Report of the review:

UPS power distribution of LHC Beam Dumping System (LBDS)

On behalf of the
-TE-ABT design team
- the review speakers
- the review panel

<u>Outline</u>:

- Technical review general information
  - facts, aims, reviewers, agenda
- Basic introduction to LBDS
  - beam dump process, components, timing, safety, powering scheme, power hold-on
- 230 V power mitigations and +12 V common mode coupling
- UPS and power distribution, selectivity improvements, proposal for LS1
- Power distribution inside racks, crate power supplies
- LBDS architecture improvements
  - DC common mode coupling, beam interlock system safe dump, power surveillance
- Tests
  - power failures studies, commissioning
- Conclusions and recommendations

Technical review: general

- Held on June 20th at CERN

- The facts:
  - LBDS is an essential critical element of the LHC operation and protection

    it carries out the safe disposal of the energy stored in the two circulating beams
  - Two unexpected failures of the VME power supplies were observed in 2012, alerting on:
    a) weakness in the fault tolerance architecture of the LBDS powering system
    b) unsatisfactory circuit breaker selectivity of the 230V a.c. power system
  - A common mode failure point was discovered in a +12 V DC power feed line

- Aims of the review:
  - Give boost to LBDS Team to investigate powering aspects of system
  - Get input from other system experts who have knowledge in the various domains of this subject (beam dump, UPS, power network, power supplies, controls, system reliability and redundancy)
  - Debate technical implementations, mitigation actions and promote technical knowledge sharing
  - Validate proposed immediate technical changes and planned actions in perspective of LS1

- Agenda, slides and report available at:

  \\cern.ch\dfs\Departments\TE\Projects\Electr_Coordination\Technical reviews\UPS power distribution of LBDS

Technical review: reviewers and technical expertise

Gerard Cumer EN/EL-OP
power electrical network including UPSs, operation, tests, fault analysis and performance

Wieslaw Iwanski PH/ESE-BE
back end electronics systems for physics experiments, crates and power supplies infrastructures

Hugues Thiesen TE/EPC-MPC
LHC commissioning electrical systems, power conversion, loads and a.c. distribution

Benjamin Todd TE/EPC-CC
power converter controls, formerly beam interlocks & machine protection systems

Jan Uythoven TE/ABT-BTP
reference for TE-ABT, studies of injection & extraction, transfer lines and beam dumping systems, beam physics, equipments and performance

Marc Vanden Eynden BE/CO-FE
RT embedded systems and S/W framework for LHC & injectors, support contract for Wiener crates and PSs for accelerators

Technical review: agenda

- 3 introduction topics
- 6 detailed presentations
- Wide and very motivated participation from BE, EN, PH, TE

Scope of the review, proposals, plans

General overview on LBDS challenges, beam equipments, safety concepts

6 core technical presentations:

- main power system description
- dump triggering schemes, hardware
- UPS powering and selectivity
- power distribution inside crates
- system reliability improvements
- power failure impact studies and tests

Technical review on UPS power distribution of the LHC Beam Dumping System (LBDS)

Wednesday, June 20, 2012 from **09:00** to **12:30** (Europe/Zurich)
at **CERN (864/1-C02)**

Description Reviewers:

Gerard Cumer EN-EL, Wieslaw Iwanski PH-ESE, Hugues Thiesen TE-EPC, Benjamin Todd TE-EPC, Marc Vanden Eynden BE-CO, Jan Uythoven TE-ABT

Participants Alain Antoine; Magnus Bjork; Vincent Bobillier; Frederick Bordry; Jean-Paul Burnet; Etienne Carlier; Vincent Chareyre; Pierre Charrue; Gerard Cumer; Reiner Denz; Francois Duval; Philippe Farthouat; Fabio Formenti; Brennan Goddard; Eugenia Hatziangeli; Wieslaw Iwanski; Mike Lamont; Nicolas Magnin; Volker Mertens; Valerie Montabonnet; Anastasia Patsouli; Jerome Pierlot; Rudiger Schmidt; Andrzej Siemko; Hugues Thiesen; Yves Thurel; Benjamin Todd; Jan Uythoven; Marc Vanden Eynden; Francois Vasey; Markus Zerlauth

Wednesday, June 20, 2012

09:00 - 09:05 Welcome and agenda *5'*
Speaker: Fabio Formenti (CERN)
Material: Slides

09:05 - 09:10 Reminder on technical motivations, objectives and plans *5'*
Speaker: Volker Mertens (CERN)
Material: Slides

09:10 - 09:20 Introduction to the LBDS system and its functionality *10'*
Speaker: Dr. Jan Uythoven (CERN)
Material: Slides

09:20 - 09:40 The LBDS powering architecture *20'*
Speaker: Etienne Carlier (CERN)
Material: Slides

09:40 - 10:00 The LBDS trigger and re-trigger schemes *20'*
Speaker: Alain Antoine (CERN)
Material: Slides

10:00 - 10:15 Coffee break

10:15 - 10:35 LV safe powering from UPS to client *20'*
Speaker: Mr. Vincent Reymond Chareyre (CERN)
Material: Slides

10:35 - 10:55 WIENER power supplies *20'*
Speaker: Magnus Bjork (CERN)
Material: Slides

10:55 - 11:15 Proposals for LBDS powering improvements *20'*
Speaker: Anastasia Patsouli (CERN)
Material: Slides

11:15 - 11:35 Failure mode impact studies and LV system commissioning tests *20'*
Speaker: Nicolas Magnin (CERN)
Material: Slides

11:35 - 12:00 Reviewers closed session discussion *25'*

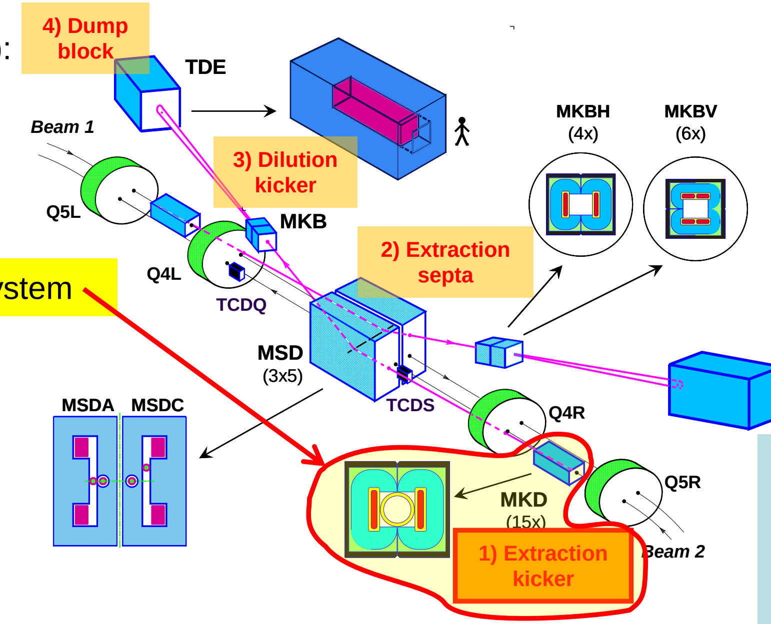
https://indico.cern.ch/conferenceDisplay.py?confId=195055

System introduction 1/4: beam dump process, main components and timing

4 main components compose the LHC beam dump system (per beam):

- 15 extraction kickers (horizontal deflection ~0.27 mrad)
- 15 extraction septa (vertical deflection ~2.4 mrad)
- 10 dilution kickers (4 horizontal, 6 vertical, h/v deflections 0.27 mrad)
- 1 dump block

