TSU CONS Reliability Meeting - 2

Top-level architectural analysis

Top-level FMECA table
Concept

- **The goal is to establish high-level functions of the TSU**
  - We want to establish the context in which the function is used (“Situation”, can be “LBDS function”)
  - What the TSU is doing (“Function”/“TSU Function”)
  - What can go wrong in the TSU scope (“Failure”)
    - Effect of that failure on the TSU, accelerators, etc.
    - Assesment of the failure’s criticallity:
      - Optimally, in the duration of downtime caused by the failure and its effects (i.e., up to 3 hours, or 1 month to 1 year).

Situation	Function	Failure	Effect	Criticality
Operation	Do not dump	Wrong signal sent	Spurious dump	Repair up to 3 hours
…	…	…	…	…

Table: an example of a top-level FMECA summary

Top-level FMECA table I
Main functions of the system

Situation	LBDS Function	TSU Function	Failure	Effect	Criticality
Normal operation	Do not dump the beam	Do not trigger the dump and return status to BIS	Spurious generation of a beam dump signals	Synchronous beam dump	No damage, investigation, 1y
				Asynchronous beam dump (more likely)	No damage, investigation, dry runs, 10y
TSU in LOCAL operation/LBDS testing	-	Testing	Fail and triggering an asynchronous beam dump	Asynchronous beam dump	No damage, investigation, dry runs, 10y
Dump request: from BIS (CIBAB), LBDS BETS, BLMs, LBDS Kickers, LHC Fast Timing (all above active only when in REMOTE), LBDS local pulse generator (active only when in LOCAL)	Dump the beam	Issue a synchronous dump request, an asynchronous dump request and DRT.	Fail to issue a synchronous dump request	Asynchronous beam dump	No damage, investigation, dry runs, 10y
			Fail to issue synchronous and asynchronous beam dump requests	Missed beam dump (-> Asynchronous beam dump via CIBDS)	Access on-site, dry runs 100y (if no CIBDS, massive damage) 1000y
			Fail to issue DRT	No timestamp for Post Mortem, IPOC, …	Investigation, on-site, 1y

Top-level FMECA table II
Main functions of the system

Situation	LBDS	TSU Function	Failure	Effect	Criticality
Injection	-	Allow injections when TSU is in READY state; prevent them otherwise. Permit signal goes to false as soon as there is a dump request. Opposite way only on ARM command (?)	Fail to allow injections despite conditions OK	Downtime	No damage, investigation, dry runs, 1y
			Allowing injections when conditions NOT OK (2 TSU per beam, each sends a separate permit and there is also a user permit for the Ring BIS)	Risk of damages (not being able to dump)	Investigation, etc; 100y If no CIBDS, masssive damage, 1000y
Arming	-	Receive an ARM command, check if clients are TRUE, control is REMOTE, synchronisation is correct, post-operational checks are unlatched; set TSU status to READY if successful, injection permit to TRUE. Limit the execution duration to 5 seconds.	Fail to arm when conditions are OK	Downtime	Investigation, 1y
			Arming when conditions NOT OK (2 TSU per beam, each arms separately)	Risk of missed beam dump	Investigation, etc; 100y If no CIBDS, masssive damage, 1000y
Power outage	-	Remain operational to issue a synchronous and asynchronous requests	Fail to maintain power to complete the synchronous dump request	Worst case: asynchronous beam dump	No damage, investigation, dry runs, 10y
				Synchronous dump from the other TSU	Availability, 1y

Row-by-row

Top-level functions of the TSU

Top-level function FMECA
Normal operation

Situation: normal operation

Expected LBDS action: do not dump the beam

TSU function: do not trigger the dump and return status to BIS.

