LBDS overview on system analysis and design upgrades during LS1

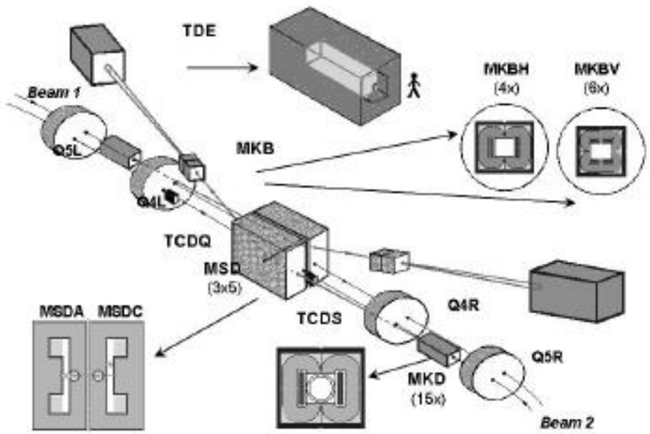
Roberto Filippini, Etienne Carlier, Nicolas Magnin, Jan Uythoven
CERN Workshop Machine Availability for post LS1 LHC, 28th Nov 2013

- Outline

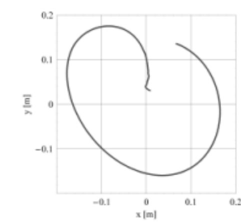
  - LBDS system analysis overview
  - Insights on tools and methodologies
  - System changes during LS1
  - Conclusions and outlook

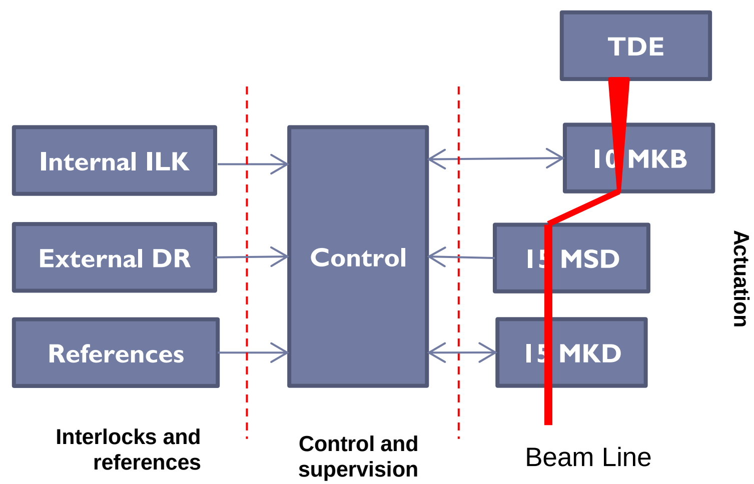
The LHC Beam Dumping System

- The LBDS is the final element of the protection chain, it performs the extraction of the beams <u>on demand</u> (dump requests) either at the end of machine fills or because of safety reasons. Two LBDS exist, one per beam.



LBDS physical layout – point 6





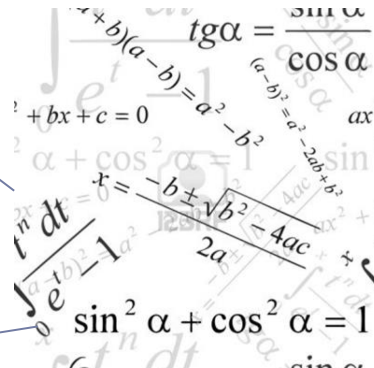
350 MJ destructive power

Functional layout

System analysis overview

Theoretical reliability models 2003-2006

Failure Statistics 2010-2012



Updated failure models

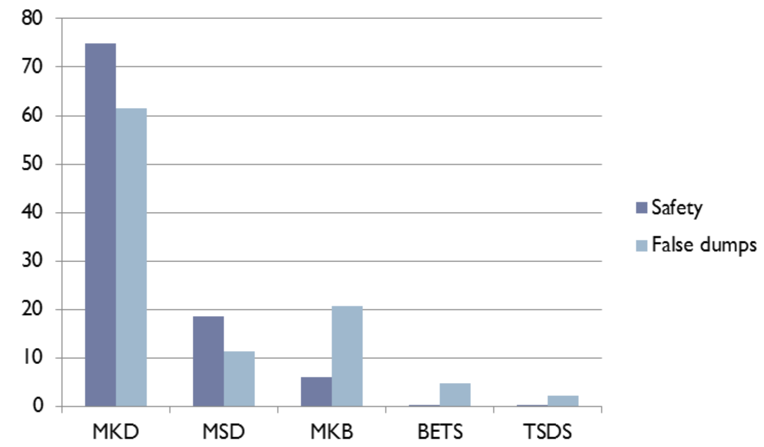
Special reliability studies
TCDQ - 2009
Triggering Synchronization and Distribution System - 2013

Estimates of availability and safety

LBDS system analysis 2003-2006

- The scope
  - TSDS, the beam energy tracking BETS, the septa MSD, extraction kickers MKD and dilution kickers MKB. Passive protection elements not in the scope.
- Assumptions
  - Operation profile of 10 hours, 400 machine fills, 200 days of operation
  - Post mortem diagnostics returns the system to an "as good as new" state
- Results
  - The LBDS is **SIL 4**
  - False beam dumps **8 +/- 2** per year
  - Asynchronous dumps **2** per year

MKD most critical system (74%) and main cause of false beam dumps (61%)