The LBDS powering review treated only part of the extraction kicker system

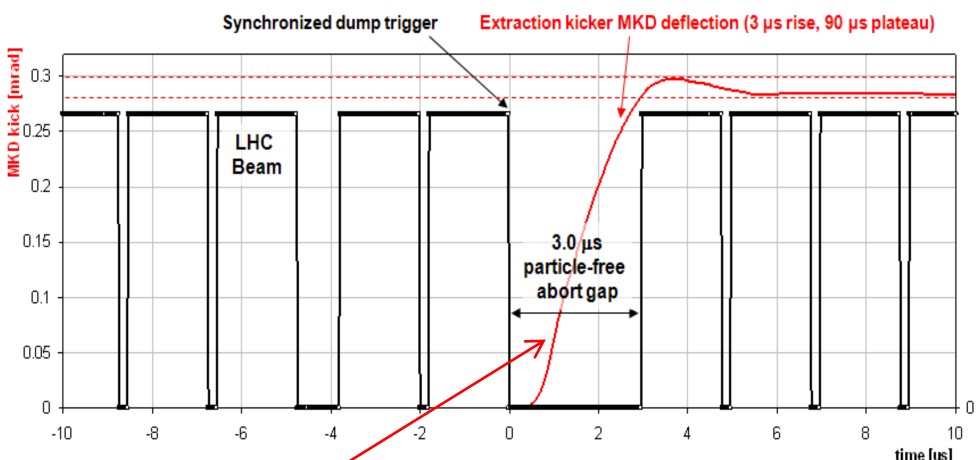


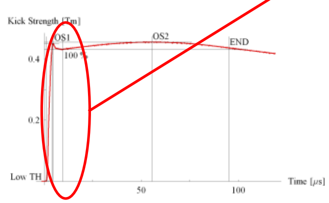
Courtesy J. Uythoven

The dump process **is triggered** by:

– Dump request during normal operation (machine protection for emergencies and timing system for scheduled dumps)

– Internal request in case of system (powering) failure





Beam losses will occur if:

- the dump trigger is not synchronized with the abort gap
- the abort gap contains spurious particles
- the MKD kick is not in tolerance (kick strength depends on beam energy)
- the local orbit is out of tolerance

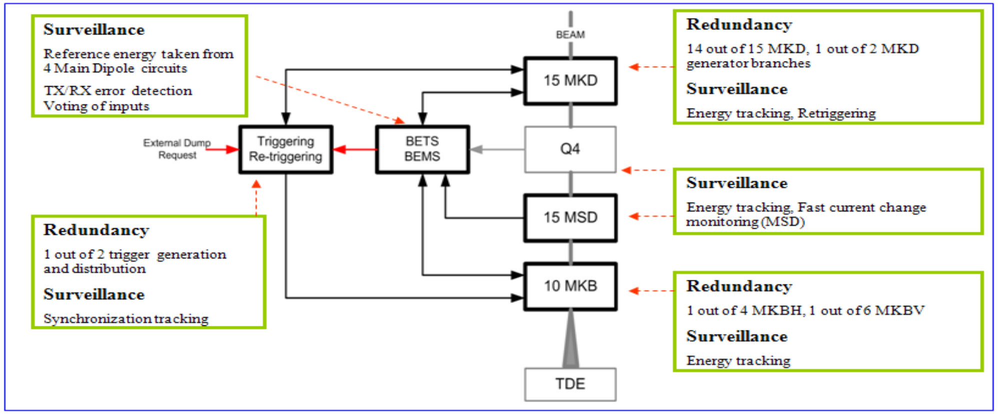
=> Beam losses shall be minimized <=

Asynchronous (forced) dumps are allowed but must be limited (e.g. magnet quenches, electronics SEU)

System introduction 2/4: safety implementation

- The main concern for such a critical system is to operate with the highest reliability:
  - Fault-tolerant architecture by built in redundancy (system continues to run w/o causing unnecessary dumps; problems will be fixed at earliest possible stop)
  - Fail-safe actions and components (responses to failures are aimed at minimizing dangerous consequences)
  - Continuous remote surveillance and diagnostics of important parameters (energy, timing, false triggering)
  - Post mortem analysis (IPOC/XPOC) (inhibits next injection if parameters out of tolerance)

Courtesy J. Uythoven



- Failure Modes, Effects and Critical Analysis detailed studies
  (Ph.D. thesis Roberto Filippini, CERN-THESIS-2006-054)
  - Objective: guarantee SIL4 safety level
  - Studied more than 2100 failure modes
  - Arranged into 21 system failures and related actions

Case studied	Unsafety/year	False dumps/year
Default scenario	2.41×10^{-7} (> SIL4)	4.06
No redundant power triggers	2.34×10^{-6} (SIL4)	3.02
No redundant triggering sys.	4.68×10^{-4} (SIL2)	4.02
14 MKD	0.011 (SIL1)	3.89
No BETS	0.059 (< SIL1)	3.40
No RTS	0.32 (< SIL1)	4.06

SIL(Safety Integrity Level) = define a risk reduction factor
SIL4 highest reduction

Large efforts have been done to try mastering functional failures (avoid asynchronous dumps) …
… but what about UPS power distribution ?

System introduction 3/4: initial powering system scheme (& components considered in this review)

- LBDS is made of 4 large electronics systems:

  SCSS, BETS, TSDS, FASS
- LBDS is fully symmetrical for both Beam1 & Beam2

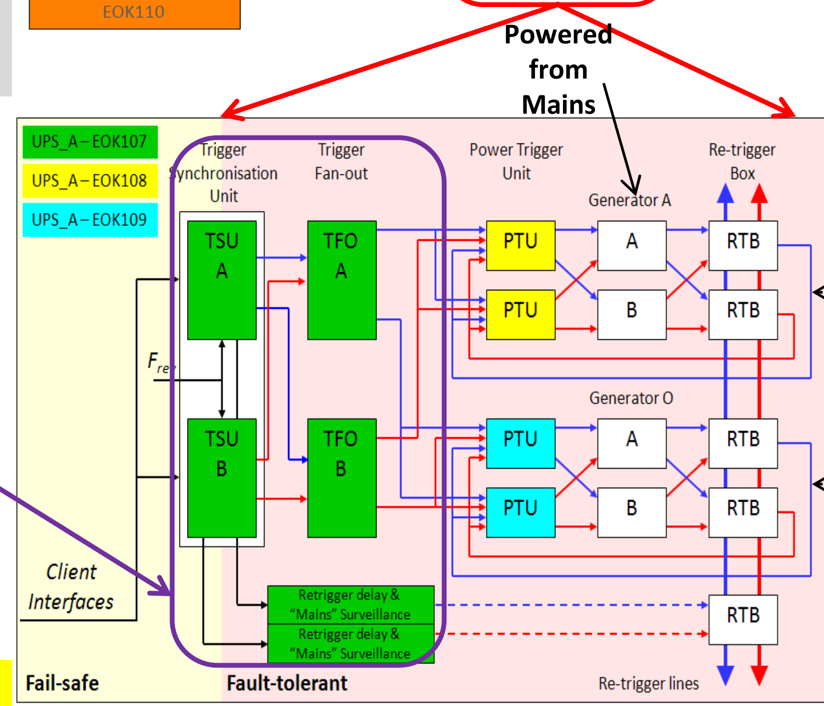
- The LBDS of each beam is connected to a single fully redundant UPS
- Four independent CANALIS are used within each LBDS (EOK107, EOK108, EOK109 & EOK110)

LBDS

State	Strength	Timing	Monitoring
State Control & Surveillance System [SCSS]	Beam Energy Tracking System [BETS]	Trigger Synchronisation & Distribution System [TSDS]	Fast Acquisition & Analysis System [FASS]
Fail-Safe Redundant	Fail-Safe Redundant	Fail Safe Fault Tolerant Redundant	Redundant
	EOK107	EOK107	EOK107
EOK108	EOK108	EOK108	
EOK109	EOK109	EOK109	
EOK110			

EBS11/EBS12	Equipment Powered	Sub-systems
EOK107	7 general purposes racks	BETS, FASS & TSDS
EOK108	7 generators (I to O)	BETS, SCSS & TSDS
EOK109	8 generators (A to H)	BETS, SCSS & TSDS
EOK110	6 general purposes racks	SCSS, BIS, LASS

Sub-system powering discussed in the review



Courtesy E. Carlier

From this review no global conclusions on:
- overall LBDS safety performance
- complete exclusion of other potential unsafe failure modes

