TSU CONS Reliability Meeting - 3

Reliability Block Diagrams of the main functions

Meeting details

List of contents

1. Excerpt of the top-level FMECA
2. Reliability Block Diagram
3. Synchronous Beam Dump
4. Asynchronous Beam Dump
5. Additional top-level failure mode

Meeting objectives

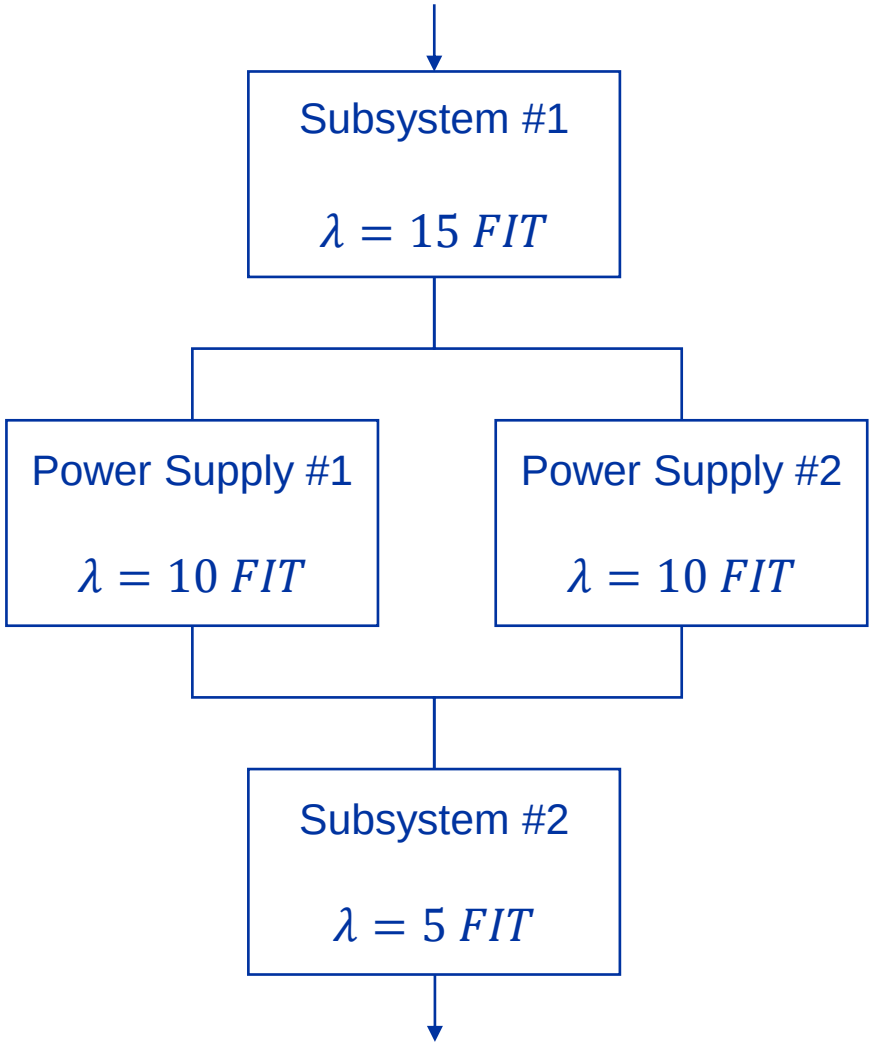
- Establishing Reliability Block Diagrams for most critical functions as input for simulation model
- Clarifying the interfaces with other systems

Recap – Top-level FMECA table (excerpt)
Most critical failures (acceptable once in 1,000 years)

Situation	Failure	Effect	Criticality
3. Dump request	3.2. Fail to issue synchronous and asynchronous beam dump requests	3.2.1. TSU missing a beam dump.	3.2.1.1. With CIBDS: investigation, access on-site required, dry runs • **Acceptable once in 100 years** 3.2.1.2. No CIBDS: massive damage • **Acceptable once in 1,000 years**

