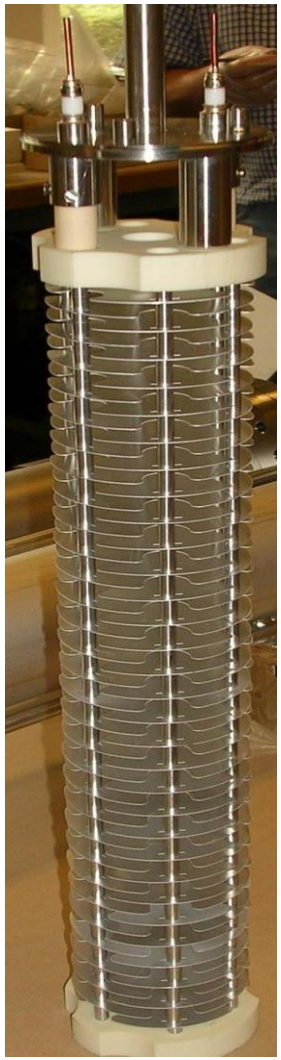
Specification: Beam Loss Durations and Protection Systems



Since not active protection possible for ultra-fast losses => passive system

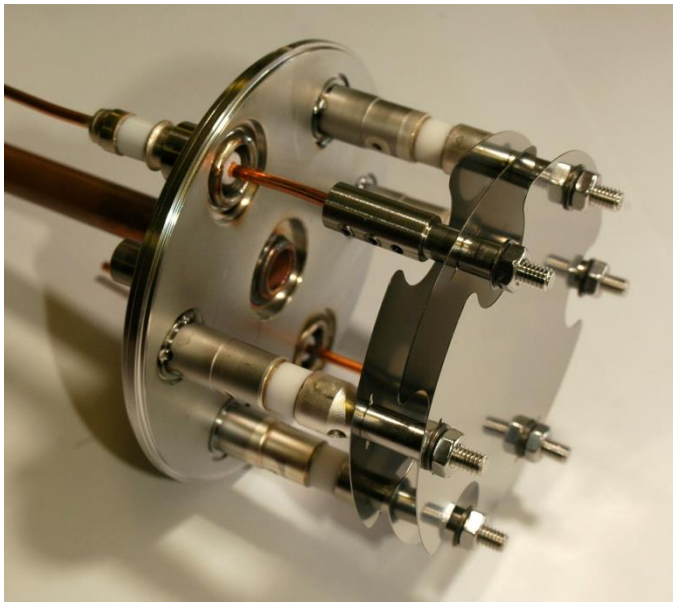
Classification loss signals to be used for functional and technical specification

Ionisation Chamber and Secondary Emission Monitor



- Stainless steal cylinder
- Parallel electrodes distance 0.5 cm
- Diameter 8.9 cm
- Voltage 1.5 kV
- Low pass filter at the HV input

Signal Ratio: IC/SEM = 60000



IC:

- Al electrodes
- Length 60 cm
- Ion collection time 85 us
- N_2 gas filling at 1.1 bar
- Sensitive volume 1.5 l

SEM:

- Ti electrodes
- Components UHV compatible
- Steel vacuum fired
- Detector contains 170 cm2 of NEG St707 to keep the vacuum < 10-4 mbar during 20 years

Combiner card inside the LHC BLM system

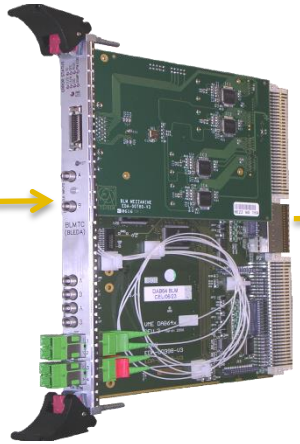
Beam Loss Monitors (4000)

around the LHC ring

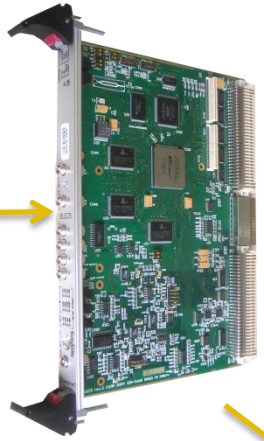
Tunnel Cards (700)

Tunnel Card test benches (5)

Threshold Comparators (350)



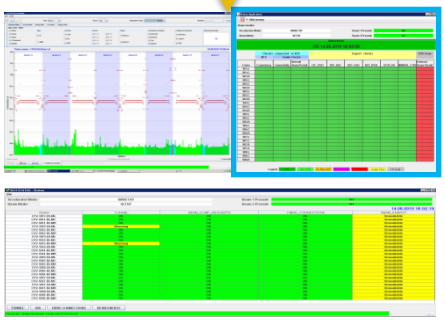
Combiner and Survey (25)



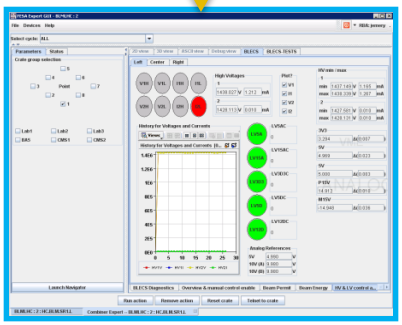
Beam Energy Receivers (8)
[CISV]
Hardware:
BE-CO-HT (P. Alvarez)
Responsible:
TE-MPE-MI (B. Puccio)
Energy measurements:

Interlock Interfaces (16)
[CIBUS] TE-MPE-MI
(B. Puccio, B. Todd)

BLM HV supplies

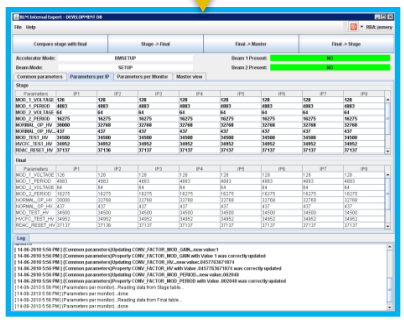


Operational applications (2)



Expert applications (2)