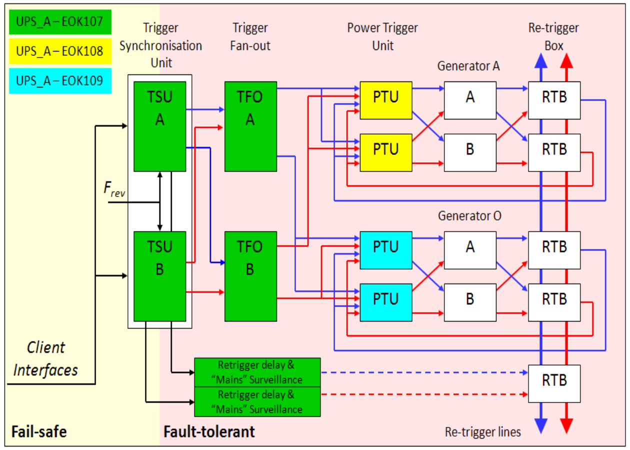
System introduction 4/4: power hold-on feature

In ultimate failure cases of total power loss

- capacitors provide energy required to distribute the dump request up to the kicker HV generators
- energy is validated before a beam permit signal is issued

Courtesy E. Carlier

System	Nominal (full performance)	Maximum (reduced performance)	Effect after hold-on
Trigger Synchronisation	150ms	200ms	
Trigger Fan Out	100ms	125ms	Missing trigger pulses after 100ms
Power Trigger Unit	100ms	175ms	Linear power supplies Modification of generator turn-on delay after 100ms
HV Generator	100ms	150ms	Kick strength outside BETS window after 100ms



Hold-on working principles:

- In order to **execute a <u>synchronous dump,</u>** the **fail-safe** part of the system must **react faster** than the hold-on time of the **fault-tolerant** part**.**
- If **no synchronous dump** is executed **before the end of the nominal hold-on** time, an **<u>asynchronous dump</u>** is executed (Retrigger delay unit)

Hold-on safety effectiveness:

the power hold-on function shall rely on the capacitor's reliability

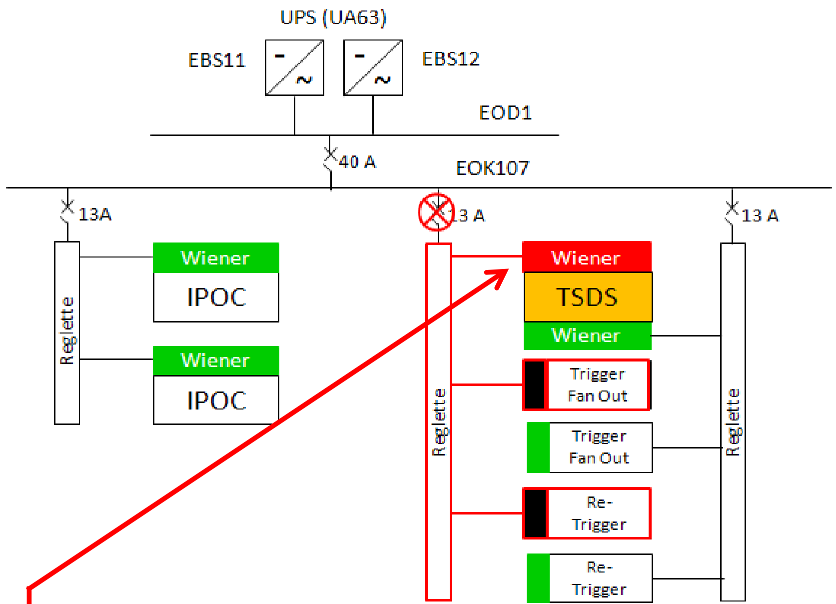
(then what about: ageing? damage? surveillance? preventive maintenance?)

and on the reaction timing of some parts of the system (details beyond of review scope)

First power incident (February 2012)

Courtesy E. Carlier

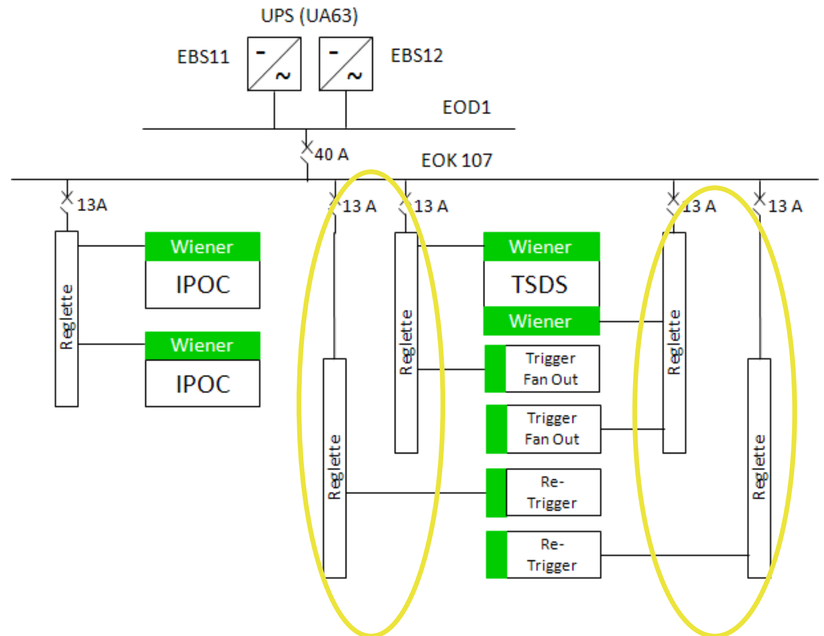
Before mitigation (initial powering system)



	Event	Consequence
1	Failure of one WIENER power supply within the redundant TSDS VME crate.	TSDS crate still working properly on its redundant power supply.
2	Trip of rack 13A circuit breaker.	Loss of 1 re-trigger crate and 1 trigger fan out.
3	Re-trigger crate has detected its loss of powering.	Start 100ms delay before generation of asynchronous dump.
4	SCSS detects the loss of 1 re-trigger crate and generates a dump request (internal failure).	Dump request asynchronous with Master PLC cycle. (26ms [min], 45ms [typ], 77ms [max])
5	TSDS receives SCSS dump request and issues the dump trigger.	Synchronous dump with 50% loss of redundancy.
6	100ms after the trip of the circuit breaker, re-trigger unit generates a dump trigger (mains surveillance interlock).	Asynchronous dump.

Synchronous or asynchronous dumps

After mitigation (Xmas break 2012)



Connect re-trigger crates and TSDS WIENER power supplies on separate “reglette”

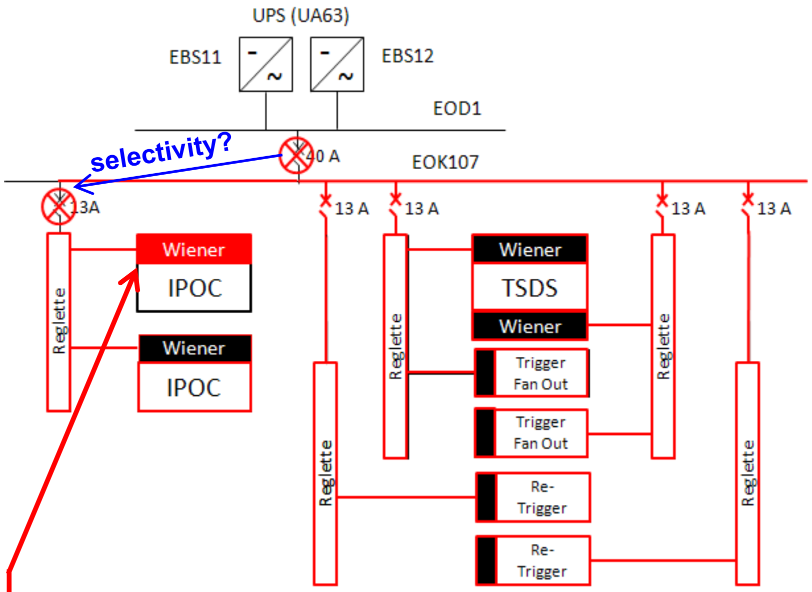
→ Surveillance of EOK107 line by independent connections of re-trigger crates (better partitioning)