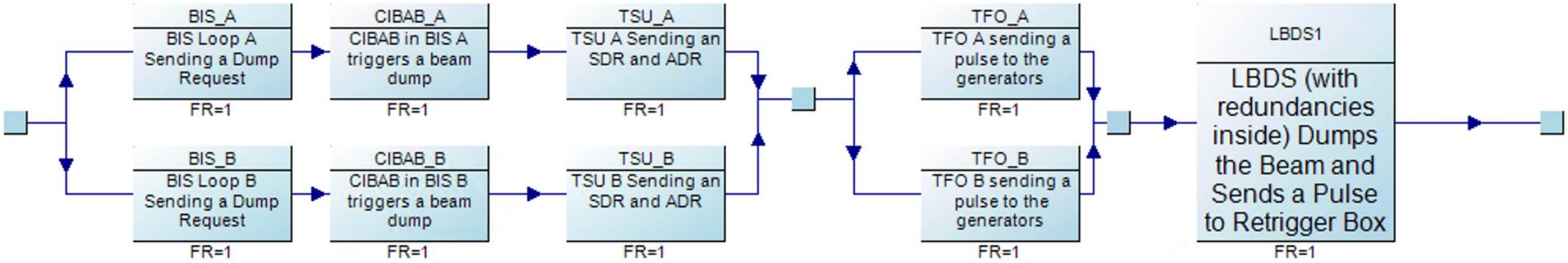
Reliability Block Diagrams
Concept

- **Method in the reliability domain to visualize failure propagation pathways**
  - Focus on functional dependencies between components (also known as Dependency Diagram).
  - Components are represented by connected blocks.
  - Elements can be connected in parallel (signifying redundancy) or in series (any failure leads to a failure of the path).
- **Used to calculate the overall reliability.**
  - Critical points of failure can be visualized.
  - They can be transformed into a success tree (for instance to use in AvailSim4) or a fault tree.



Example RDB of a system with redundant power supply

Synchronous Beam Dump (triggered by BIS)
Reliability Block Diagram

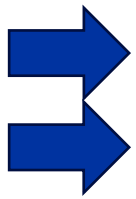


Note:

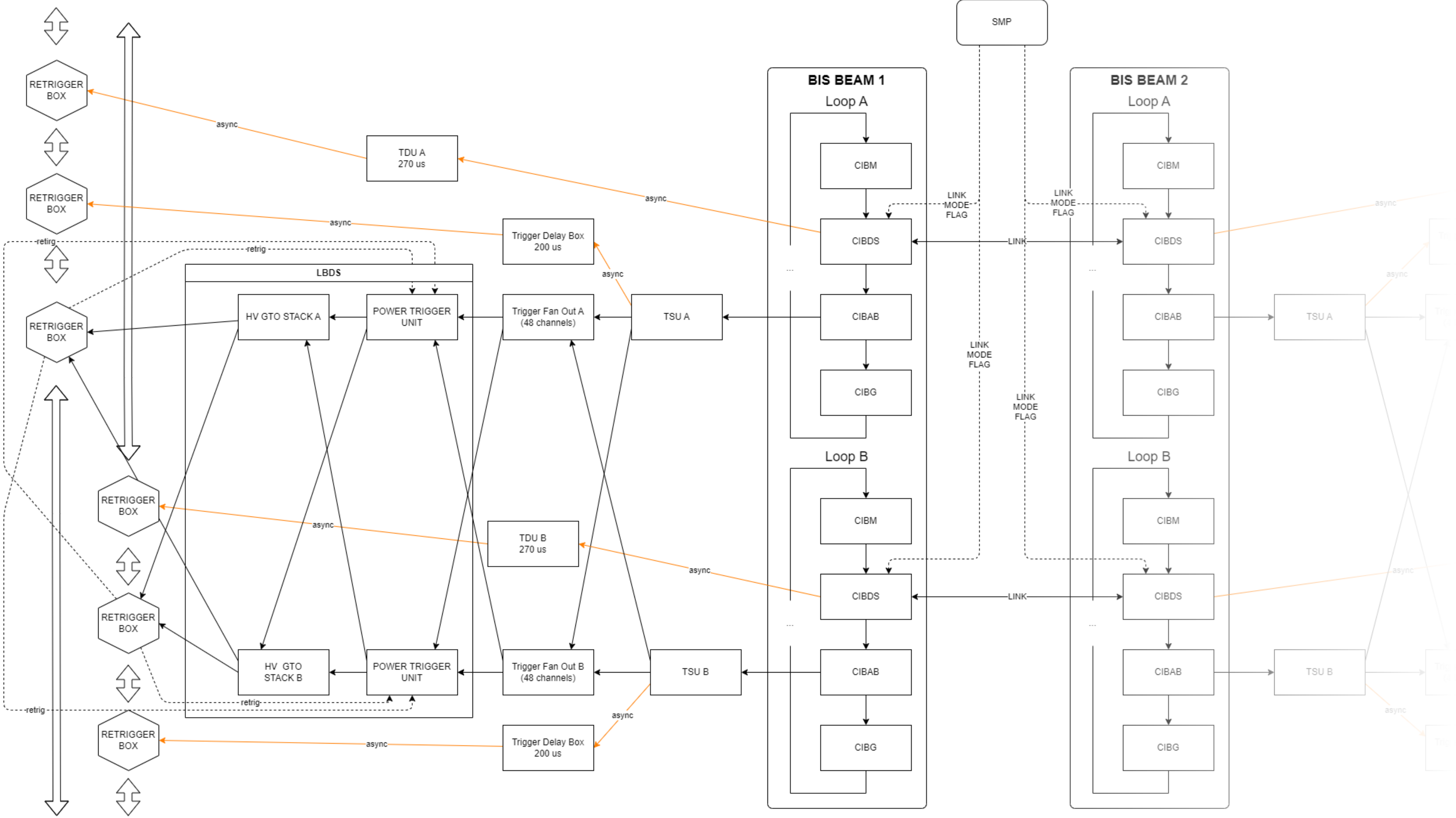
- BRF (Beam Revolution Frequency) not included as input because TSU will regenerate rBRF (regenerated Beam Revolution Frequency) upon loss of BRF signal in normal circumstances.
- Spurious asynchronous beam dump could be added as another box at the end of the chain for completeness.

