Technical Review of the Trigger Synchronisation Unit of the LHC Beam Dumping System

A. Antoine, C. Boucly, E. Carlier & P. Juteau (CERN)

S. Desjardins & N. Krohmer (STUDIEL)

Outline

- Context
- Objectives
- Content
- Results
- Actions
- Summary

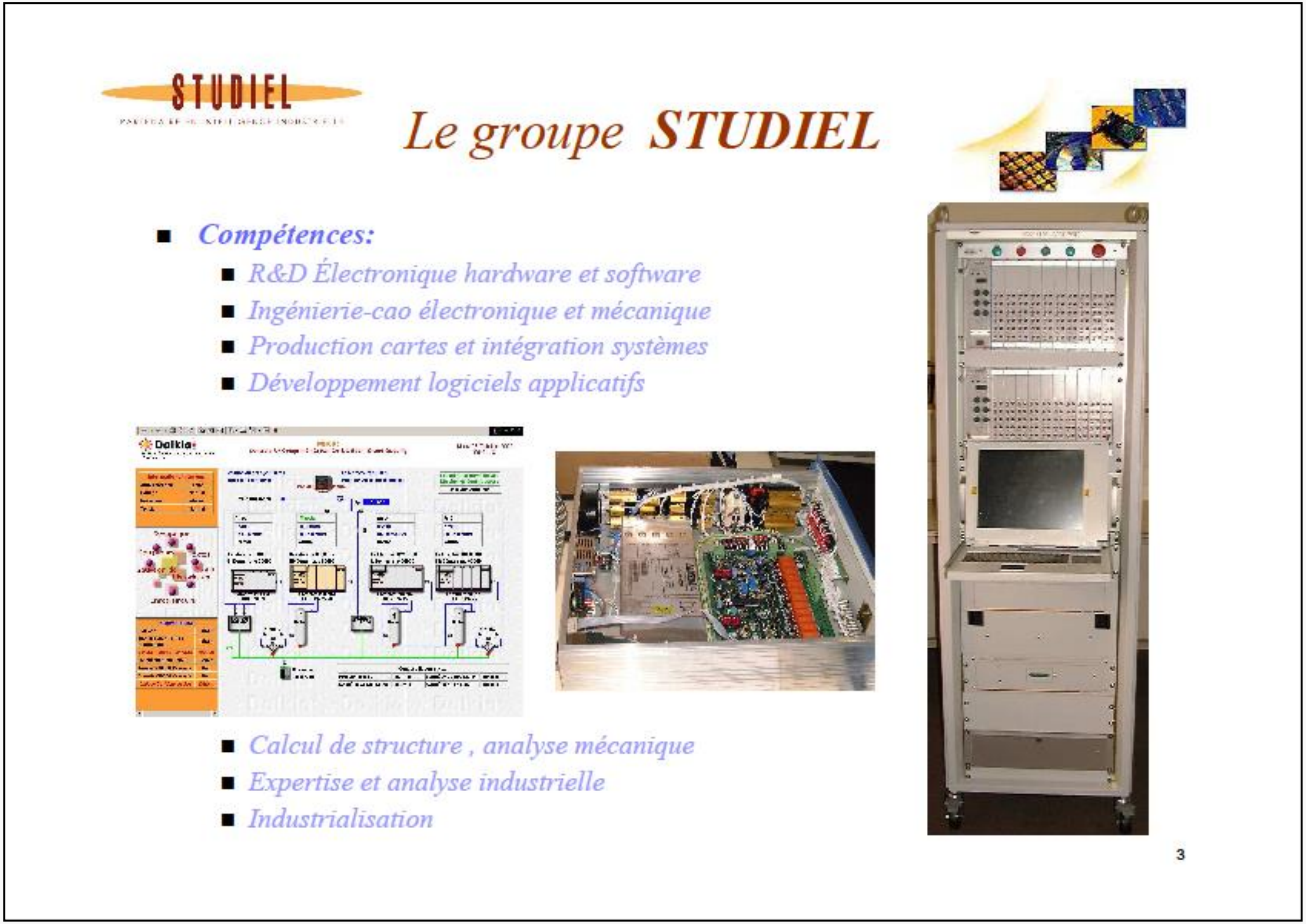
Initial conditions

- The LHC Beam Dumping System (LBDS) and, in particular, its Trigger Synchronizations and Distribution System (TSDS) that includes the Trigger Synchronizations Unit (TSU) have been internally reviewed in January 2008.
- One of the of the recommendation of this audit was *"The Board would like to encourage the LBDS team to conduct the recommended full review of the FPGA code and to deploy a FPGA test bench".* Under this statement , the TSU and its embedded firmware written in VHDL is included.
- Two actions have been triggered by this recommendation:
  - Organization of an external review by an external independent firm (contract awarded through an Invitation to Tender) ,
  - Development of a test bench with automated test sequences.