→ Avoid generation of asynchronous dump (by re-trigger crate) in case of partial loss of TSDS powering

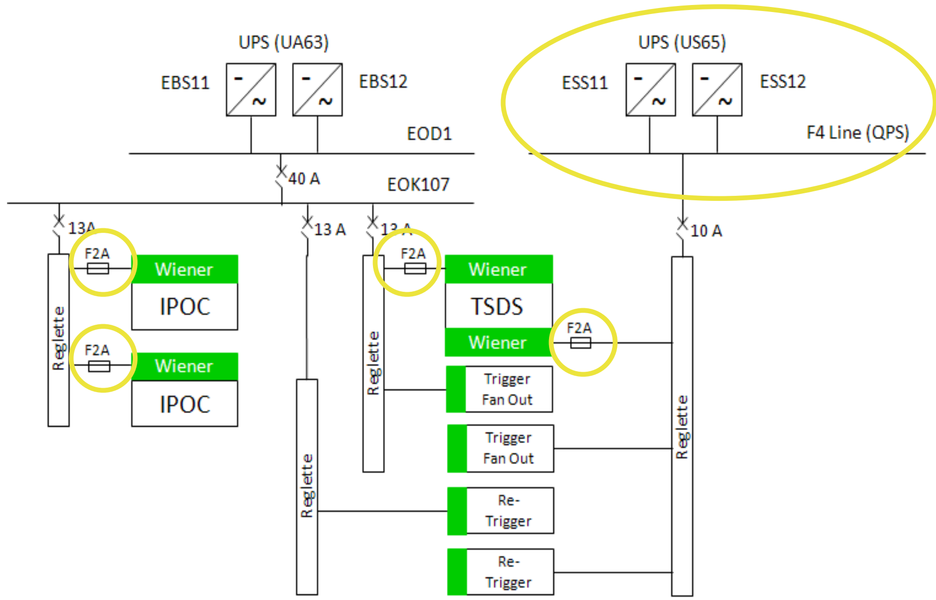
Second power incident (April 2012)

Courtesy E. Carlier

Before mitigation



After mitigation (TS1 April 2012)



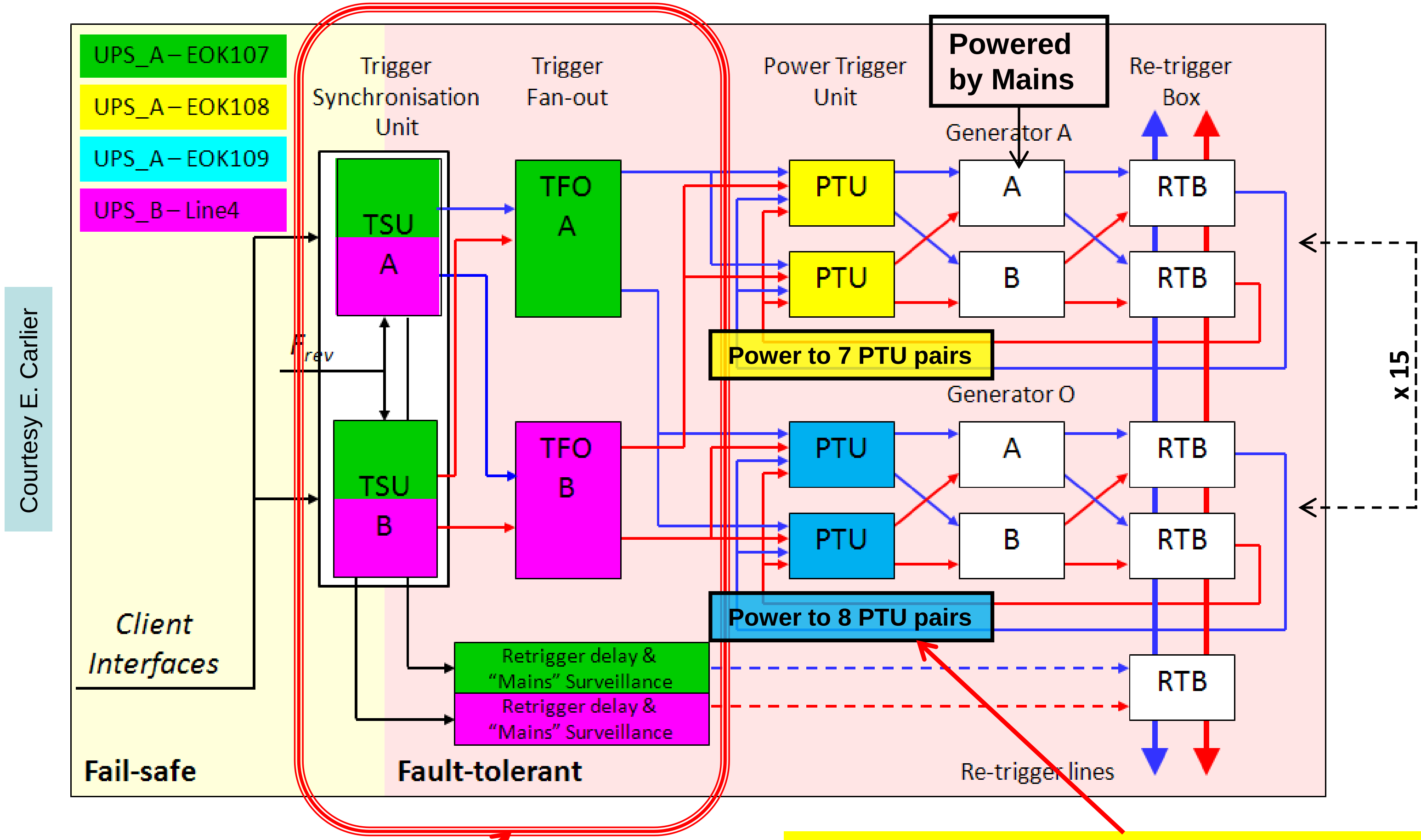
1	Failure of one WIENER power supply within one IPOC cPCI crate	Loss 50% of post-mortem data.
2	Trip of IPOC rack 13A circuit breaker	Loss of redundant IPOC cPCI crate. No post-mortem data available anymore.
3	Trip of EOK107 40A circuit breaker.(Incorrect balancing between phases induced by WIENER power supply failure)	Full loss of TSDS (both redundant power supplies), loss of both re-trigger crates & loss of both trigger fan-out crates.
4	TSDS issues an internal dump request induced by the detection of the loss of the BRF.	Synchronous or Synchronous-Asynchronous dump. **(depending on hold-on vs. reaction time)**
5	SCSS detects the loss of 2 re-trigger crates and generates a dump request (internal failure) **(via Master PLC)**	Internal failure dump request cannot be executed by TSDS due to loss of powering.
6	100ms after the trip of the 40A circuit breaker, re-trigger units generate a dump trigger.	Asynchronous dump.