Question: Of BETS, BLM, SCSS, ETRIG, Which of these also trigger the BIS? Also: LBDS Kickers, LHC Fast Timing.

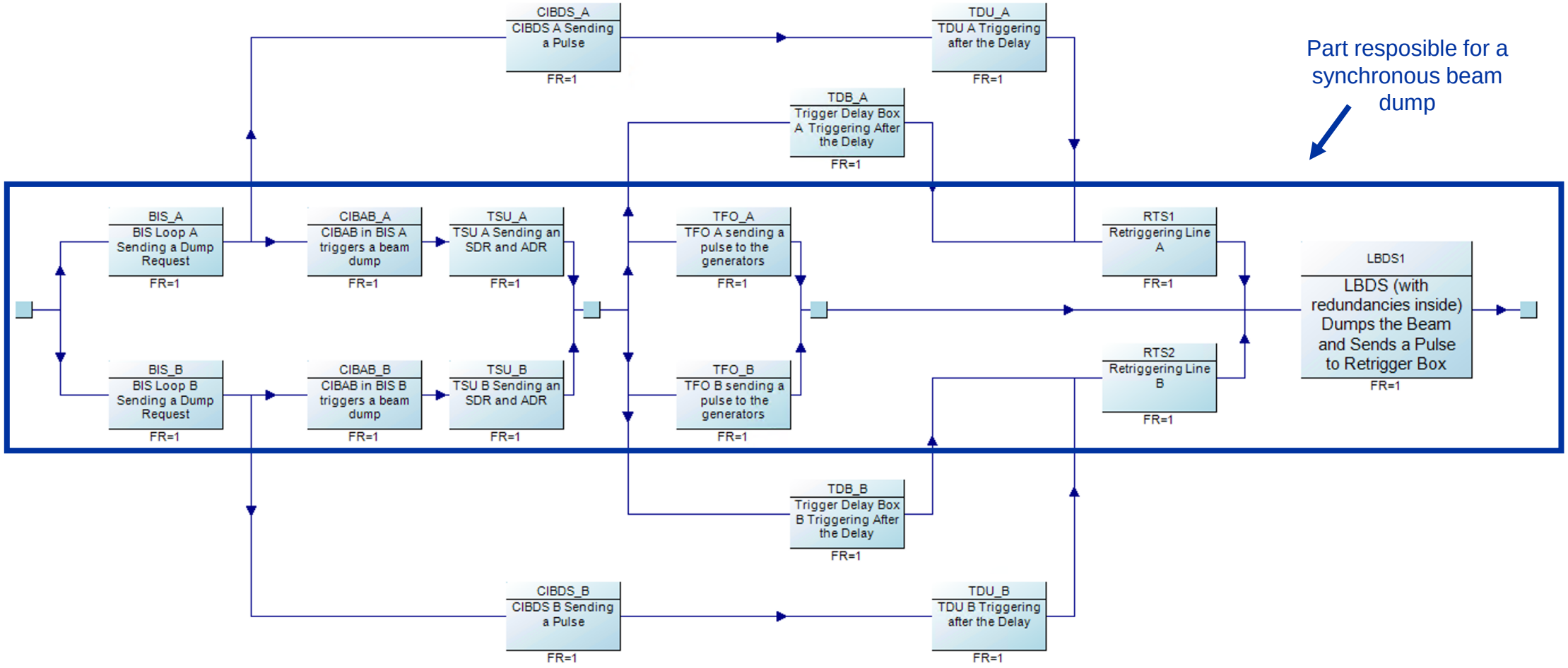
- For those triggering the BIS, they add redundancy.
- Those not triggering the BIS have to be considered separately.