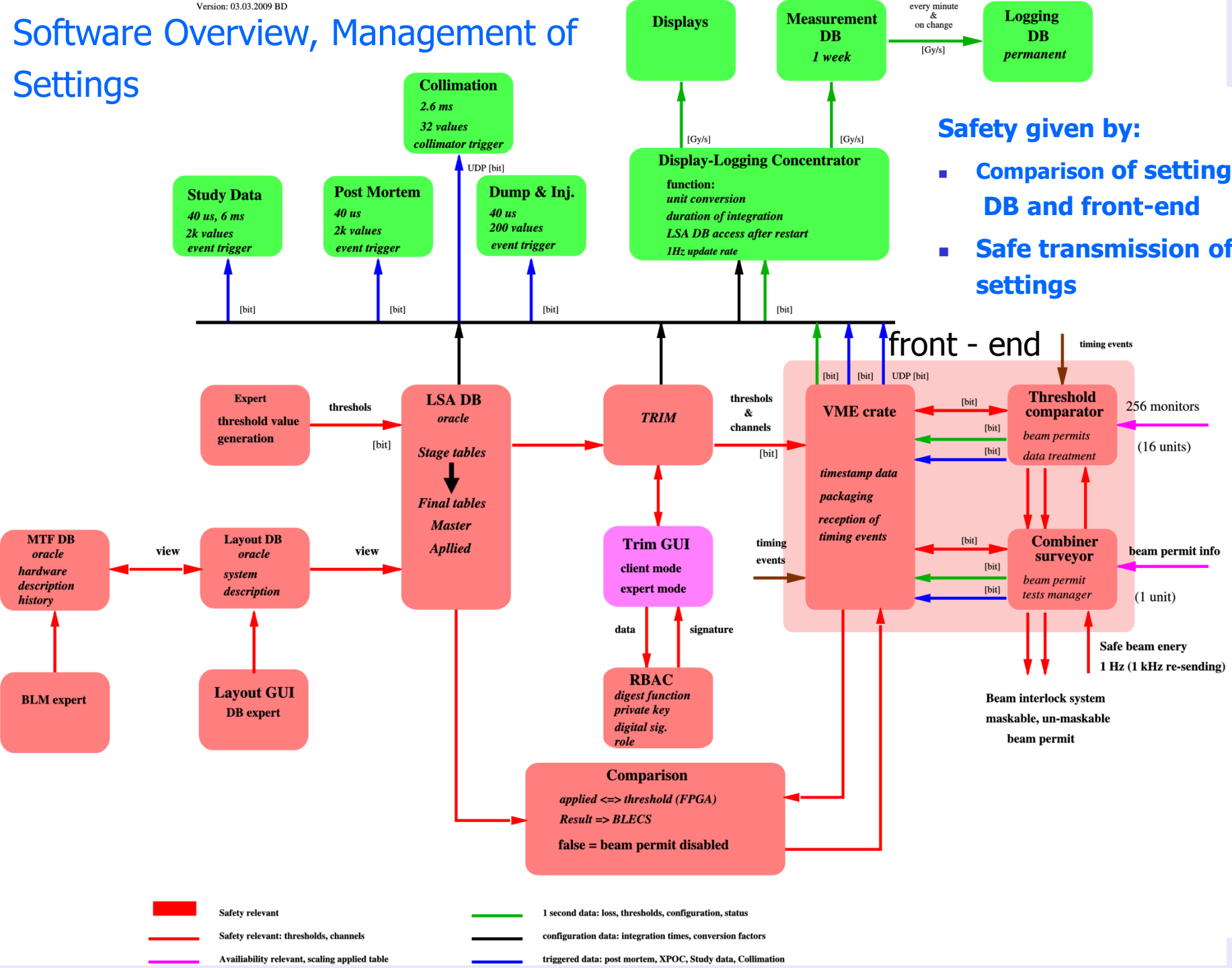
Diagnostics application,
phase and amplitude
for the connectivity check



Settings applications (2)

Version: 03.03.2009 BD

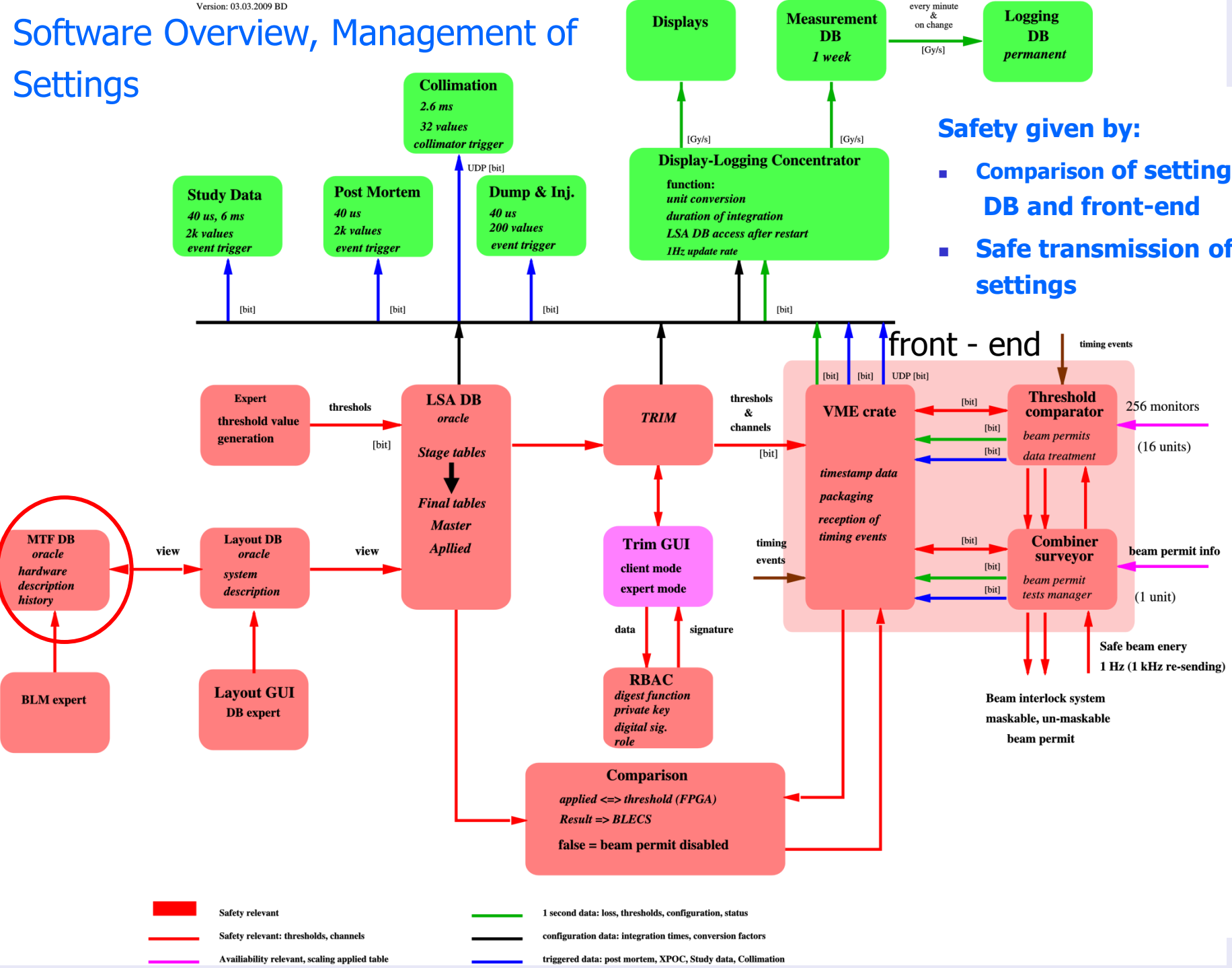
Software Overview, Management of Settings