Loss of full system

-> Connect 1 re-trigger crate, 1 trigger fan-out crate and 1 TSDS WIENER power supply to another UPS (F4 Line – QPS) to implement power redundancy

-> Add fast 2A fuse to WIENER power supply mains connections to improve selectivity (should stand inrush currents)

Present powering system and components

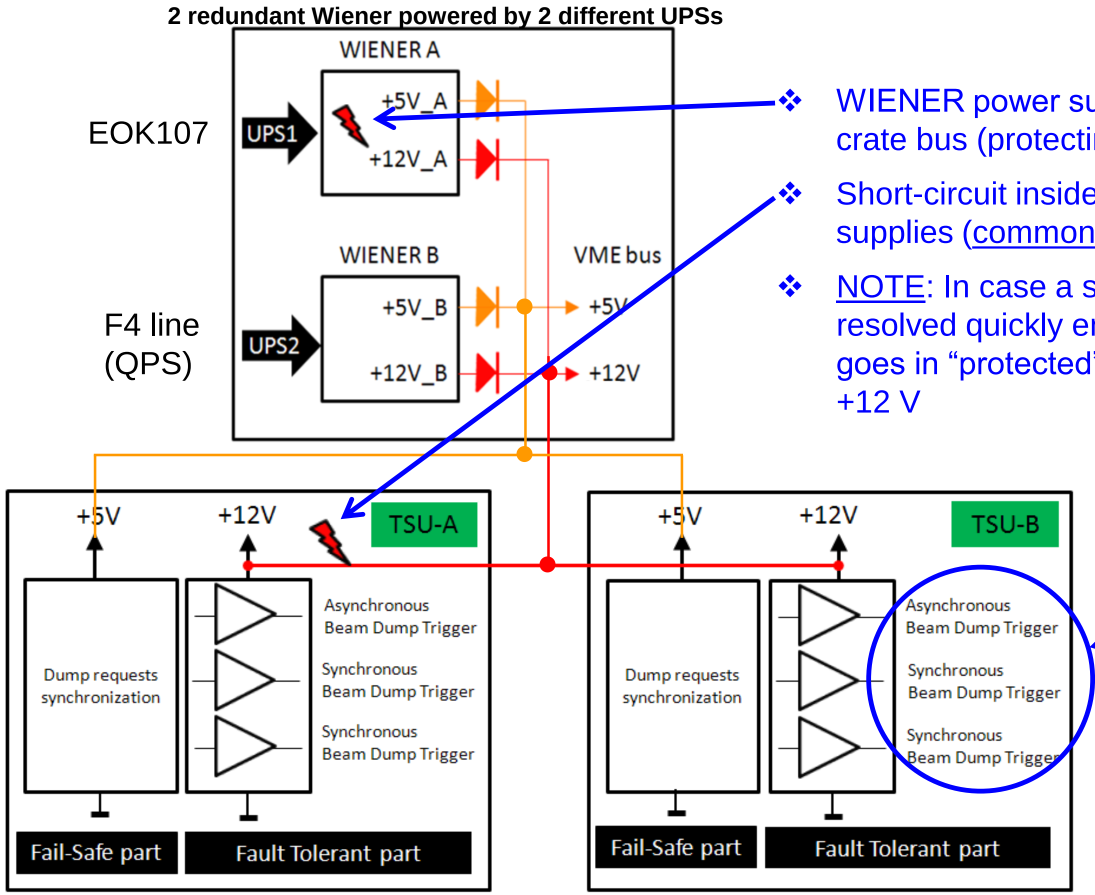


This part of the system has redundant power through 2 UPSs

PTUs are not configured with fully redundant power (however not based on Wiener power supplies)
Not in the scope of this review

Best fixes <u>for the main timing part of TSDS</u>
have been implemented during a short LHC technical stop

Additional risk discovery: +12 V common mode coupling in TSU crate



- WIENER power supply internal failure doesn't affect VME crate bus (protecting diodes)
- Short-circuit inside VME crate affects both WIENER power supplies (common mode failure coupling)
- NOTE: In case a short-circuit on either +12 V or +5 V is not resolved quickly enough (within ~50ms), the Wiener supply goes in "protected" mode and switches OFF both +5 V and +12 V

- All trigger output driver stages of each TSU powered from same +12 V

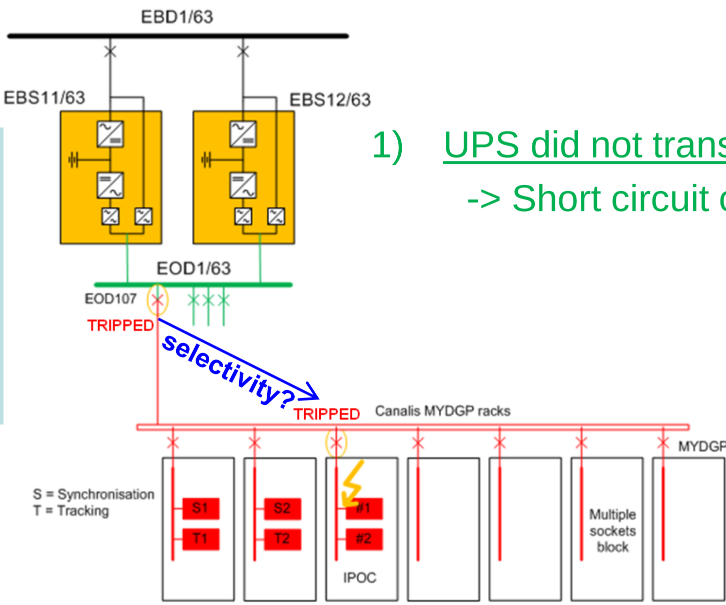
- **Short-circuit** on the +12 V results in the **complete loss of triggering capabilities** (synchronous & asynchronous) of **both** TSUs.
- **"Long duration" short circuit** on +5 V results in **complete switch OFF of +12 V**

Broken rule of fault tolerance

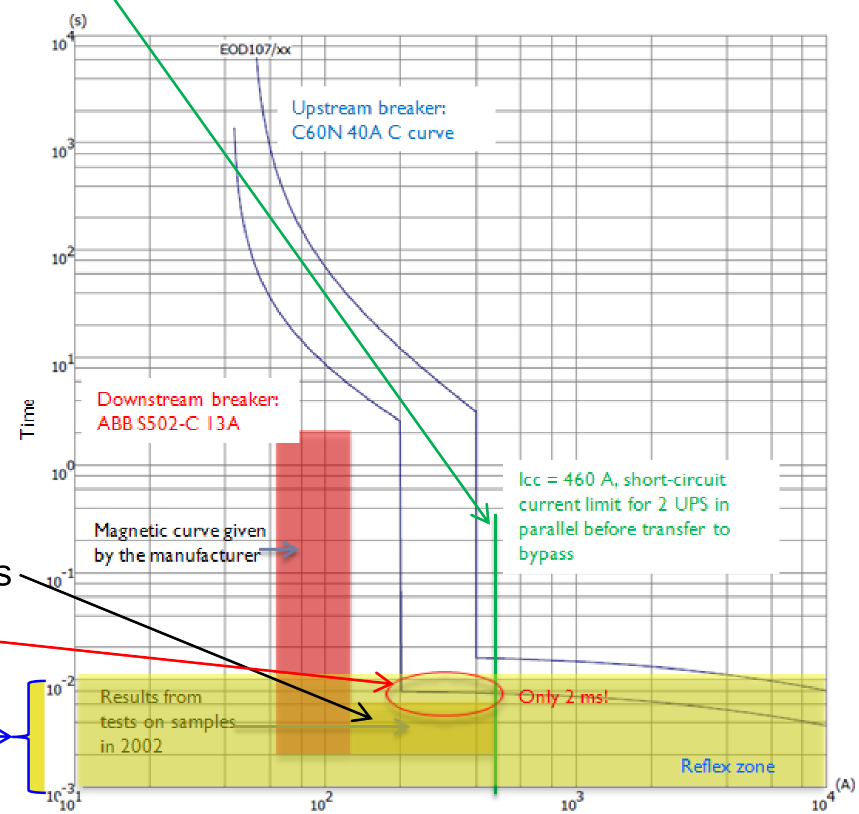
Mitigation action performed: external survey of +12 V crate line and trigger asynchronous dump via retrigger system