Objectives

- The validation of the correct implementation of the functional requirements,
- The verification of the pre-series performance,
- The identification of possible hardware and/or software anomalies,
- The recommendation of possible improvements,
- The proposal of guidelines of possible maintenance procedures for the embedded software.

STUDIEL



STUDIEL

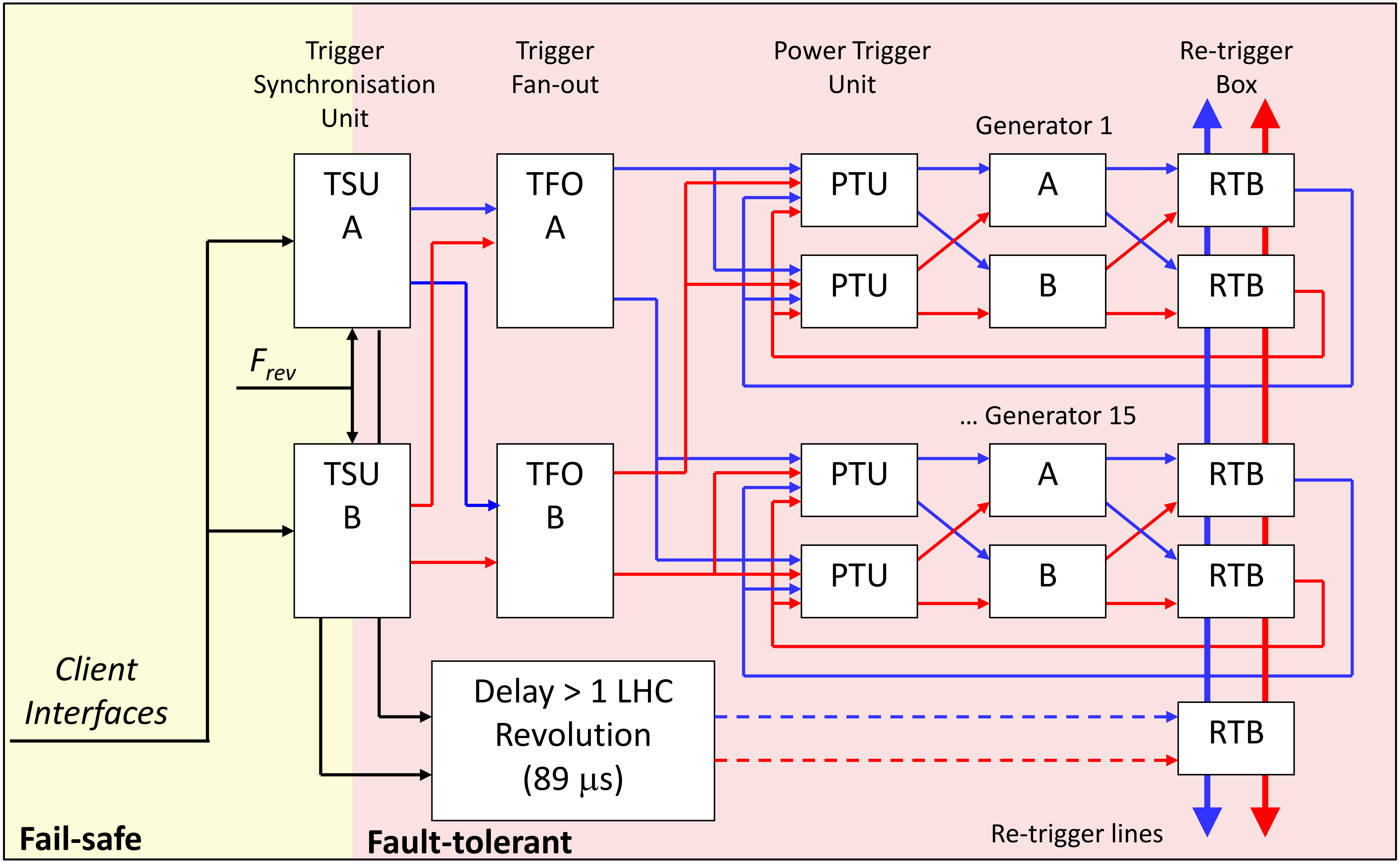
PARTENAIRE EN INTELLIGENCE INDUSTRIELLE

Le groupe STUDIEL

- *Compétences:*
  - *R&D Électronique hardware et software*
  - *Ingénierie-cao électronique et mécanique*