Safety given by:

- Comparison of settings at DB and front-end
- Safe transmission of settings

Software Overview, Management of Settings

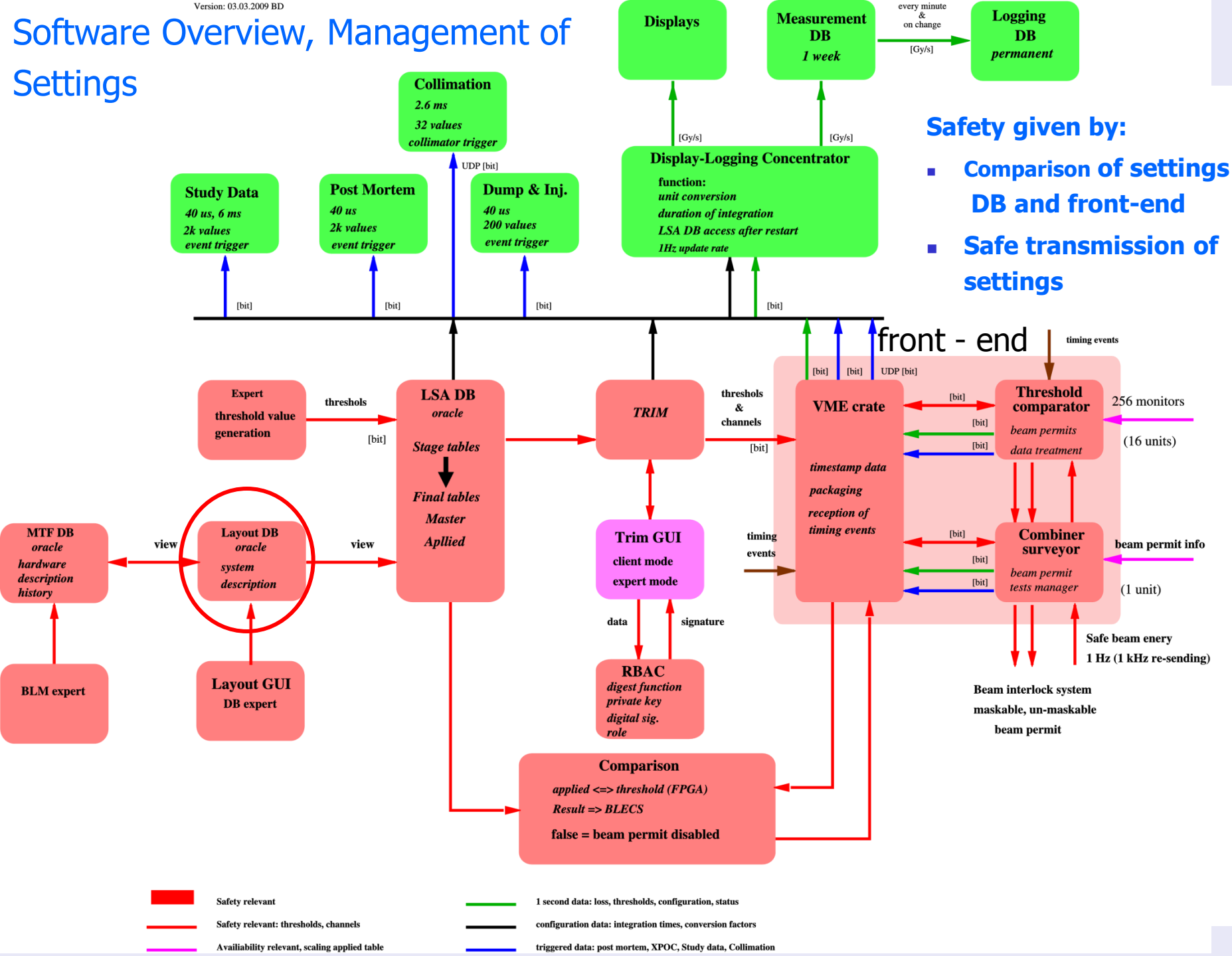


Safety given by:

- **Comparison of settings at DB and front-end**
- **Safe transmission of settings**