UPS power distribution selectivity analysis of second power incident

Courtesy V. Chareyre



1) UPS did not transfer to bypass
-> Short circuit current < 460 A



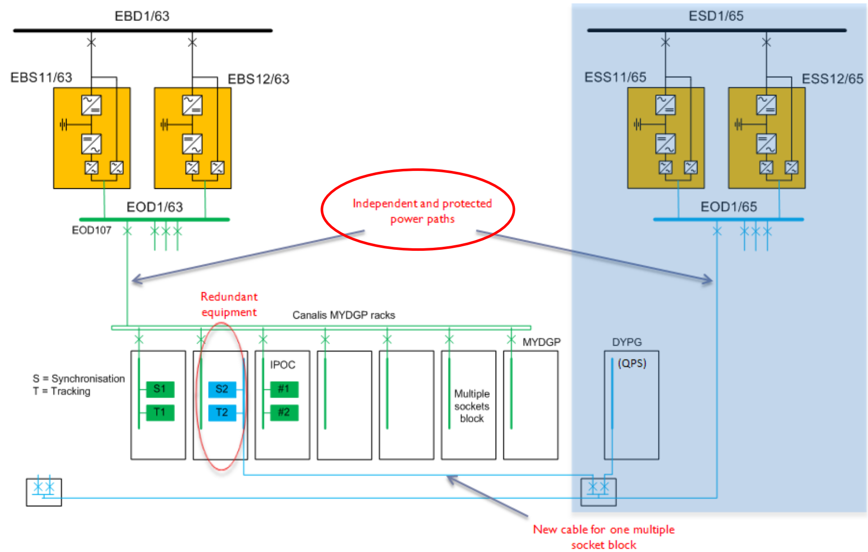
2) Both breakers tripped

- Two different circuit breaker brand names
- ABB S502-C 13A tripping curve from sample tests
- Only 2 ms between the curve of the upstream breaker and the ABB tripping zone (estimated!)
- <10 ms: breakers working in the ‘reflex zone’ (unpredictable selectivity)

These two circuit breakers cannot guarantee selectivity under all load conditions

Present powering system mitigation

Courtesy V. Chareyre



<u>TSDS equipments powered by 2 different UPSs</u>

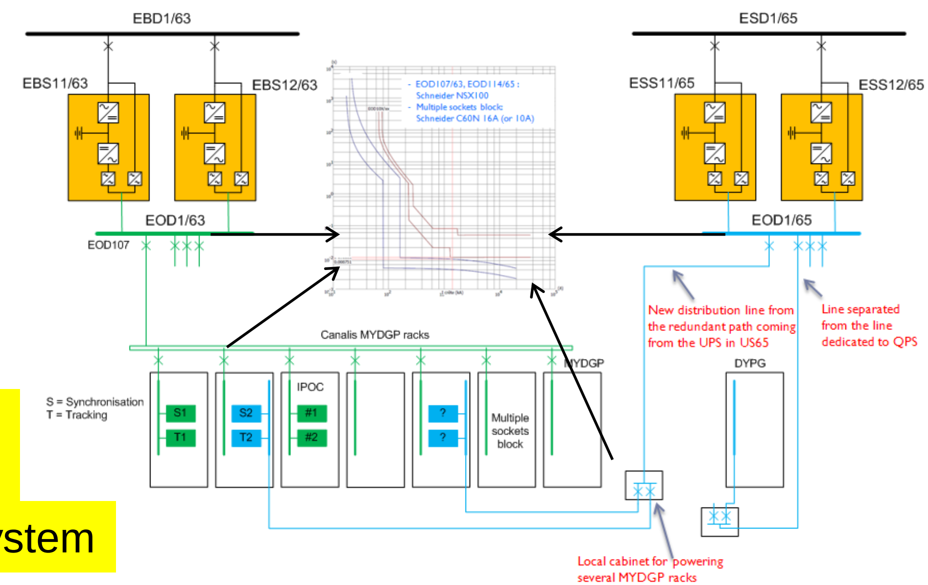
- Quick fixings implementing good redundancy for TSDS

<u>However:</u>

- Selectivity problem is not fully addressed
- Attention to be paid at QPS client

Proposal for LS1

1) QPS and other clients on separate power lines for better protection (partitioning)
2) More reliable breaker selectivity (guaranteed by same manufacturer - Schneider)
3) Optimal matching of breaker types (NSX100 and C60N 16A or 10A)
4) <u>Power distribution further improved inside racks</u> (next slide)

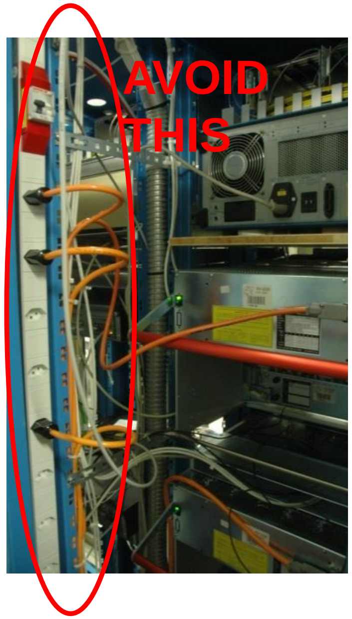


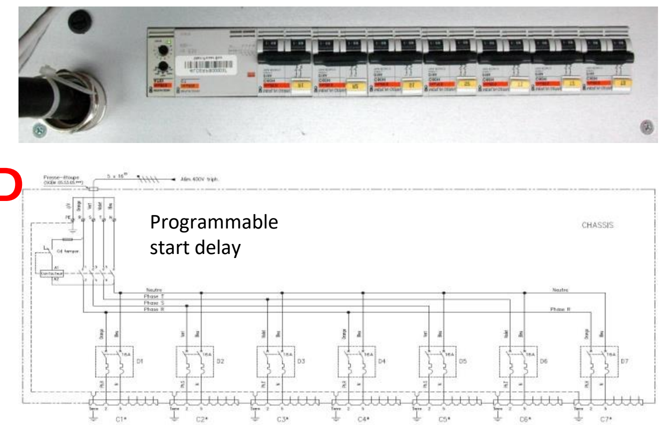
Implementation of fully double redundant power distribution

Improve selectivity and check it in the real system

A good example of power distribution inside racks (LHCb)

Courtesy M. Bjork





- Individual circuit breakers per crate power supply for best power partitioning
  - 16 A recommended for full load
  - 10 A sufficient as maximum input current of our power supplies is 6,5 Amperes (VME)
- Special power sockets to prevent unauthorized accesses
  - e.g. Burndy connector with 10 A pins are acceptable
  - (the pins can handle instantaneous short circuit current, then the circuit breaker reacts)

Individual power supply protection inside racks by means of crate power distribution boxes
Design already qualified by LHCb

What about the Wiener power supplies failures?

The Power Factor Corrector (PFC) is the weak point

- To protect the PFC the manufacturer introduced the by-pass D2
- Extensive tests done in PH-ESE did not confirm the modification effectiveness of D2 (not been able to reproduce the failure)
- Failure rates are ~2%/year, which is inside manufacture predictions

