# TSU CONS Reliaiblity Study – Meeting 4

## Simulation scenarios parameters and inputs

# List of contents

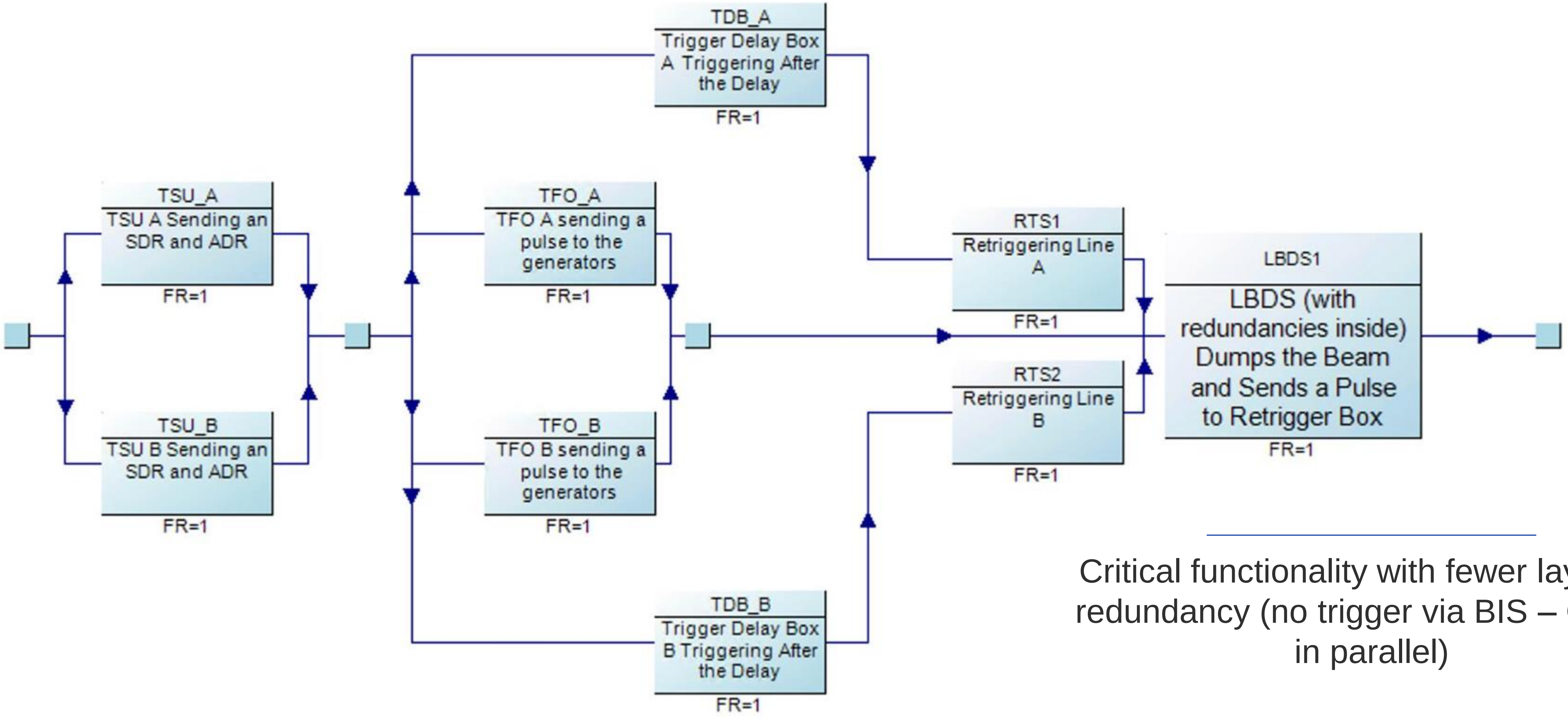
1. **Simulations for requirements.**
    1. Assumptions.
    2. Reliability Block Diagram (RBD) of the model.
    3. General results.
    4. Results for various mission lengths.
    5. Conclusions.
    6. Synchronous Beam Dump simulations.
2. **Remaing questions.**
3. **Next steps.**