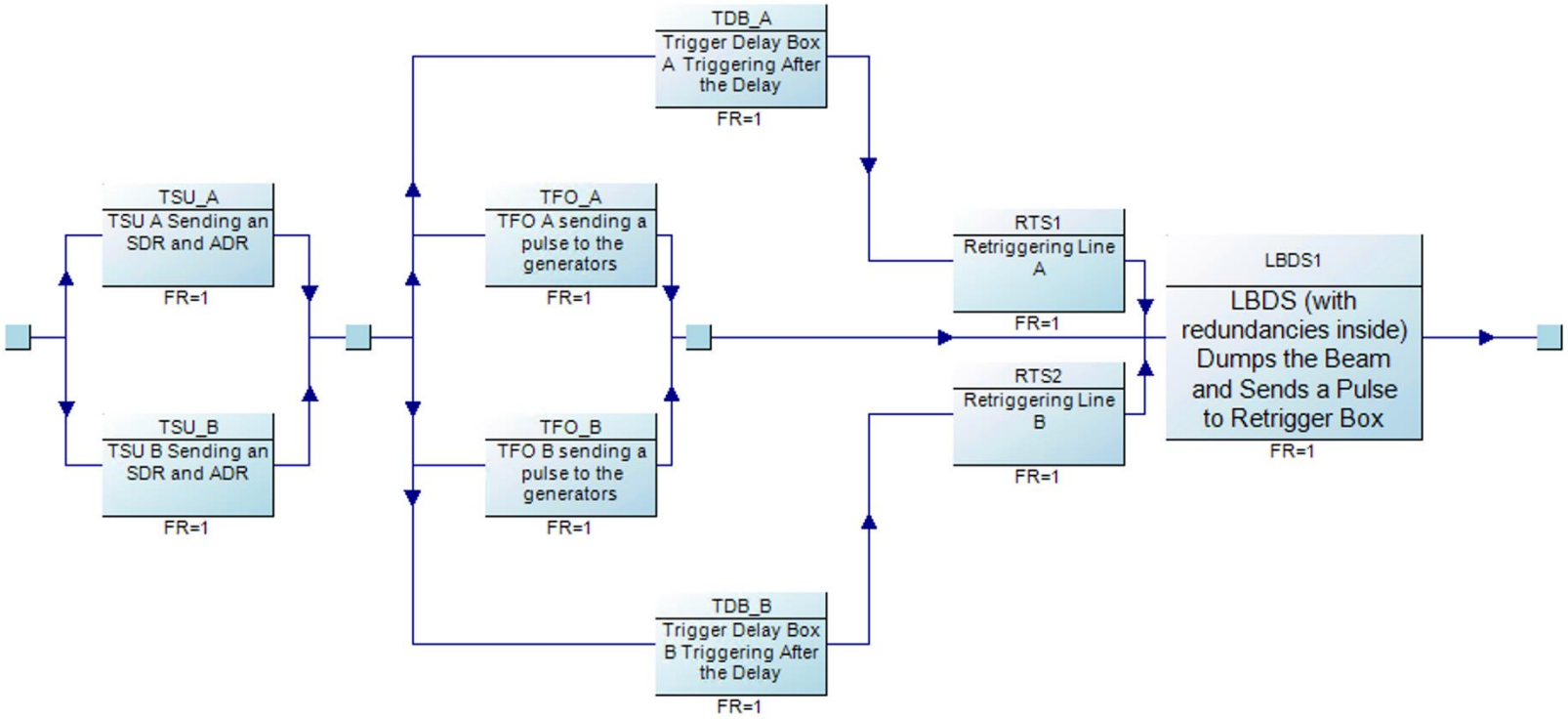
DRS-01	TSU accepts dump request from the LHC Beam Interlock System (BISDR).	***OK***
DRS-02	TSU accepts dump request from the LBDS Beam Energy Tracking System (BETSDR).	***OK***
DRS-03	TSU accepts dump request from the LSS6 Beam Losses Monitors (BLMDR).	***OK***
DRS-04	TSU accepts dump request from the LBDS Kicker Systems (LBDSDR).	***OK***
DRS-05	TSU accepts dump request from the LHC Fast Timing System (TIMDR).	***OK***
DRS-06	TSU accepts dump request form LBDS local pulse generator (LOCDR).	***OK***
DRS-07	TSU generates an internal dump request in case of internal failure (INTDR).	***OK***
DRS-08	TSU accepts dump request from the redundant TSU (REDDR).	***OK***