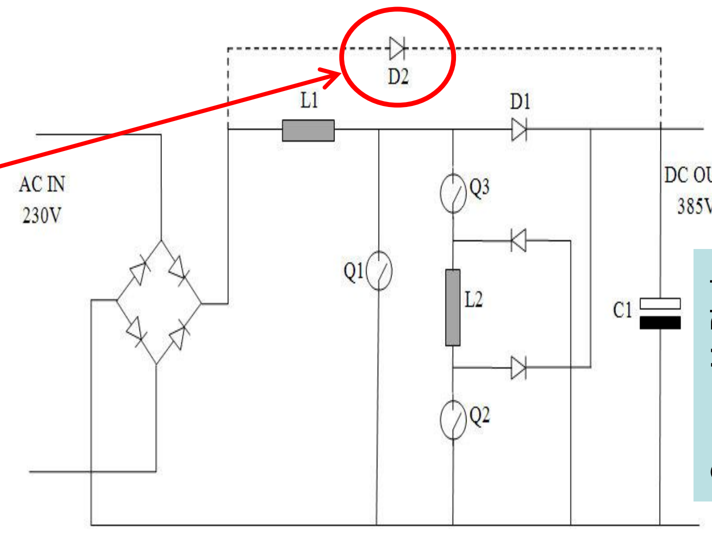


Figure 1: Simplified diagram of the PFC

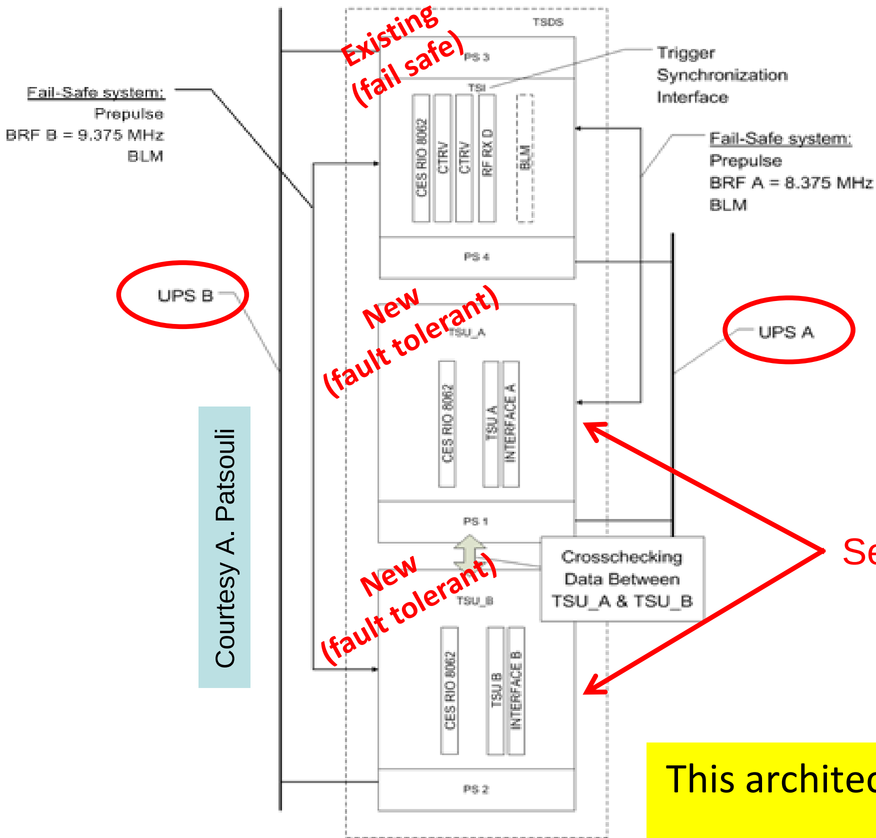
Courtesy M. Bjork

The reasons of the PFC failures in experimental zones still remain unclear

- Wiener failures could lead to significant operation downtime in case of critical LHC applications
- BE-CO is investigating the ELMA CPA500 power supply
  - it is equipped with PFC,
  - has soft-start and low inrush current
  - can be used in redundant configuration

Join efforts of BE-CO, TE-EPC and PH-ESE for qualifying new power supply solutions

Proposed solution for the TSU +12 V common mode failure



Separate +12 V and +5 V power lines

- TSDS implementation within 3 separate VME crates:
  - 1st Crate with single power supply hosting **TSU_A**
  - 2nd Crate with single power supply hosting **TSU_B**
  - 3rd Crate with Redundant Power Supply hosting the **T**rigger **S**ynchronization **I**nterfaces (BRF, BLM, pre-pulse, …)

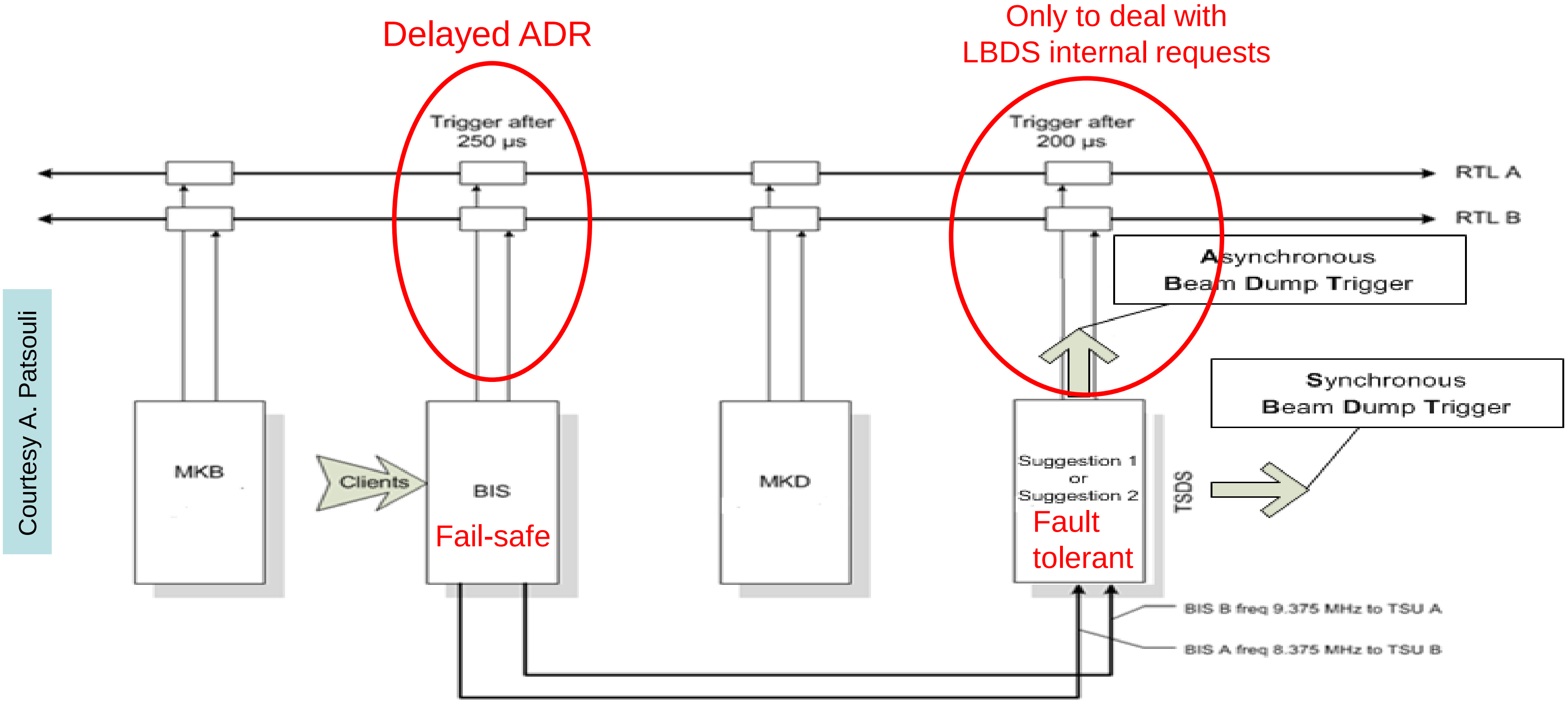
This architecture is a solution to the +12 V common mode coupling

TSI crate is still a single point of failure, nevertheless this belongs to the fail safe area (synchronous dump)

Study correct implementation of fail safe and fault tolerant concepts for <u>whole</u> LBDS