  - *Production cartes et intégration systèmes*
  - *Développement logiciels applicatifs*
  - *Calcul de structure , analyse mécanique*
  - *Expertise et analyse industrielle*
  - *Industrialisation*

3

LBDS Trigger Synchronization & Distribution



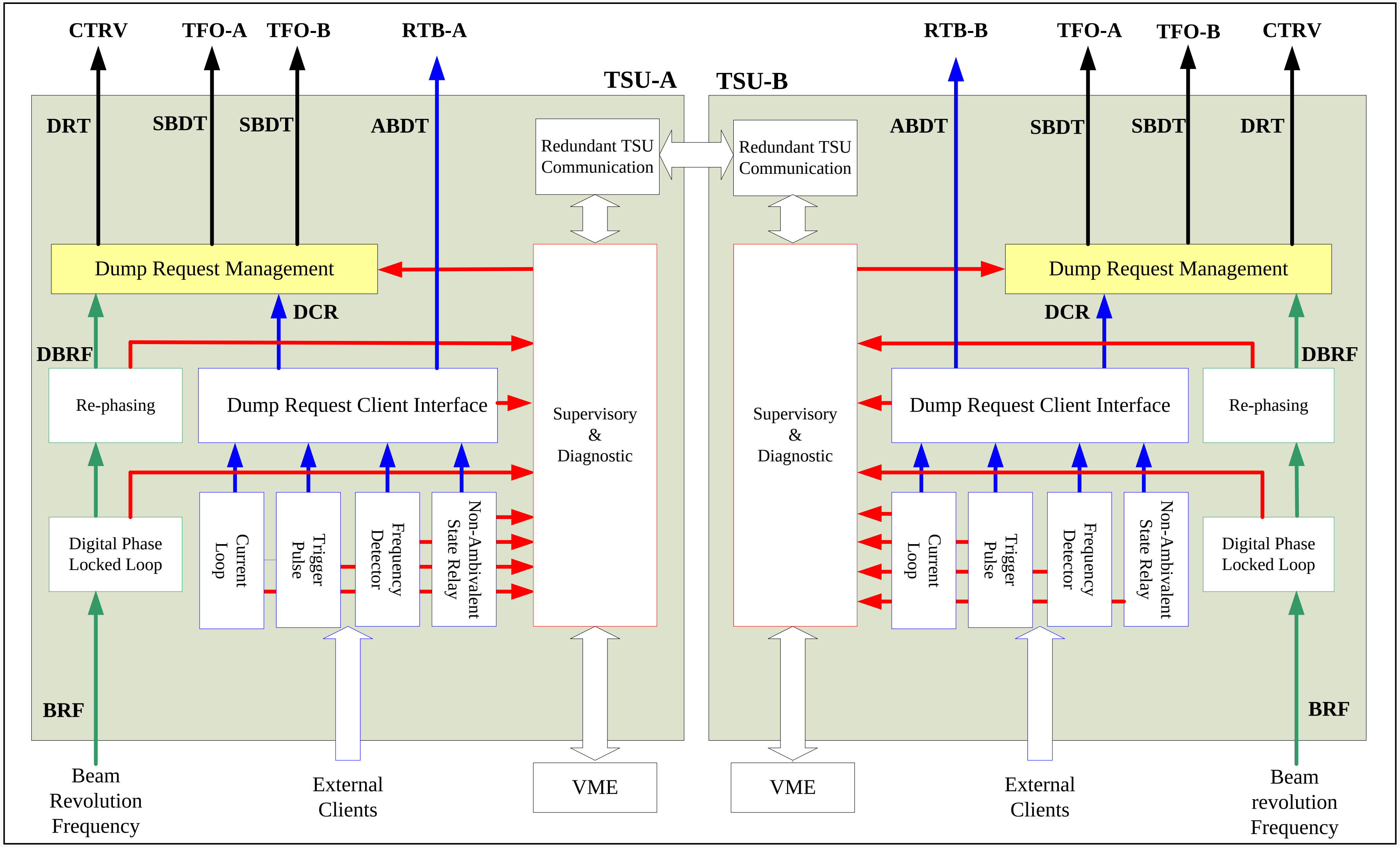
Trigger Synchronization Unit

Review Content

- IN
  - TSU functionalities
  - TSU hardware
  - TSU embedded software
  - TSU redundancy
- OUT
  - TSDS architecture
  - TSDS interface
  - TSDS monitoring
  - Trigger distribution
  - Re-trigger distribution