SMP
BIS BEAM 1
Loop A
CIBM
CIBDS
CIBAB
CIBG
Loop B
CIBM
CIBDS
CIBAB
CIBG
BIS BEAM 2
Loop A
CIBM
CIBDS
CIBAB
CIBG
Loop B
CIBM
CIBDS
CIBAB
CIBG
LINK MODE FLAG
LINK MODE FLAG
LINK MODE FLAG
LINK MODE FLAG
LINK
LINK
TSU A
TSU B
TSU A
TSU B
TDU A 270 us
TDU B 270 us
Trigger Delay Box 200 us
Trigger Delay Box 200 us
Trigger Fan Out A (48 channels)
Trigger Fan Out B (48 channels)
LBDS
HV GTO STACK A
HV GTO STACK B
POWER TRIGGER UNIT
POWER TRIGGER UNIT
RETRIGGER BOX
RETRIGGER BOX
RETRIGGER BOX
RETRIGGER BOX
RETRIGGER BOX
RETRIGGER BOX
async
retig
retrig
retrig
retrig

Beam Dump via CIBDS and TSU (triggered by BIS)
Reliability Block Diagram



Beam Dump via TSU (not triggered by BIS)



Question: Of BETS, BLM, SCSS, ETRIG, Which of these also trigger the BIS? Also: LBDS Kickers, LHC Fast Timing.

- For those triggering the BIS, they add redundancy.
- Those not triggering the BIS must be considered separately.

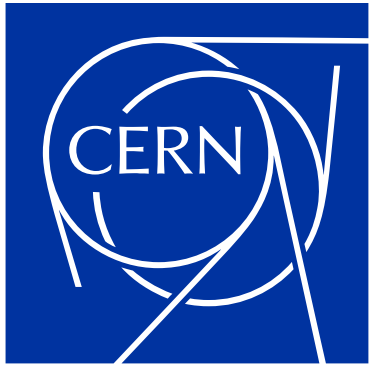
Additional top-level failure mode
Discrepancy between frequencies in TSUs

Situation	**Failure**	**Effect**	**Criticality**
7. Dump when discrepancy between TSUs is detected	7.1. Failure to detect the discrepancy within acceptable time	7.1.1. Exposing the machine to the risk of an asynchronous dump. ///OR/// Asynchronous dump (if proceeds anyways)	7.1.1.1. Investigation required • **Acceptable once in 10 years**
	7.2. Fail to dump the beam within 5 revolutions OR send an asynchronous dump request only	7.2.1. – same effects and criticality as 7.1.1	

Question: Discrepancy of which parameters would trigger a dump? (RBRF, DRBRF, AGK Status signals (CRC, PS surveillance))

Next steps

- **Parameters for beam dump request simulation:**
  - Failure modes and rates -> bottom-up FMECA for TSU (assumptions for now), existing studies for other elements.
  - Inspections (XPOC/IPOC/Post Mortem scope, yearly tests, …)
    - Detectability of component failures
    - Any blind failures not detected in XPOC/IPOC/Post Mortem
  - Operational phases
  - Demand rate (to be extracted from Post Mortem database)
- **Defining blind failure requirements from sensitivity analysis and spurious failure requirements from availability targets**
- **Starting bottom-up FMECA once design files available and compare with the requirements**
- **Development of a reliability model of LBDS Power distribution?**



home.cern