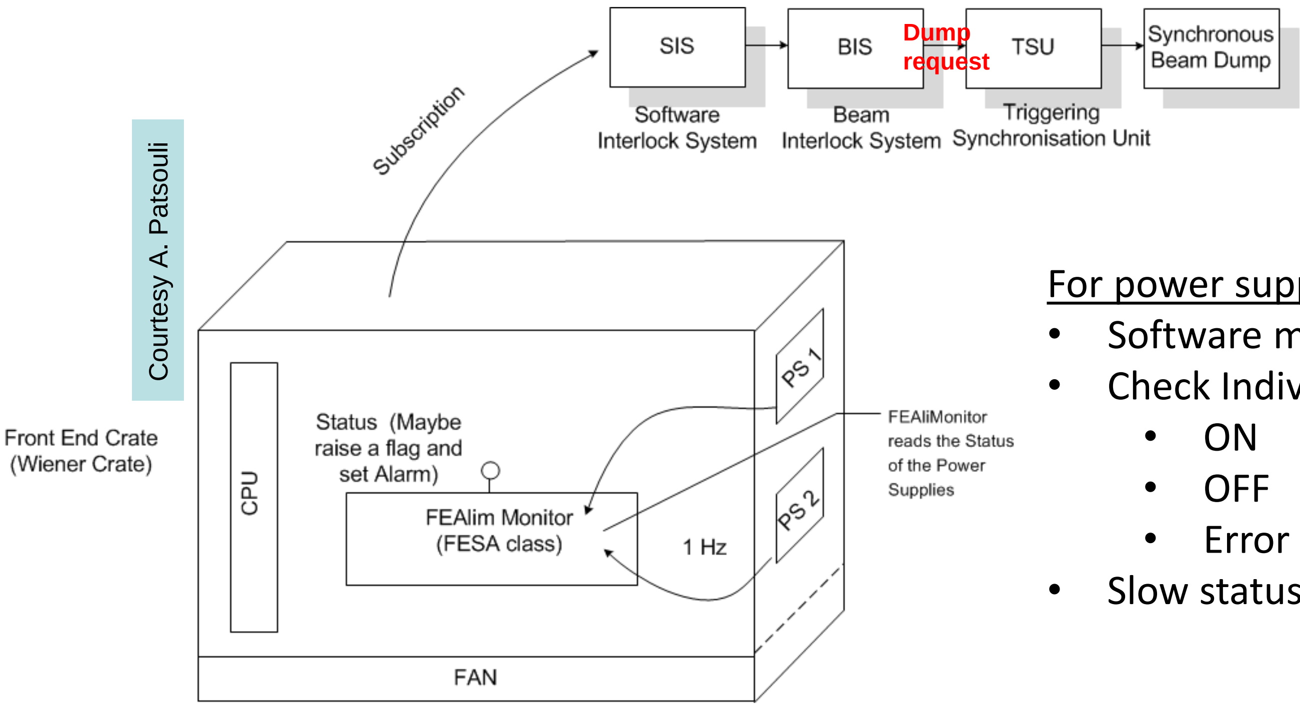
Proposal for fail-safe asynchronous beam dump through BIS

- Injection from BIS of **A**synchronous **D**ump **R**equest into the **LBDS** re-triggering lines (RTL A and B)
- The **D**ump **R**equest should be delayed 250µs after detection of the **BIS** loop opening
- BIS triggers synchronous dump request into LBDS (< 250µs)



BIS to provide fail–safe ultimate asynchronous dump protection

Proposal of surveillance of the redundant features



<u>For power supplies:</u>

- Software monitor
- Check Individual Status
  - ON
  - OFF
  - Error (to be defined)
- Slow status update rate

<u>For all critical DC voltages:</u>

- External surveillance (preferred to internal hardware)
- Use fail-safe criteria
- At crate level

Synchronous dump as soon as a redundant feature is lost to minimize operation period with high risk

Power failure tests

Courtesy N. Magnin

Systems	MAIN	UPS-A	UPS-B	Function
15 MKD HV PS	X			LBDS operation
15 MKD PLC		X		LBDS operation
15 MKD PTU		X		LBDS operation
LBDS MASTER PLC		X		LBDS operation
TFO-A		X		LBDS operation
TFO-B			X	LBDS operation
RTU-A		X		LBDS operation
RTU-B			X	LBDS operation
TSU-A FEC		X		LBDS operation
TSU-B FEC			X	LBDS operation
TSI FEC		X	X	LBDS operation
BETS FEC		X	X	LBDS operation
IPOC - TSU FEC		X	X	LBDS diagnosis
IPOC1 - MKD FEC		X		LBDS diagnosis
IPOC2 - MKD FEC			X	LBDS diagnosis

New studies initiated

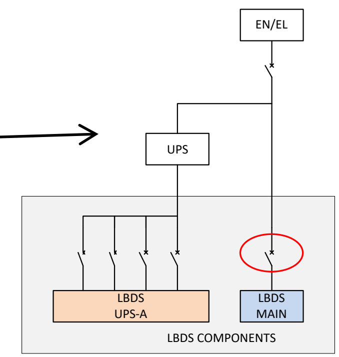
- based on configuration with:
  UPSA + UPSB + Triplicate TSDS crate
- 7 cases of power failures studied

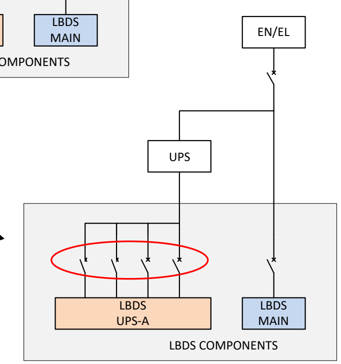
An example of UPSA failure table

Loss of operation devices -> triggering synch dump
Partial loss of diagnostics

Practical tests

- MAIN failure:
  - *Already done in 2006 -> Synch dump*
- UPS-A failure:
  - *Already done in 2006 (manually = not real UPS failure ?) -> Synch dump*
- UPS-B failure:
  - Never done so far !
- UPS-A + UPS-B failure
  - Never done so far !
- TOTAL failure (Main + UPS-A + UPS-B)
  - Never done so far !





Reference document in final architecture listing all failure predictions and on-line test validation

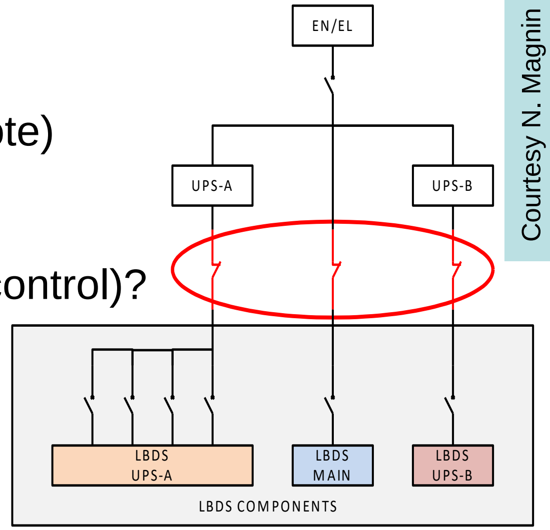
LBDS power commissioning tests

Many questions are still open for discussion:

1) Perform remotely (CCC) or local (point 6) or combine both?

2) How to maintain the diagnostics available (especially in remote)
(SCSS, TSU-FESA, IPOC-TSU, IPOC-MKD, XPOC, …)

3) How to perform power failures (additional breakers, remote control)?



Courtesy N. Magnin

4) How to avoid shutting down other LHC protection systems?

5) When to do it?
at end of LS1 -> yes, complete check, test procedure t.b.d.
on regular basis -> winter shut down, technical stops
-> define appropriate time slots for LBDS safety tests

Commissioning procedures to be upgraded and discussed in MPP
Reduce risk of introducing new elements for tests

Conclusions

- Quickly implemented solutions are appropriate and fulfill the immediate needs
- Additional coordinated global actions are recommended as indicated in the following summary table (to be planned in view of LS1)

	Recommendation	Main purpose	Central action on
1	Use BIS for triggering a delayed asynchronous dump	Provide ultimate protection in all cases where the LBDS synchronous triggering system fails	TE-ABT TE-MPE EN-EL
2	Modify UPS electrical distribution and upgrade circuit breaker technology	Implement a.c. power fault-tolerance by redundant powering and assure selectivity quality (from UPS up to electronics crates)	EN-EL BE-CO
3	Modify TSDS architecture	Implement d.c. power fault-tolerance by redundant powering	TE-ABT
4	Survey the power availability of all power converters and inside crates	Provide prompt alert in case of lost power redundancy and reduce time of operation at high risk by scheduling a synchronous dump	TE-ABT BE-CO
5	Study alternatives to Wiener supplies	Remove the cause of the power supply weakness	BE-CO (+ support of TE-EPC & PH-ESE)
6	Actualize the LBDS system safety study and define validation criteria	- Analyze the impact on reliability of changes done on LDBS with a full system view - Evaluate consequences of all possible causes of power failures - Define qualification tests and commissioning procedures	TE-ABT MPP

NOTE: the TE Electronics Coordination can provide background for technical discussions and follow-up

Thank you for your attention !