# Simulations
## Assumptions

- **Hybrid Monte-Carlo analytical model**
  - Each iteration draws the mission length of from a probability distribution with mean set to 12 hours.
- **Assumptions:**
  - Each mission ends with a check (IPOC/XPOC, Post Mortem, active surveillance) which removes blinds failiures and brings the system back to “as good as new” state. Assuming full coverage (see simulations for various mission lengths).
  - Each year has 250 operational days.
  - Not considering software or other common cause errors.
- **Failure rates:**
  - TFO assigned 548 FITS (TO1 “TO unit failed open”, RF’s thesis, Table A.6)
  - TDU/TDB assigned 130 FITS (V. Vatensever thesis, Equation 5.9)
  - RTS assigned 78 FITS (L “Re-triggering line failed”, RF’s thesis, Table A.7)
  - LBDS assigned ("< 14 MKD available”, RF’s thesis, 0.084 FITS, Table 7.2)

# Simulated model

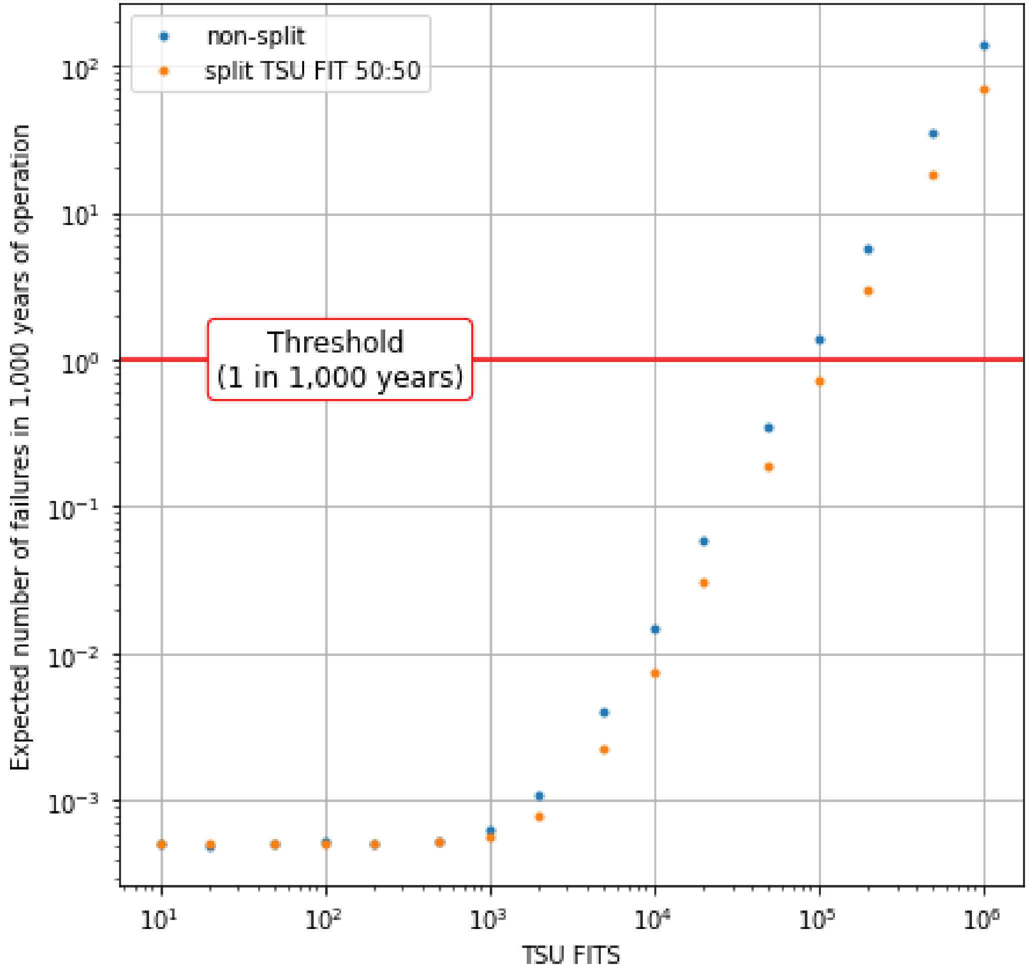
## Async Beam Dump via TSU (not triggered by BIS)