Version: 03.03.2009 BD

Software Overview, Management of Settings

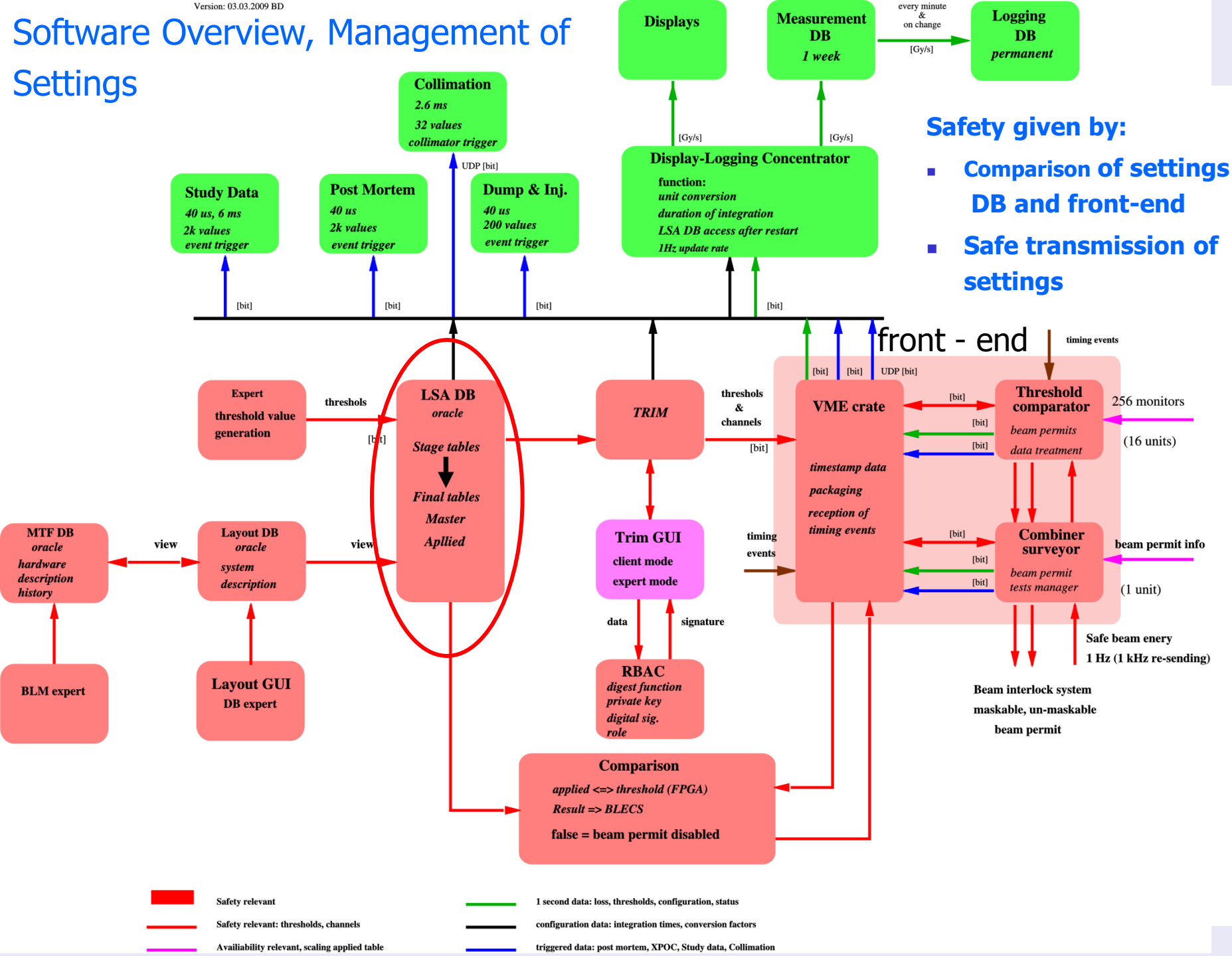


Safety given by:

- Comparison of settings at DB and front-end
- Safe transmission of settings

Version: 03.03.2009 BD

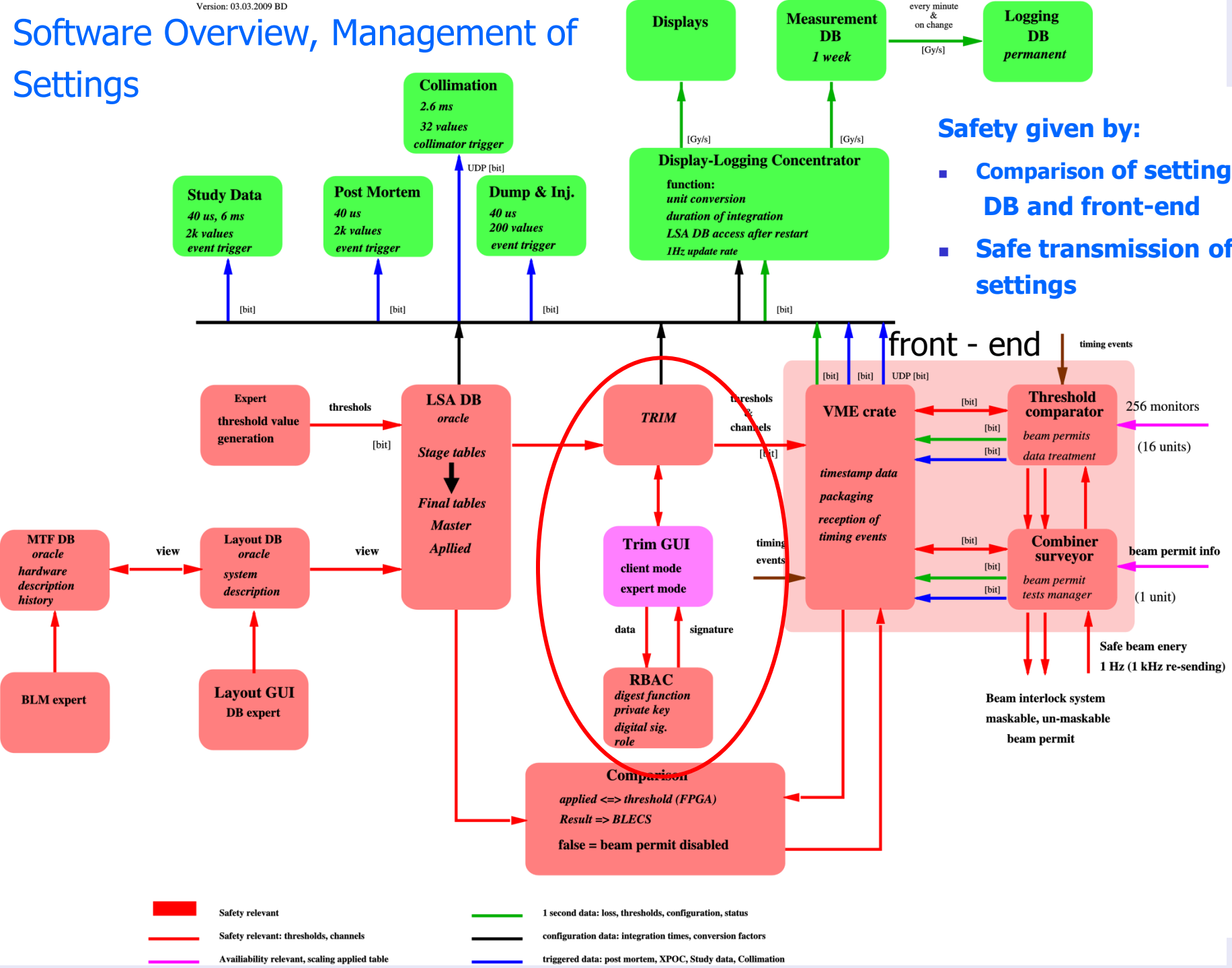
Software Overview, Management of Settings



