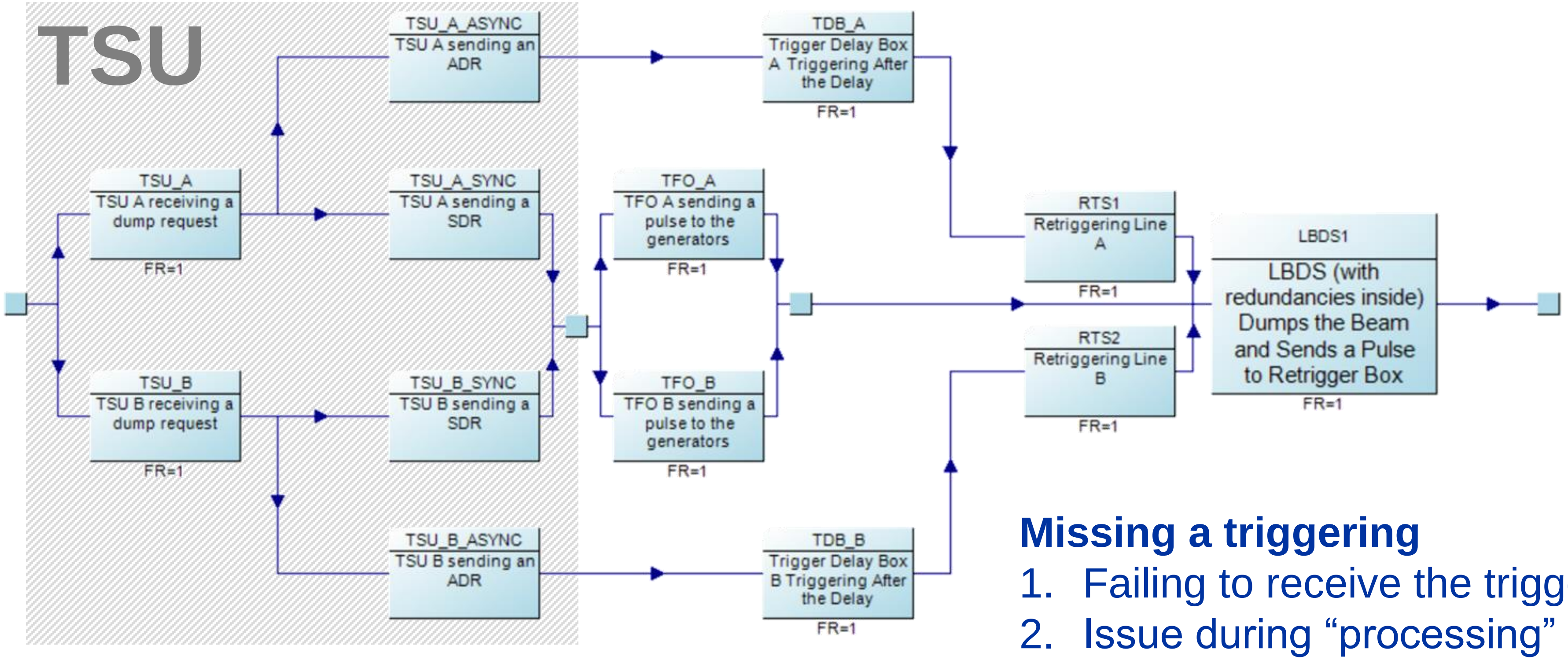
Reliability Model of Critical TSU Failure – Missing the Triggering