Trigger Synchronization Unit

Block Diagram



Organization

- 3 phases:
  - The requirement review,
  - The design review,
  - The hardware & software review.
- At the end of each phase:
  - An executive summary of the phase,
  - A summary of the technical issues reviewed, still open and not considered.
- 6 months duration & 3 meetings:
  - One kick-off meeting at the beginning of the review,
  - One progress meeting in the middle of the review,
  - One closeout meeting at the end of the review.
- Review entirely based on specification (i.e. no hardware tests)
- Review fully documented in EDMS
  - https://edms.cern.ch/document/1059444/1

Review Criticality Levels

1	Major failures that can induce a dysfunction considered as serious
2	Failure that can affect a functionality considered as non-critical or with a low probability to occur
3	Minor failure with no risk for the global functionality
4	No failure risk identified

Phase 1 – Requirements Review

Ascertain the adequacy of the requirements in defining the characteristics and the functionalities of the TSU module

- **Understandability** – Is each individual requirement and the set of requirements understandable?
- **Completeness** – Do the requirements describe completely the requirements of the module? Do they cover quality and performance characteristics?
- **Verifiability** – Can each of the requirements be verified?
- **Consistency** – Are the requirement consistent?
- **Traceability** – Will the requirements be traceable throughout the development life cycle?
- **Testability** – Can each of the requirements be tested?

Phase 1 – Requirements Review

- Reverse engineering
  - Set up of a high level architecture of the TSU on the basis of a low level analysis of the hardware and embedded software
- Hierarchical analysis with identification of dependencies
- Establishment of a requirements verification matrix (requirement Vs implementation)

🟩	All requirements are taken into account
🟩	All requirements are covered by at least one sub-module (hardware and/or software
🟩	Links between modules are coherent
🟩	Hardware architecture is correct, well structured and don't need to be modified
🟨	Architecture seems sometime too complex for the required functionalities to be implemented. Simplification possible

Phase 2 – System Design Review

Ensure that the TSU module conceptual design meets baseline-required functionalities and that its performance levels, typically reliability and availability, are within specification.

- The conceptual design of the TSU module,
- The DPLL design and implementation,
- The TSU module redundant operation,
- The post-operational check diagnosis,
- The arming sequence,
- The ready state management.

Phase 2 – System Design Review

11 requirements out of 200 have been identified as not properly implemented

🟥	One is critical and affects the redundancy of the system
🟧	Four are minor but can affect availability of the system
🟨	Two are linked to external conditions not taken into by the TSU itself but covered by the LBDS system
🟨	Four are due to incomplete functional specifications

Phase 2 – System Design Review

FAIL-04	In case of internal failure, TSU: • Generates an ABDT signal in phase with the occurrence of the internal failure detection (INTDR), • Sends an internal dump request to the redundant TSU, and • Inhibits the internal generation of the SBDT signal.

🟥	In case of internal failure, only the redundant TSU generates an ABDT… The faulty TSY doesn't generate an ADBT

FSM-08	Transition from NOT_READY to READY generate neither ABDT nor SBDT signals.
ARM-008	Unsuccessful execution of an ARM sequence don't generate ABDT and SBDT signals
DRM-02	ABDT, SBDT and DRT signals are generated only when the TSU state changes from READY to NOT_READY.

🟨	Possibility to generate dump triggers during the execution of an arming sequence (transition of NOT_READY to READY state) if a dump request is issued one clock tick before the end of sequence

Phase 2 – System Design Review

DRM-01	TSU generates ABDT, SBDT and DRT signals upon reception of dump request.

🟧	Possibility of a spurious dump trigger at power-on due to undefined state of trigger feedback flip-flops;

DRC-01	BISDR, BETSDR, BLMDR, LBDSDR, TIMDR, INTDR and REDDR inputs are active only when TSU is in REMOTE.