TSU's failure I: spurious generation of a beam dump signals

- Effect of the TSU's failure: synchronous beam dump
  - Criticality: no damage, investigation
    - 1 in 1Y
- Effect of the TSU's failure: asynchronous beam dump (more likely)
  - Criticality: no damage, investigation, dry runs
    - 1 in 10Y

Top-level function FMECA
Testing

Situation: TSU in LOCAL operation/LBDS testing

Expected LBDS action: not applicable

TSU function: Testing

TSU's failure: fail and triggering an asynchronous beam dump

- Effect of the TSU's failure: asynchronous beam dump
  - Criticality: No damage, investigation, dry runs,
    - 1 in 10Y

Top-level function FMECA
Beam dump request

Situation: dump request: from BIS (CIBAB), LBDS BETS, BLMs, LBDS Kickers, LHC Fast Timing (all above active only when in REMOTE), LBDS local pulse generator (active only when in LOCAL)

Expected LBDS action: dump the beam

TSU function: issue a synchronous dump request, an asynchronous dump request and DRT.

TSU's failure: fail and triggering an asynchronous beam dump

- Effect of the TSU's failure: asynchronous beam dump
  - Criticality: No damage, investigation, dry runs,
    - 1 in 10Y

TSU's failure: fail to issue synchronous and asynchronous beam dump requests

- Effect of the TSU's failure: Missed beam dump(-> Asynchronous beam dump via CIBDS)
  - Criticality: Access on-site, dry runs
    - 1 in 100Y
  - If no CIBDS, massive damage
    - 1 in 1000Y

TSU's failure: fail to issue DRT

- Effect of the TSU's failure: No timestamp for Post Mortem, IPOC, etc.
  - Criticality: Investigation, on-site,
    - 1 in 1Y

Top-level function FMECA
Injection

Situation: Injection

Expected LBDS action: -

TSU function: Allow injections when TSU is in READY state; prevent them otherwise. Permit signal goes to false as soon as there is a dump request. Opposite way only on ARM command

TSU's failure: Fail to allow injections despite conditions OK

- Effect of the TSU's failure: Downtime
  - Criticality: No damage, investigation, dry runs,
    - 1 in 1Y

TSU's failure: Allowing injections when conditions NOT OK (2 TSU per beam, each sends a separate permit and there is also a user permit for the Ring BIS)

- Effect of the TSU's failure: risk of damages (not being able to dump)
  - Criticality: investigation, etc;
    - 1 in 100Y
  - If no CIBDS, massive damage,
    - 1 in 1000Y

Top-level function FMECA
Arming

Situation: Arming

Expected LBDS action: -

TSU function: Receive an ARM command, check if clients are TRUE, control is REMOTE, synchronisation is correct, post-operational checks are unlatched; set TSU status to READY if successful, injection permit to TRUE. Limit the execution duration to 5 seconds.

TSU's failure I: Fail to arm when conditions are OK

- Effect of the TSU's failure: Downtime
  - Criticality: Investigation,
    - 1 in 1Y

TSU's failure II: Arming when conditions NOT OK (2 TSU per beam, each arms separately)

- Effect of the TSU's failure: Risk of missed beam dump
  - Criticality: investigation, etc;
    - 1 in 100Y
  - If no CIBDS, massive damage,
    - 1 in 1000Y

Top-level function FMECA
Power outage

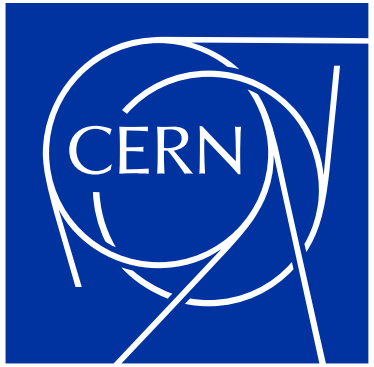
Situation: power outage

Expected LBDS action: dump the beam

TSU function: remain operational to issue a synchronous and asynchronous requests

TSU's failure: fail to maintain power to complete the synchronous dump request

- Effect of the TSU's failure I: (worst case) asynchronous beam dump
  - Criticality: No damage, investigation, dry runs,
    - 1 in 10Y
- Effect of the TSU's failure II: (worst case) asynchronous beam dump
  - Criticality: Availability,
    - 1 in 1Y



home.cern