TSU CONS Reliability Study Progress Meeting #9

List of contents

TSU Missing Triggering Model
Discussed in the previous meetings

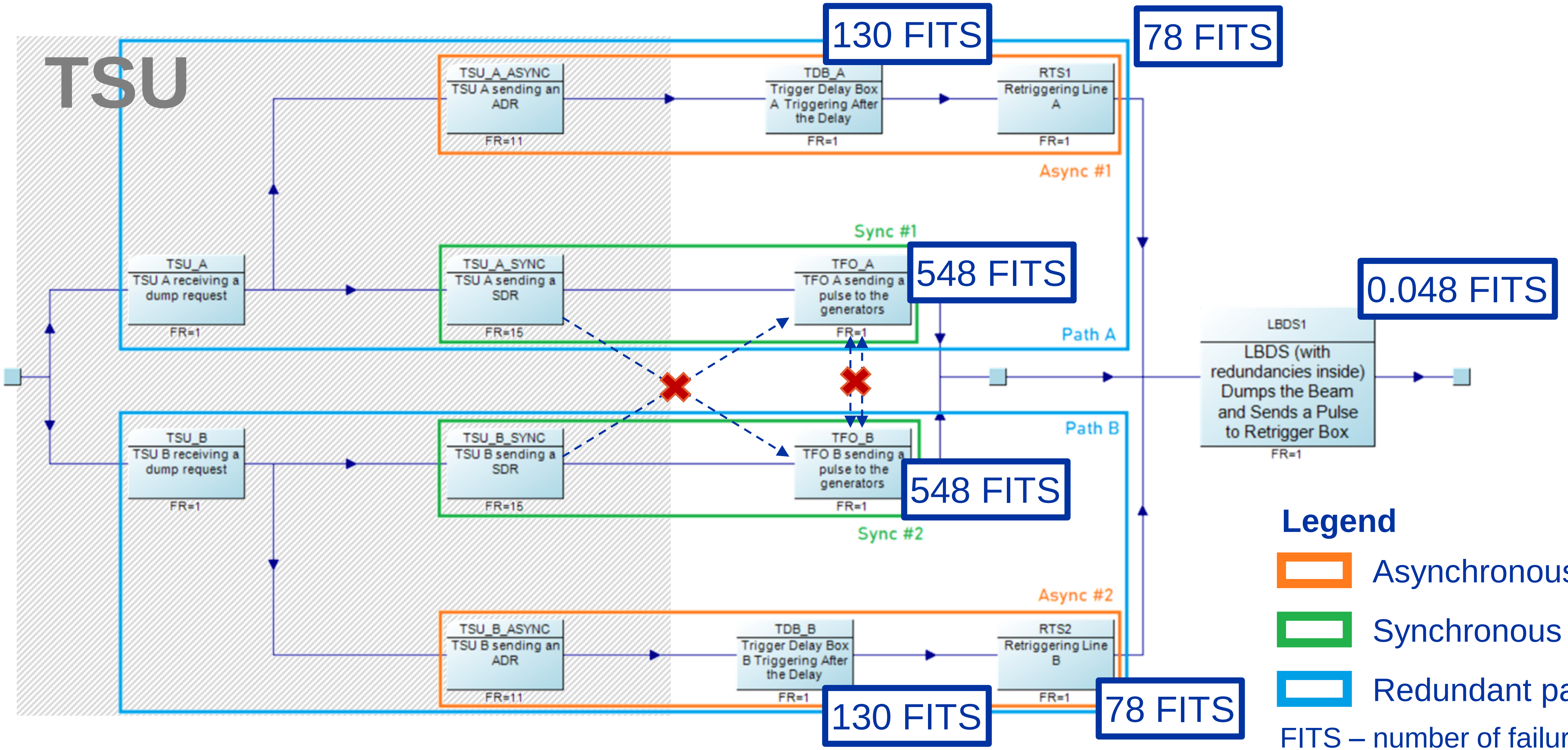


Missing a triggering

1. Failing to receive the trigger from the external sources.
2. Issue during “processing” of the trigger inside the TSU.
3. Failing to trigger any of the 2 synchronous paths.
4. Failing to trigger any of the 2 asynchronous paths.
5. LBDS critical malfunction.