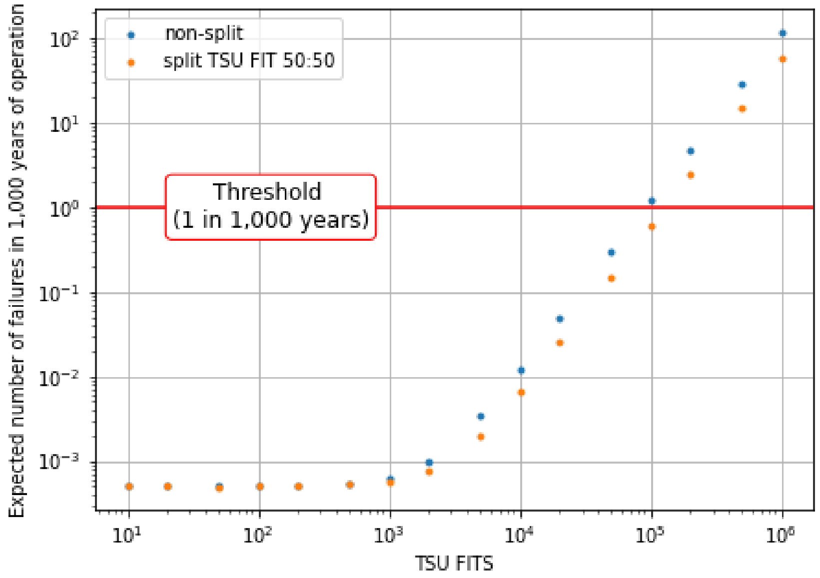



Critical functionality with fewer layers of redundancy (no trigger via BIS – CIBDS in parallel)

# Simulation results
## Sensitivity analysis of the TSU FITS

- **Accceptable failure probability threshold**
  - 1 failure every 1,000 years.
  - **Fulfilled** as long as FITS of TSU's blind failures << 10^5 (equivalent to 0.6 failures per 250 days)
  - Result should have at least an order of magnitude margin to account for other critical scenrios.
- **Mission length sampled from the exponential distribution with mean of 12 hours.**
- **Two model variants considered:**
  - **Blue dots:** model without the inter-TSU dump request communication.
  - **Orange dots:** model assuming that each TSU exchanges information with the other one (parts responsible for receiving and transmitting have the failure rate divided equally).