🟨	Uncontrolled conditions in the TSU internal state machine when LBDS is operated in LOCAL mode that keeps open the possibility to generate dump triggers on a request of an external client

CTRL-03	In case of discrepancy of the LOCAL/REMOTE input signal, TSU control is assumed to be in LOCAL.

🟨	If the system is identified neither in LOCAL nor in REMOTE (cable disconnected), TSU control is undefined

Phase 2 – System Design Review

DRM-05	ABDT signal is generated in phase with the TRUE to FALSE transition of DRC.
DRM-06	ABDT signal phase offset error with TRUE to FALSE transition of DRC is < 100ns.
DRM-07	DRT signal is generated in phase with the TRUE to FALSE transition of DRC.
DRM-08	DRT signal phase offset error with TRUE to FALSE transition of DRC is < 100ns.

🟨	ABDT & DRT signal are not generated in phase with the TRUE to FALSE transition for BIS, BETS and LBDKS clients due to unpredictable detection duration

Phase 3 – Hardware & Software Review

Perform an in-depth analysis of the TSU module electronic and its embedded software.

- The design of the electronic circuits:
  - Powering,
  - Client's interface front-end circuits including the Beam Interlock Controller System Optical Daughter Module (CIBO board),
  - Dump request combinatorial logic,
  - Core logic (CPLDs and FPGA),
  - Diagnostic, VME, slow control and redundant communication interfaces.
- The embedded VHDL software:
  - Client's detections,
  - Synchronization,
  - State control,
  - VME interface.

Phase 3 – Hardware & Software Review

Hardware

🟥	Unprotection / un-polarization of unused inputs in some logical circuits. *Risk of perturbation to used part of the circuit in case of failure.*
🟥	No protection of principal powering circuits (+5V, +12V) against internal failure in the board (short-circuit). *Failure can propagate outside the board and affect up to the complete crate (loss of redundancy).*
🟥	Components sized for pulse mode operation but not for DC operation *Risk to destroy synchronous trigger output circuit in case output signal is maintained at a high level.*
🟥	Under-sized or inappropriate type of capacitors. *Risk of early degradation and loss of performance.*

Phase 3 – Hardware & Software Review

Hardware

🟧	Missing protection at the level of the board input and output signals. *Risk to be unprotected against over-voltage, short-circuit, electrostatic discharge, electromagnetic interference.*
🟧	Potential weakness identified at the level of the powering circuits (+1.2V, +2.5V & +3.3V)
🟨	Homogenization of circuit family and circuit types
🟨	Update Bill of Material with the correct type of components mounted on the board

- Good expertise in electronic design
- Recommendation for corrections of failure (criticality level 1)
  - Possible propagation of internal hardware failure
  - Lack of protection against external environment
- Recommendation for possible improvement (criticality level 2 & 3)
  - ESD and EMI protection to be implemented on a case by case study base on signal and transmission characteristics

Phase 3 – Hardware & Software Review

Embedded Software

🟥	No re-synchronization of asynchronous input signals inducing a high risk of metastability.
🟧	Asynchronous logic used for output signal generation should be replaced with synchronous logic.
🟧	Improvement of input debouncer entity for better sensitivity

- Structure of VHDL code should be improved through a more strict programming methodology in order to guarantee a better understandability and maintainability
  - Better coherency in variable naming
  - More structured architecture
- Possible optimisation of FPGA internal timing for better performance
- More simple solutions exist for implementation of the PLL mechanism

Phase 3 – Hardware & Software Review

Simulation

SYNC-12	Nominal BRF at 450GeV is 11.245478kHz.
SYNC-13	Nominal BRF at 7TeV is 11.245500kHz.

🟩	Performance under nominal condition

FAIL-02	In case of a drift of the BRF greater than 25ns w.r.t. the nominal BRF, an internal dump request is issued.

🟩	PLL performance with 25ns jitter on BRF
🟩	PLL performance with 30ns jitter on BRF

INT -01	An internal dump request is generated in case of detection of internal failure.
INT-02	Internal dump request is sent to the redundant TSU.

🟩	Response to an internal failure of the redundant TSU

Phase 3 – Hardware & Software Review

Simulation

SYNC-01	TSU generates a DBRF signal synchronised with the BRF and in phase with BAG.
SYNC-04	DBRF rising edge is adjustable w.r.t BRF rising edge.
SYNC-05	Phase offset between BRF and DBRF is adjustable.
SYNC-07	DBRF phase offset resolution is in steps of 10ns.