TSU Simplified Analytical Model

Simplifying calculations through pessimistic assumptions



Legend

- Asynchronous
- Synchronous
- Redundant path

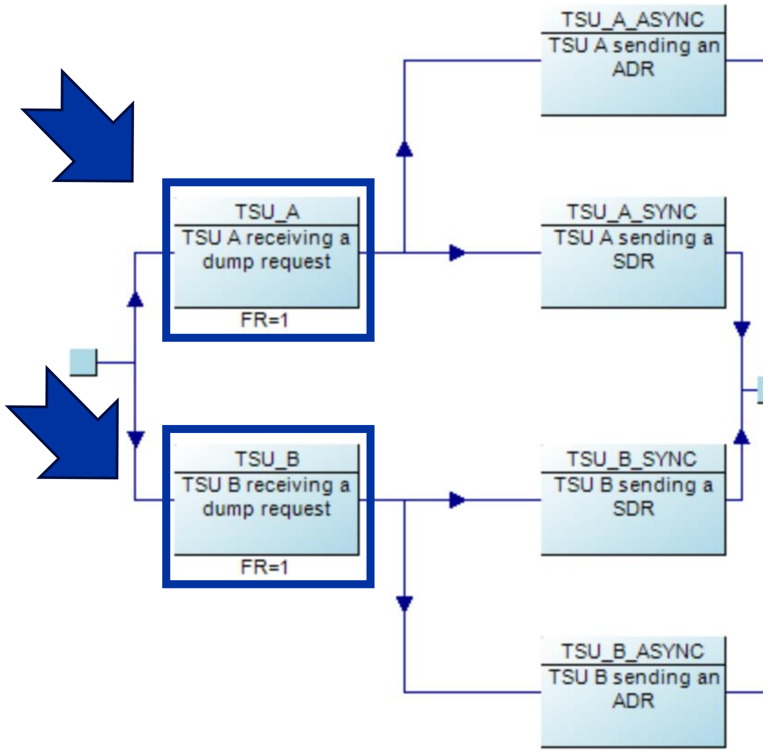
FITS – number of failures in 10^9 hours

Failure rates
Input Signals

Applicable failure modes:

- **BLM always TRUE – 2.89 FITS**
- **BETS always TRUE – 0.67 FITS**
- **BIS always TRUE – 0.67 FITS**
- **T1/T2 always TRUE – 0.5 FITS**
    - Only problematic when another failure occurs.

Total: 4.3 FITS.

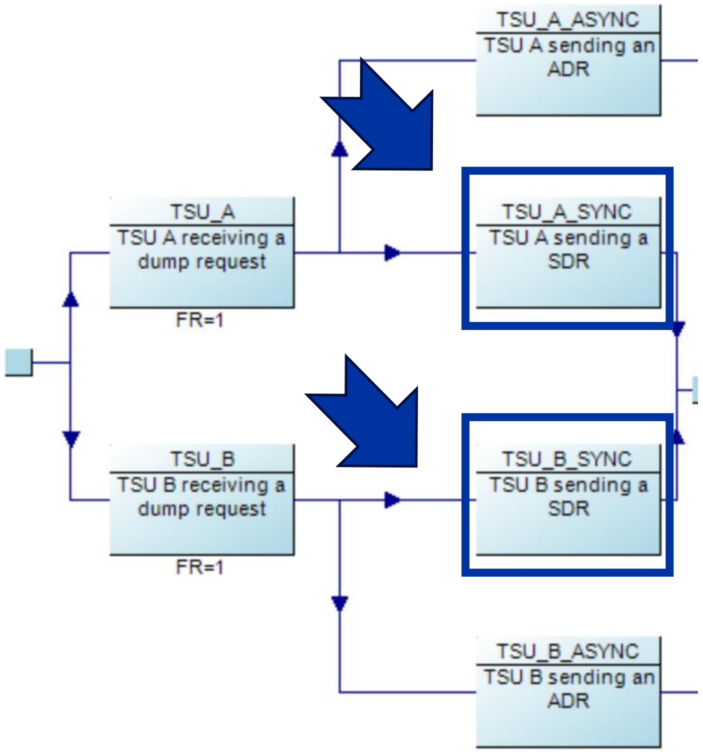


Failure rates
Synchronous Paths

Applicable failure modes:

- **Loss of SBDT A – 30.3 FITS**
  - Fuse F3 – 20 FITS
- **Loss of SBDT B – 28.7 FITS**
  - Fuses F4 – 20 FITS
- **Loss of SBDT A&B – 1.0 FITS**
  - In the simplified model there is just one path (to only one TFO) anyways.