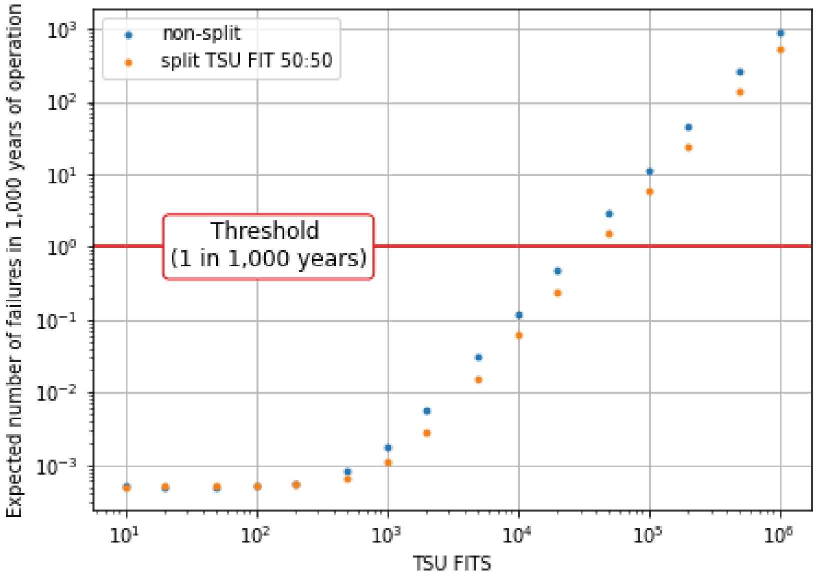




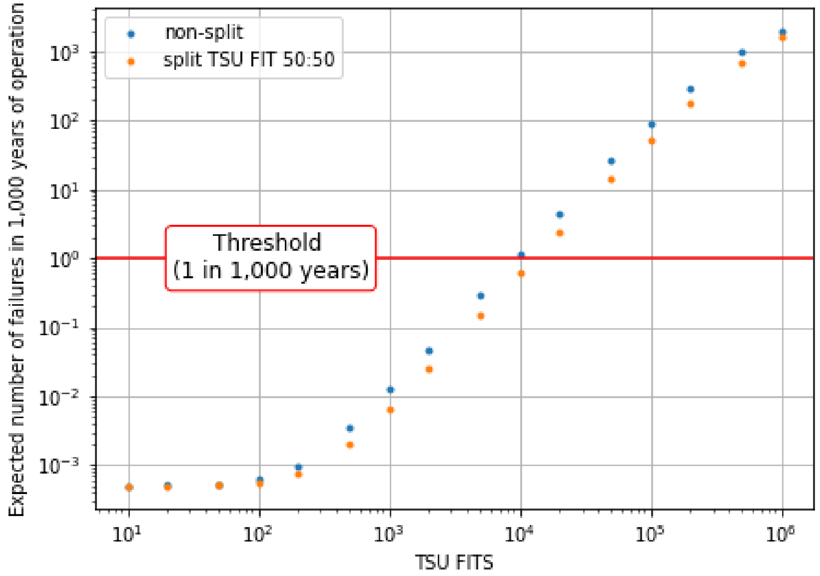

Mission length = 10h , threshold at $10^5$

## Impact of fill length

(→ time until system is as good as new)