🟩	Generation of the DBRF signal

FAIL-03	Delay between BRF failure or BRF instabilities and the execution of the internal dump request is maximum 2 periods of the BRF (1 period for the detection and 1 period for the execution).

🟩	Response to a lost of BRF
🟩	Response to a drift of BRF
🟥	Response to a jump of BRF instabilities

→ In case of a jump of BRF, an asynchronous synchronous dump will generated

Phase 3 – Hardware & Software Review

Simulation

SYNC-10	TSU crosschecks its DBRF signal with the DBRF signal from the redundant TSU.
SYNC-11	In case of discrepancy between internal DBRF and redundant DBRF, an INTDR is issued.

🟩	Response to a drift of the redundant DBRF
🟥	Response to a lost of the redundant DBRF

→ In case of a lost of the redundant DBRF, no action is issued

Others

- Power CIBO module form the +12V.
  - Require an additional +12V → +5V module with high filtering capabilities
  - Lest disturbance to the “normal” +5V
- Monitor SBDT signals in current “instead of” or “in addition to” monitoring in voltage
  - Cable connections to TFOT verification
- Implement “**V**” cycle through project life-cycle
  - Cross-check between developers and testers (blind design)
  - Reject “single man” design failure
  - Better traceability and requirement verification
- Recommendation from STUDIEL to perform a “study of operational safety” of the TSU within the LBDS
  - Risk analysis
  - Failure mode analysis
  - Failure tree analysis

Actions (2011)

Hardware & Software update

- Hardware
  - TSU boards
    - Check some resistor’s values and change when required (optocoupler polarisation)
  - Interface boards
    - Add resistors on each output to protect TSU board drivers against short circuit
    - “Dump request” diagnostic signal splits in two independent output channels through a MAX4427 chip
- Software
  - FPGA (V2.3.7)
    - Filtering of all discrete input signals to prevent metastability effect
    - Redefinition of Local mode signal
    - ABDT trigger is issued in case of timing failure on both TSUs and on redundant TSU
    - Modification of switch debouncer time from 10 msec to 1 msec
  - CPLDs
    - Filtering of all discrete input signals to prevent metastability effect

Actions (2011)

Hardware & Software Validation

Test bench for validation of TSU hardware and embedded software functionalities before operational deployment

Emulation of all input signals

- Frequency (BIS, BEC, BRF…)
- Pulse (Inject & Dump)
- Logic (Local/Remote, Arming…)
- Current loop (BLM)

Analysis of output signal

- Acquisition of output signals (DBRF, AGK…)
- Acquisition of internal diagnostic buffers
- Correlation between hardware signal and software diagnostic

- Inject “error” on emulated input signals and check the correct hardware and software response to failure modes
- Status
  - Individual failure mode successfully tested
  - Implementation of automated test sequence in progress
  - Multiple failures mode still to be done

Actions (2011)

Internal Post Operation

- Signal acquired:
  - All triggering pulsed signals (DRT, ABDT, TFO…)
  - All periodic signals (BRF, DBRF, AGK…)
- Analysis
  - Individual on each signal (frequency, pulse length…)
  - Correlated between signals (synchronisation, phase offset...)
- Extension of the existing IPOC system to the TSU
  - Visualisation
  - Analysis result
- Automatic generation of dump event sequence summary
  - History
  - Failure
- Integration within XPOC system (next steps)
  - Acknowledge in case of analysis failure

Actions

Next Steps: 2012 & 2013

- 2012
  - New interface board with better signal decoupling and isolation
  - Increase TSU embedded software online and post-operation diagnostic functionalities
  - Online monitoring of BIS frequencies
- 2013
  - TSU V3 implementing hardware modification
  - Optimized DPLL (compatibility with SPS revolution frequency)
  - Review TSU deployment architecture (FEC common mode failure)

Review Summary

- TSU hardware and its embedded software are operational and fulfill the required functionalities.
- 11 requirements out of 200 have been identified as not or partially not covered.
  - Out of 11 unfulfilled requirements, 1 is identified as critical and affects the redundancy of the system
- Possible failure modes that can induced a dysfunctional of the board have been identified due to:
  - Lack of protection at the hardware level
  - Metastability in the embedded software
- For the different cases of failures identified, no situation where neither a synchronous dump trigger nor an asynchronous dump trigger will be issued by at least one of the TSU have been identified.