Total: 31.3 FITS (SBDT A + SBDT A&B)

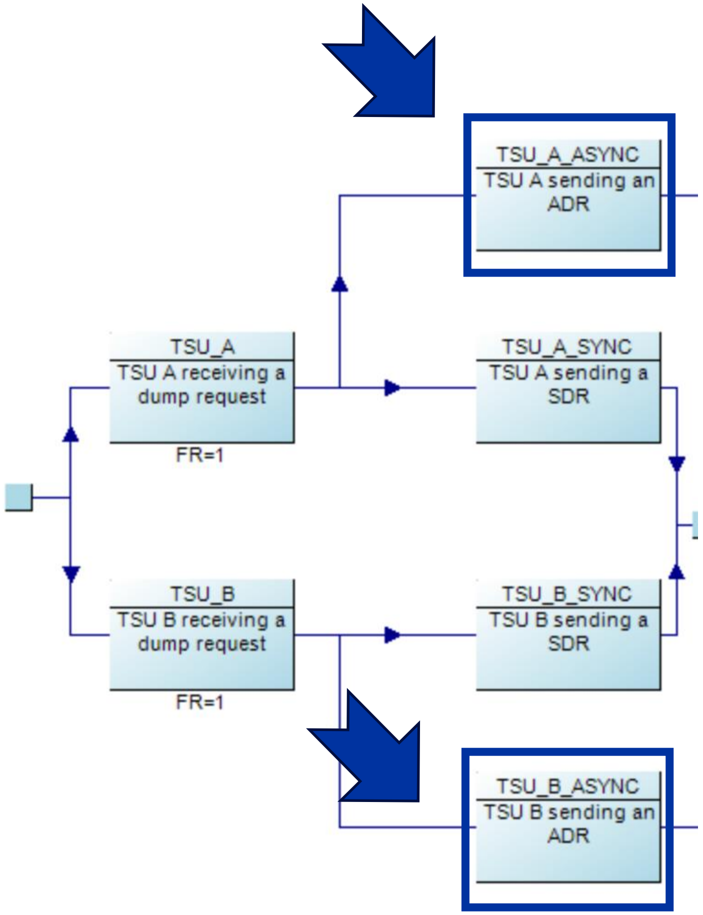


Failure rates
Asynchronous Path

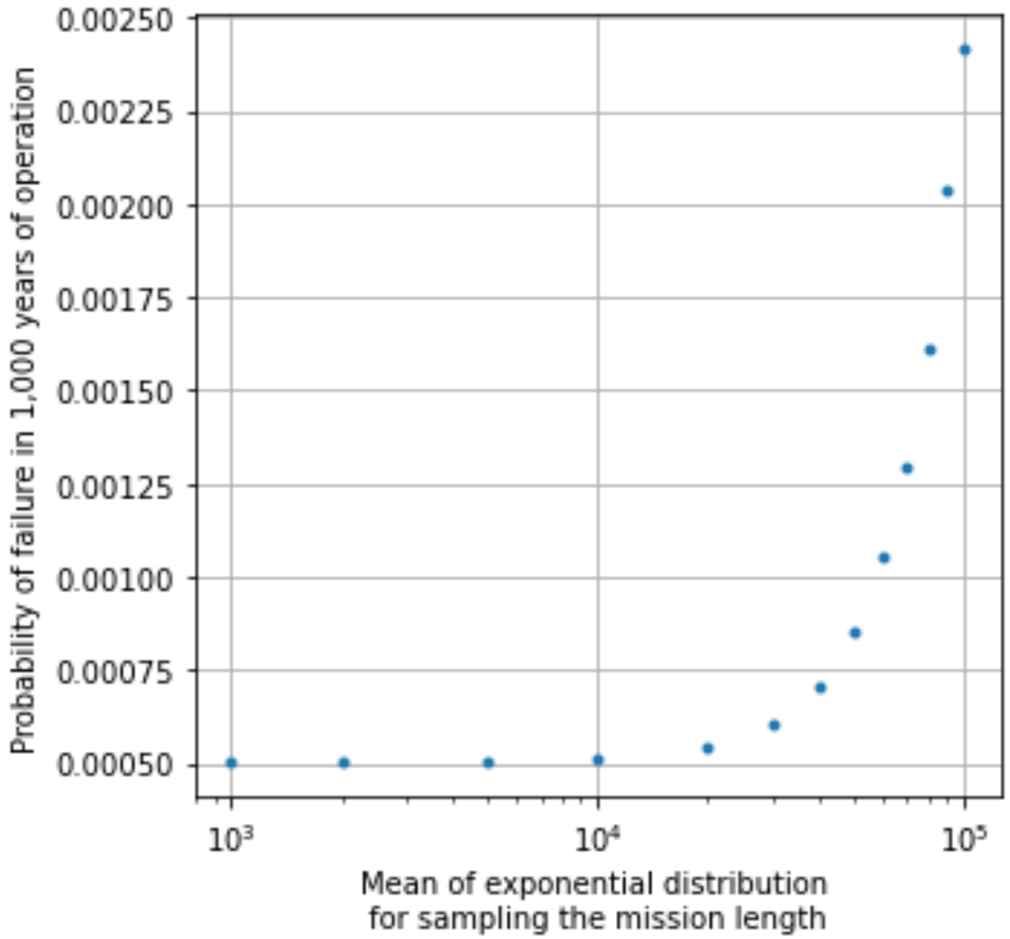
Applicable failure modes:

- **“Loss of ABDT path” – 4.9 FITS.**

- **Additional potentially relevant failure modes**
  - Comment “Loss of ABDT path”
  - However, causing immediate synchronous or asynchronous dump
  - **Total of 49.8 FITS.**



Simulation Results
Of the Hybrid MC Model



Reliability requirement:
No more than 10% probability of a failure after 1,000 years.

Assumptions:

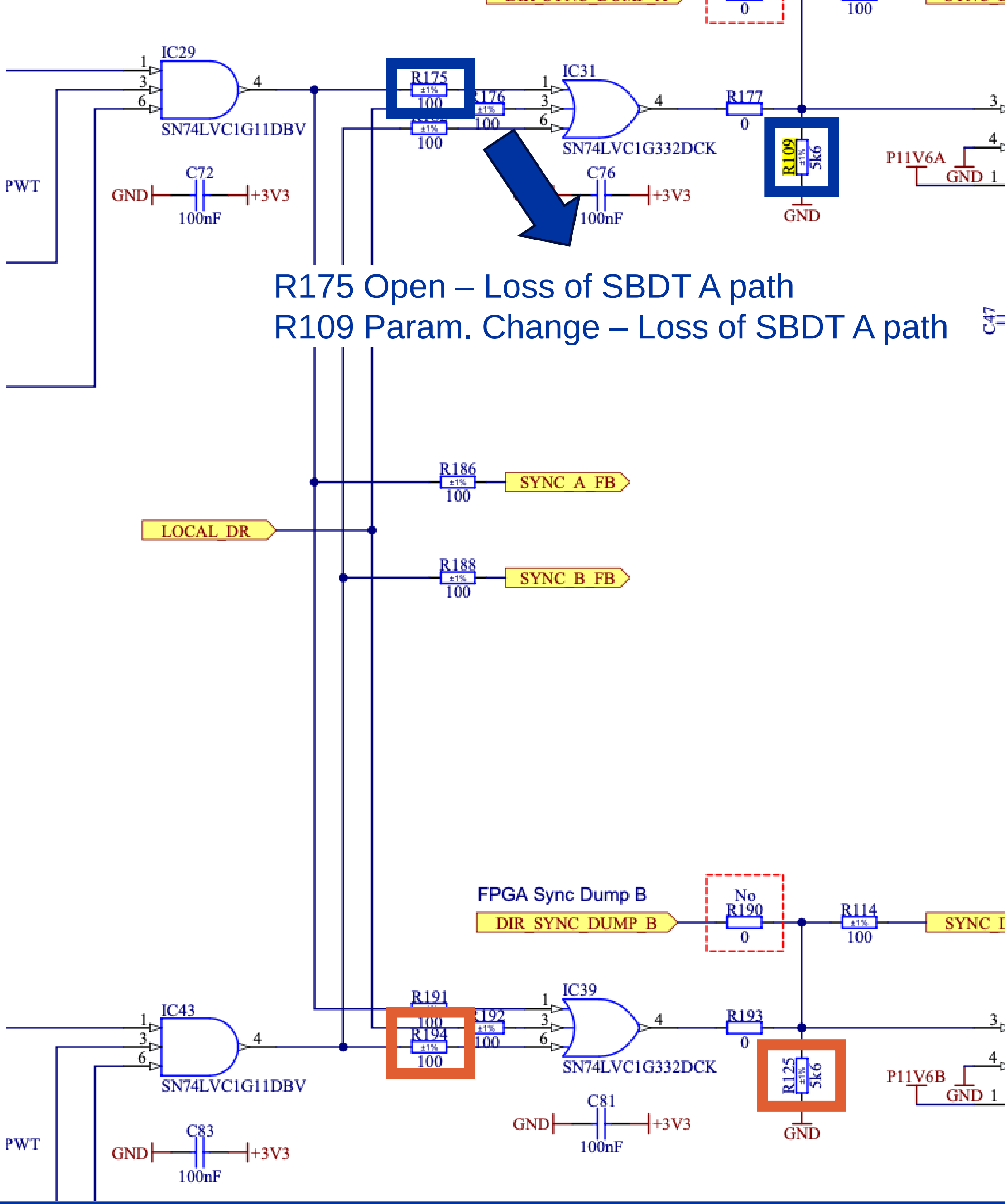
- Simulations of lifetimes lasting 1,000 years
  - A single year is assumed to have **6,000 operational hours**.
  - Within that time, there are multiple “missions” ended by triggers.
    - Mission lenghts are sampled according to the value on the x axis.
- **Each component is repaired after a trigger** (i.e., mission).

Conclusions

- **The hybrid MC model shows that the system meets the reliability requirement.**
  - With significant margins.
- **No single points of failure** identified in the analysis.
- There is reasonable confidence in the reliability of the system even with 1 year long missions.
  - Critical since the number of triggering does not impact the failure rates in the models, but decreases the testing frequency.
  - Shown by results of both, hybrid MC model and exact model.
  - Frequent testing/IPOC monitoring remain important though to avoid failure buildups, 2nd order failures, etc. (as was only partially in the scope of the FMECA and simulations).
- **Next step**: hybrid MC model of the asynchronous dumps.

Remaining questions

- **Failure modes causing ”Loss of ABDT path” but triggering asynchronous or synchronous dumps – can they be danegrous?**
- **Can a “VPSOK always TRUE” failure mode result in missing a trigger?**
- **Where is the discrepancy between failure rates assigned to “Loss of SBDT A” (10.3 FITS) and “Loss of SBDT B” (8.7 FITS) coming from?**
  - R175 Open causing loss of SBDT A path, while corresponding R194 is #N/A
  - R109 param. change causing loss of SBDT A path, while corresponding R125 no effect



home.cern