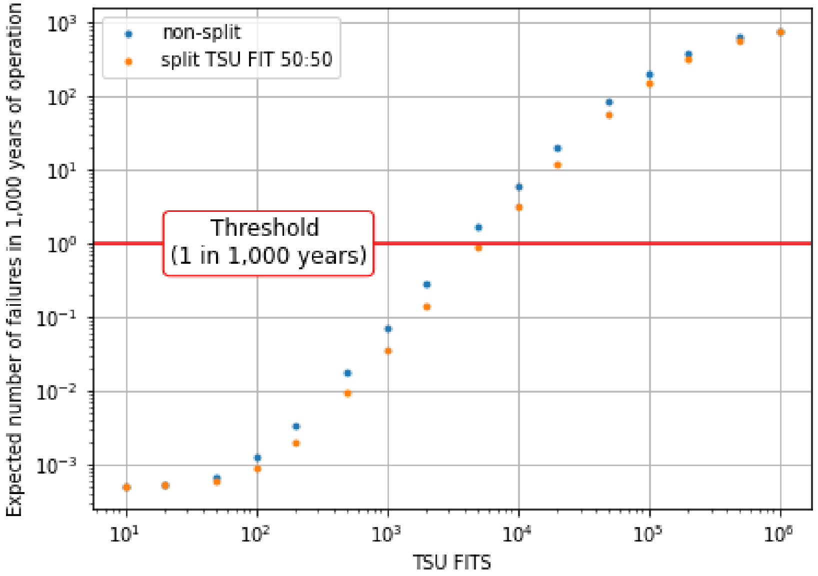

Mission length = 100h , threshold at $3 \times 10^4$




Mission length = 1000h, threshold at $10^4$

## Extreme case

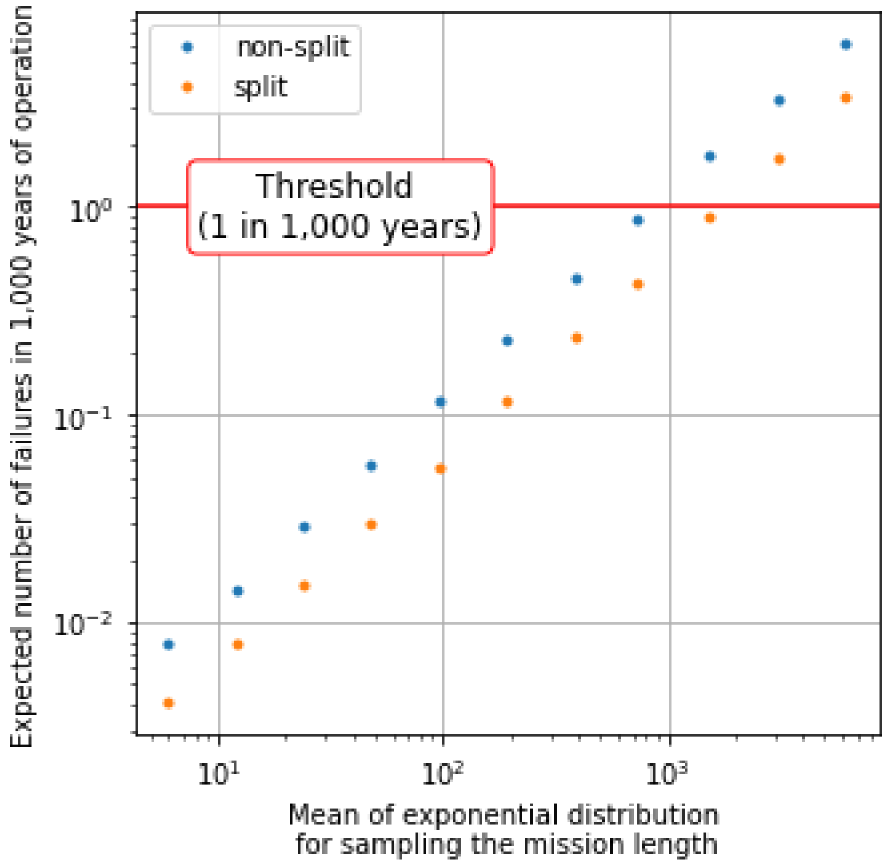
checks do not work; failures detected and removed only the end of the year




Mission length = 6000h , threshold at $5 \times 10^3$

# Simulation results
## Varying mission length

- **TSU failure rate set to 10,000 FIT.**
- **Increasing the time between missions increases the probability of a critical failure.**
  - Longer missions mean longer periods without checks, removing the possibility for the system to be repaired.
  - In effect, lack of checks leads to accumulation of the failures in redundant paths.