Safety given by:

- **Comparison of settings at DB and front-end**
- **Safe transmission of settings**

Software Overview, Management of Settings

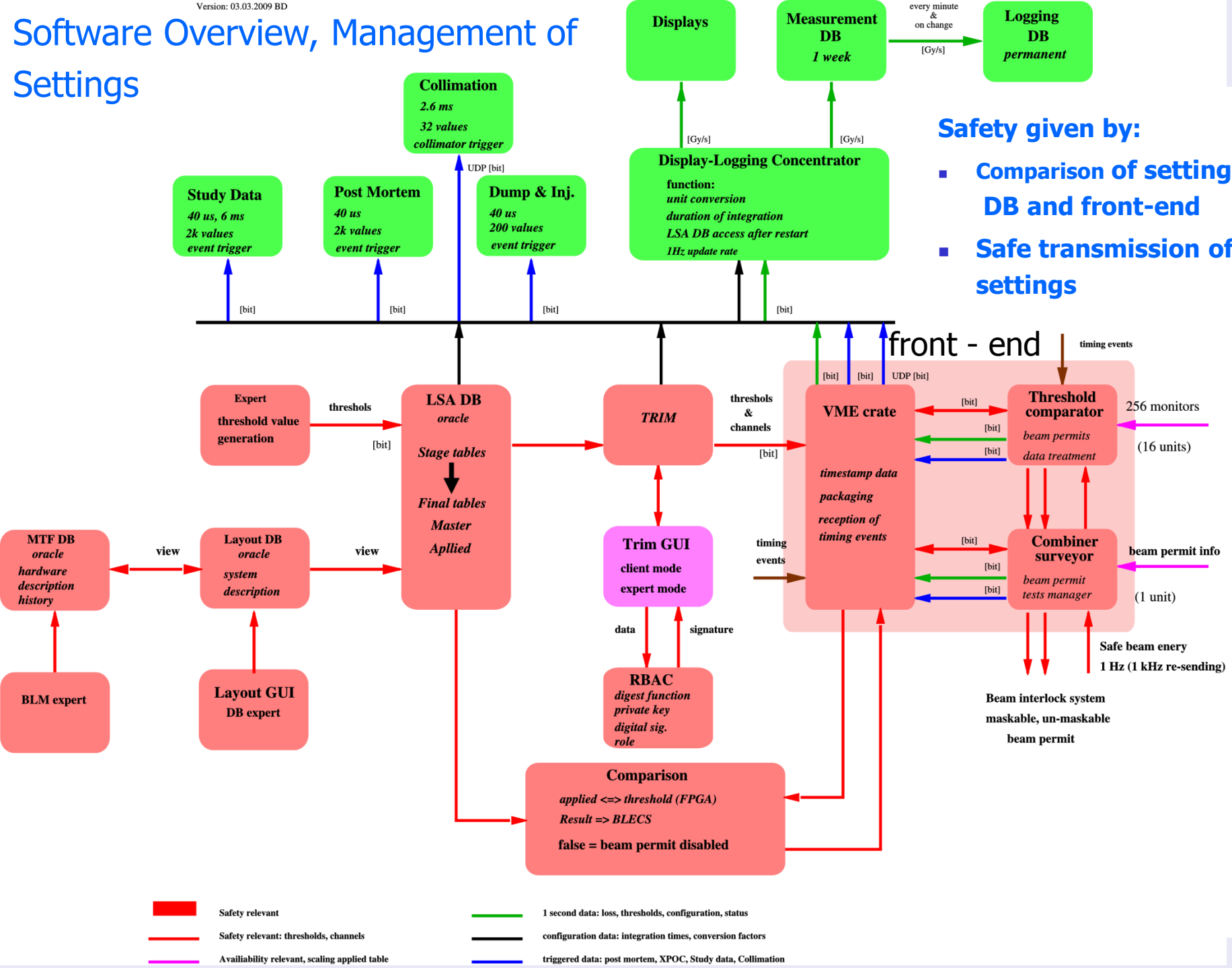


Safety given by:

- Comparison of settings at DB and front-end
- Safe transmission of settings

Version: 03.03.2009 BD

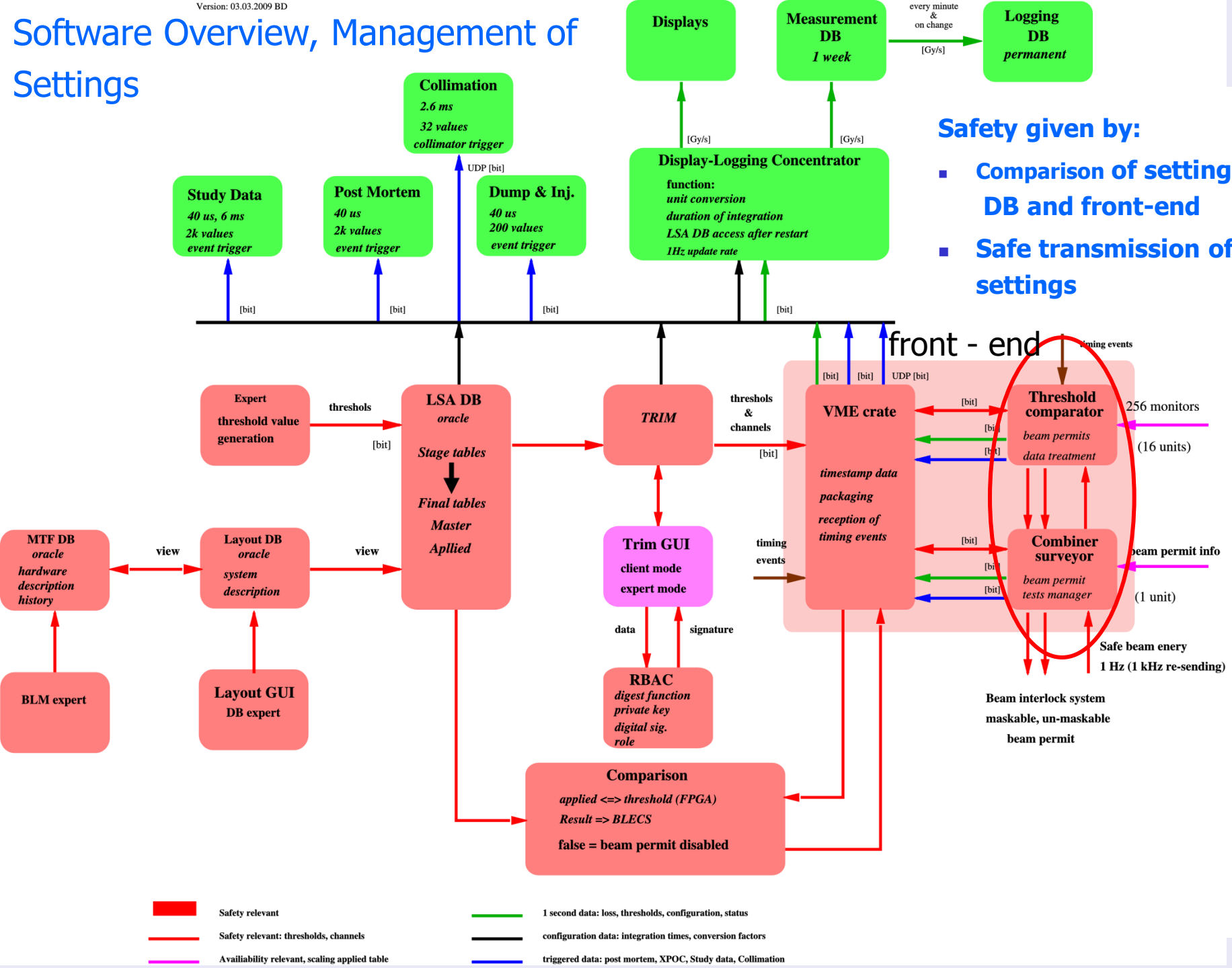
Software Overview, Management of Settings



Safety given by:

- Comparison of settings at DB and front-end
- Safe transmission of settings

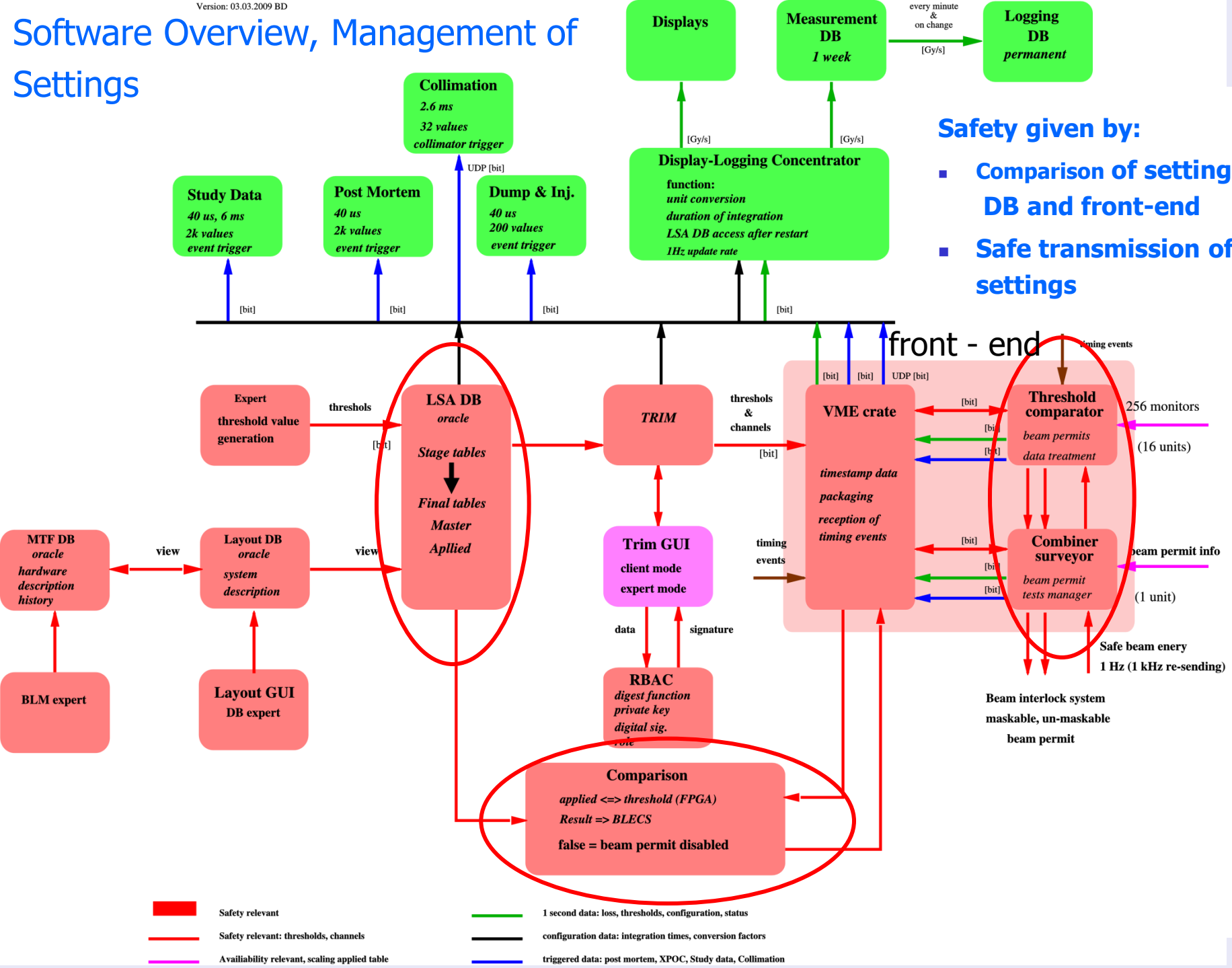
Software Overview, Management of Settings



Safety given by:

- Comparison of settings at DB and front-end
- Safe transmission of settings

Software Overview, Management of Settings

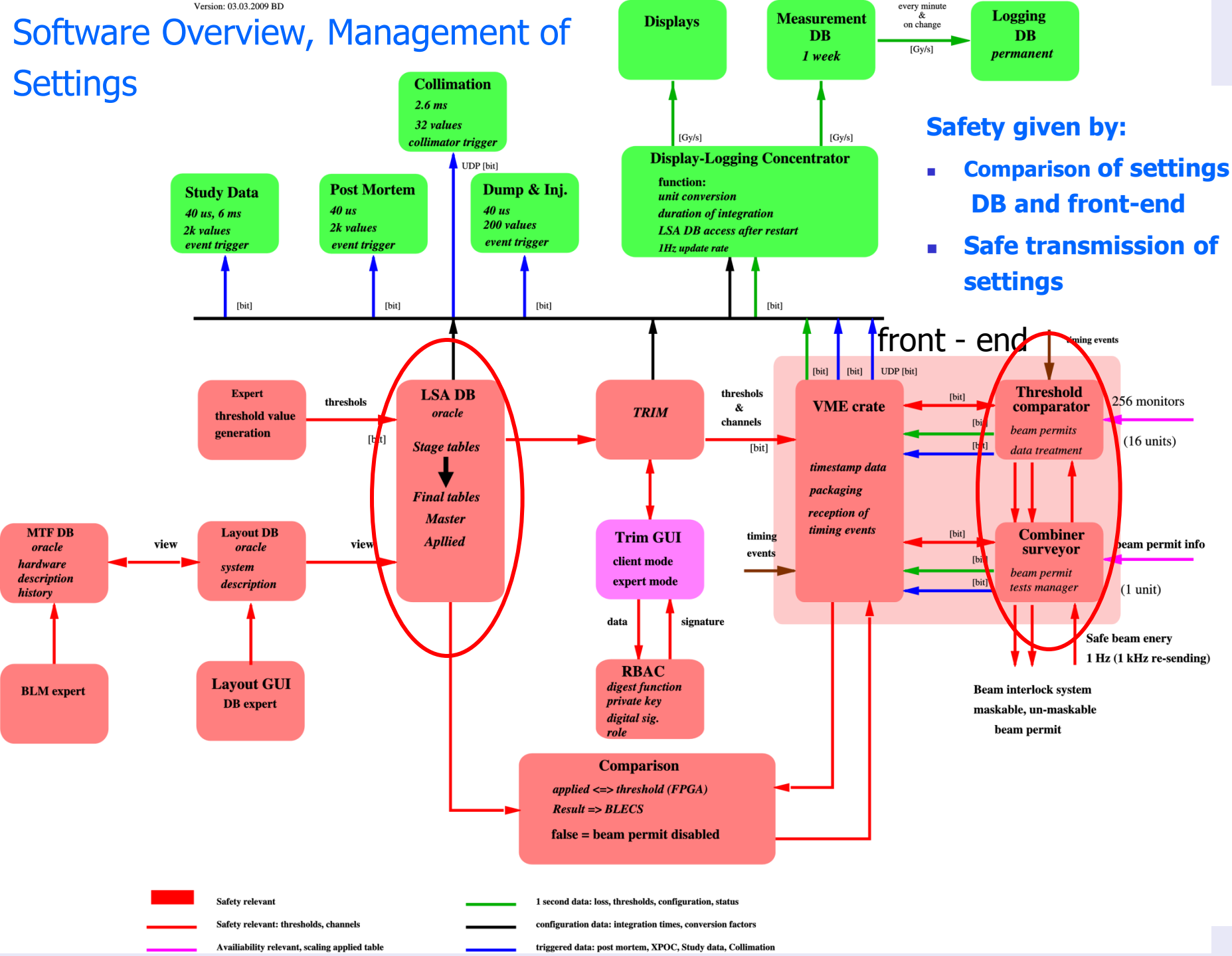


Safety given by:

- Comparison of settings at DB and front-end
- Safe transmission of settings

Version: 03.03.2009 BD

Software Overview, Management of Settings

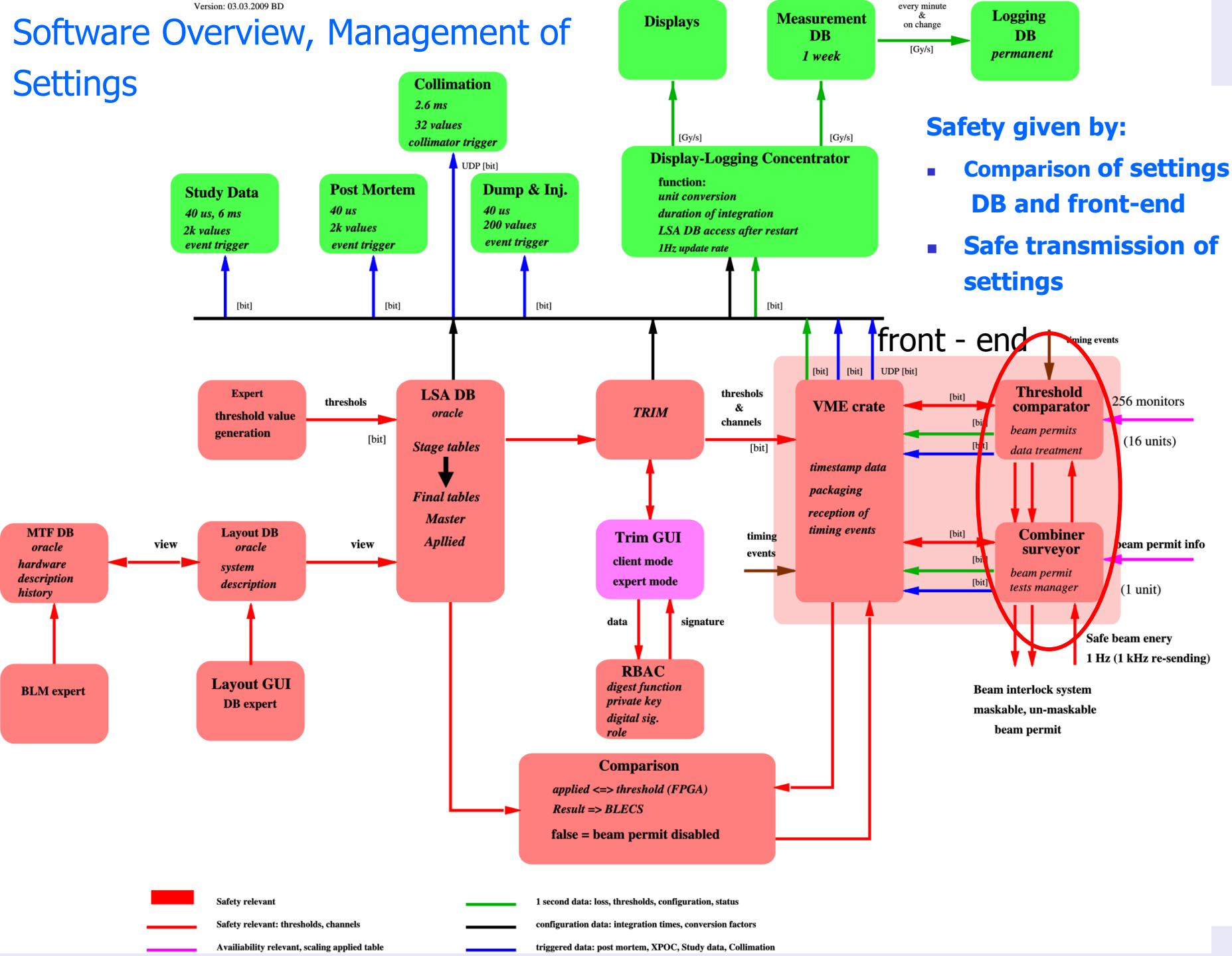


Safety given by:

- Comparison of settings at DB and front-end
- Safe transmission of settings

Version: 03.03.2009 BD

Software Overview, Management of Settings

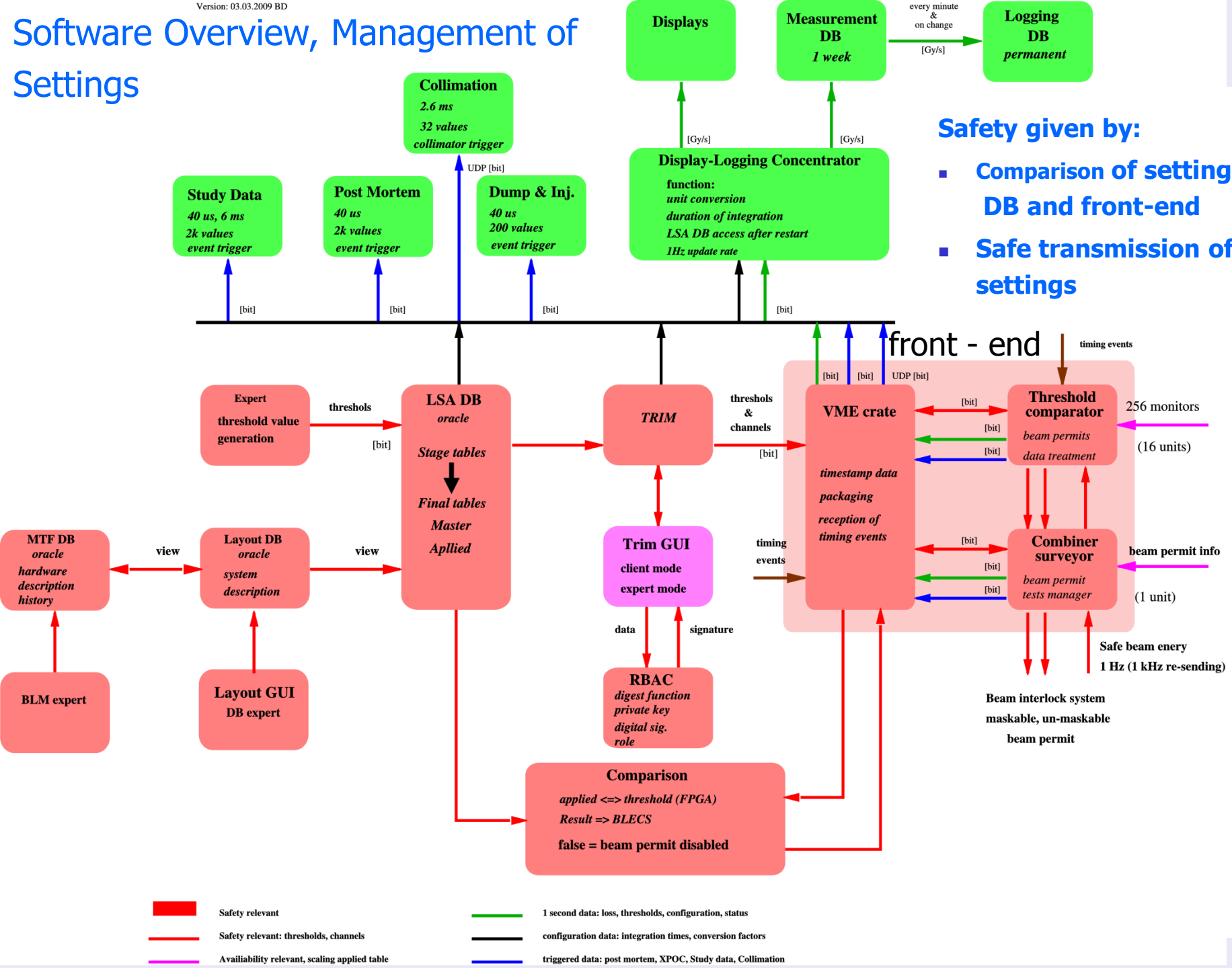


Safety given by:

- Comparison of settings at DB and front-end
- Safe transmission of settings

Version: 03.03.2009 BD

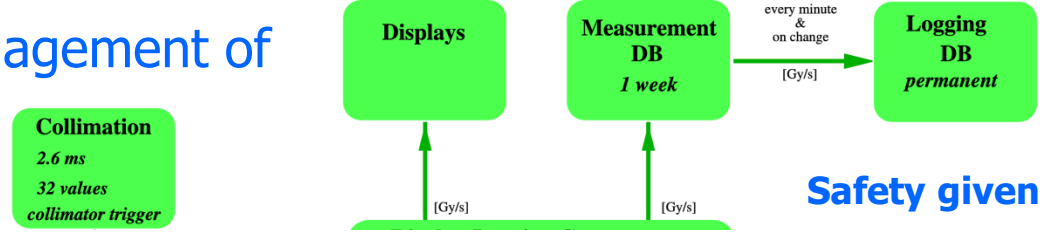
Software Overview, Management of Settings



Safety given by:

- Comparison of settings at DB and front-end
- Safe transmission of settings

Software Overview, Management of Settings



Safety given by:

1. Modular design of data base very useful (if changes are needed limited impact)
    1. MTF: history of equipment e.g. ionisation chamber, electronic cards, …
    2. Layout: description of links between equipment
    3. LSA: reference for all data needed in the front-end (some imported from MTF and Layout)
2. Storage of data in frontend in FPGA memory (even here corruptions observed)
3. Master for comparison is the front-end (this allows immediate beam inhibit)
4. Design very early defined in PhD thesis on reliability (root was followed during project)
5. Issue of design: protection and measurement functionality are implemented in same front-end (review remark).
    1. Critical, because of upgrades are more often needed on measurement functionality compared to protection functionality
    2. New design: locking of FPGA firmware, which has protection functionality (partial solution)
    3. Occupation of FPGA by firmware too large, first estimate of occupation will be about 30% for new BLM systems