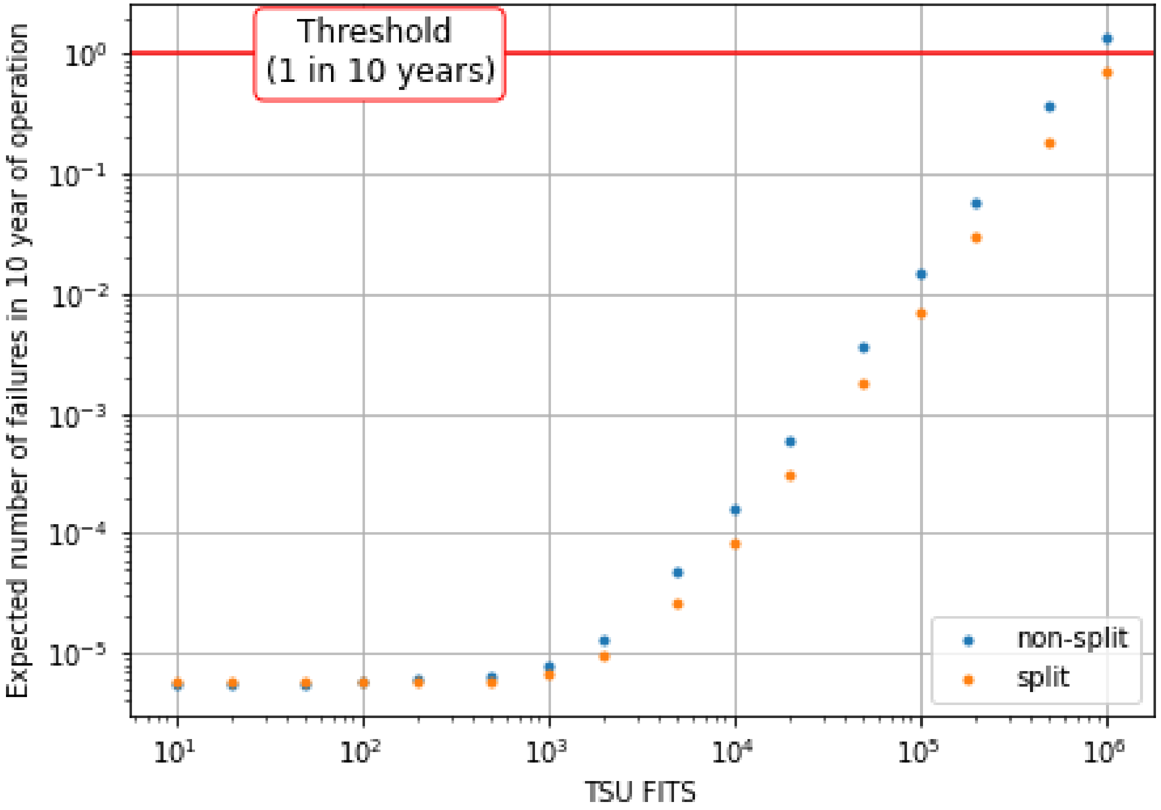


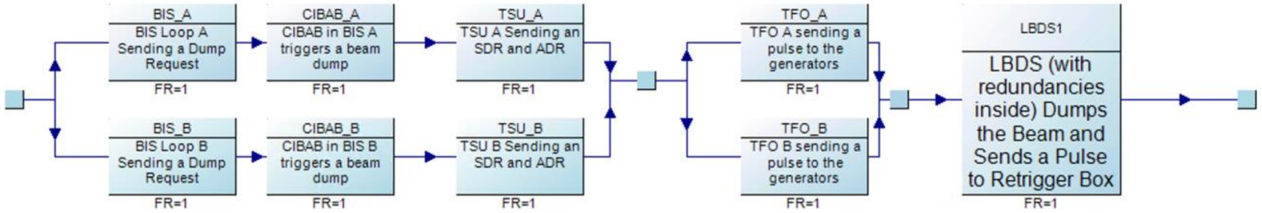
# Simulation
## First takeaways

- **C0. With current assumptions, estimated TSU blind failure rate requirement not very stringent.**
- **C1. Inter-TSU dump request doesn't make much difference.**
  - It provides additional advantage but does not seem to be changing the results significantly.
- **C2. More important: ensuring that checks cover all failures.**

# Synchronous Beam Dump (triggered by BIS)

- **Model of triggering an asynchronous beam dump in effect of a failure in the standard triggering**
  - Failure more likely (less protection layers), but given the relaxed threshold (1 asynchronous beam dump per year), FITS are not a problem
- **Simulation**
  - Completed for a mission length sampled from the exponential distribution with mean of **12 hours**
  - Increasing or decreasing that value leads to same observations as before: more time between checks increases the risk of a critical failure
    - For comparison, the threshold is reached for a TSU with 10,000 FIT when mission length is ~1,000 hours.



# Other critical failures in R. Filippini’s thesis

- **When does the BETS trigger a dump? (Unable to trigger a dump request is classified as a critical failure in R. Filippini’s thesis)**
  - The thesis explains the failure mode as the system being blind to powering failures (unable to detect an energy tracking error).
  - Or can it only cause an erratic energy measurement?

# Next steps

- **Extension of simulation model & sensitivity analysis**
  - Increased failure rate of other systems
  - Beam dump via TSU and CIBDS (triggered by BIS) model
- **Depending on status of the detailed TSU design could start bottom-up analysis**
- **Top-level analysis of LBDS Power Distribution**

home.cern