Failure statistics 2010-2012

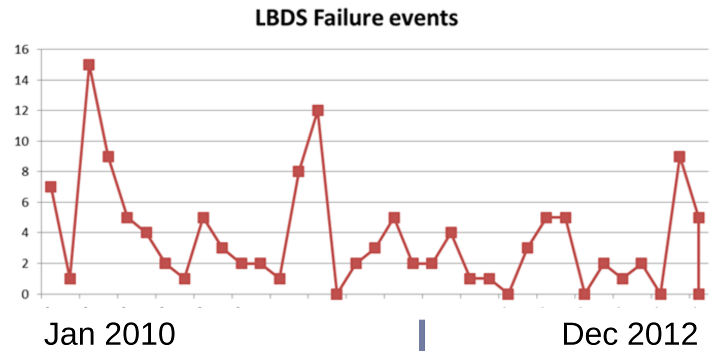
- The scope
  - MKD and MKB with control and supervision electronics and diagnostics
- Analysis of 3 years of LHC operation 2010-2012
  - Sources: LHC-OP logbook, and LHC-TE/ABT expert logbook

↓

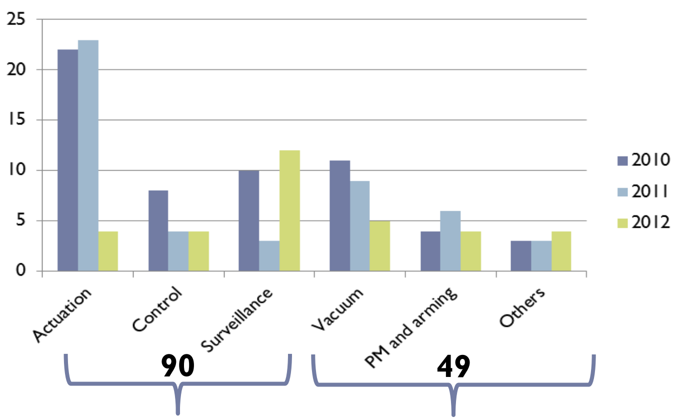
- Results
  - 139 failure events of which 90 internal to LBDS
  - Updated reliability prediction models
  - New failure mechanisms discovered
  - Availability and safety: comparison of predictions vs. statistics

Results → from raw data to statistics

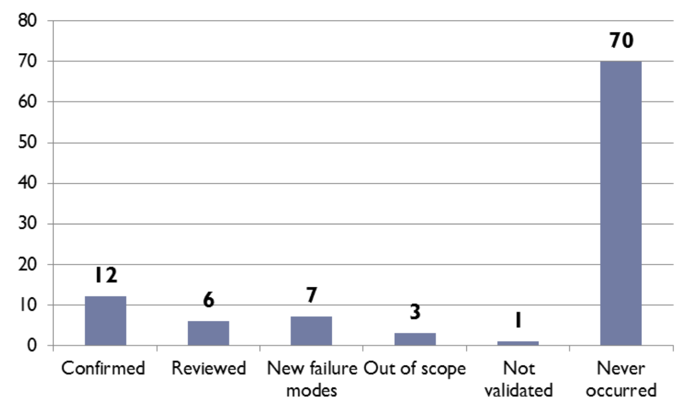
When→ Raw data series
139 failure events



Where → Failure distribution
90 within the LBDS



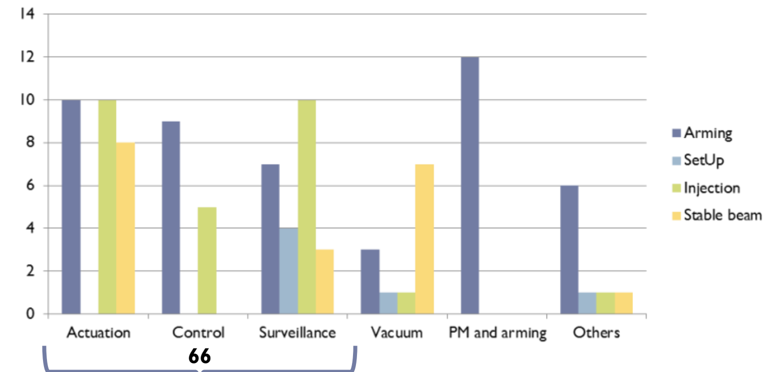
How → Failures modes observed
18 occurred over 99 identified
7 new failure modes



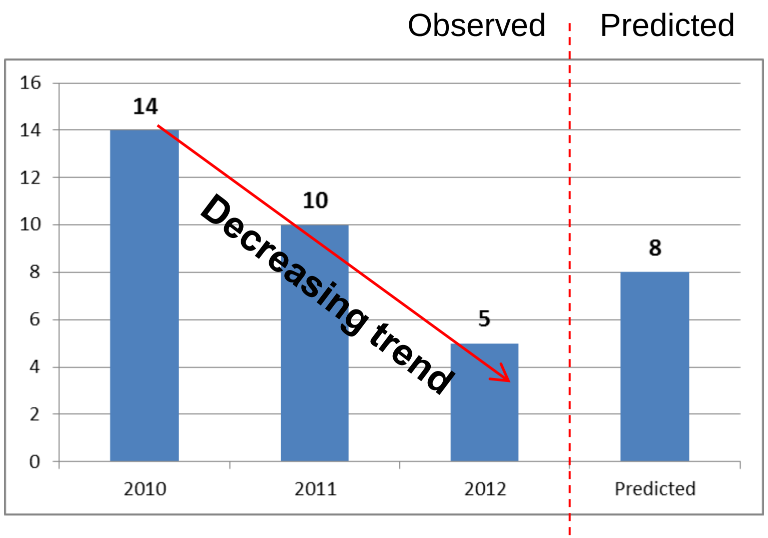
LBDS availability 2010-2012

- The LBDS counted **29 false beam dumps**, against 24 foreseen (8/year on average).
  - Actuation (15) then surveillance (12) and controls (2)

1- False dumps
66 apportioned to LBDS in every phase

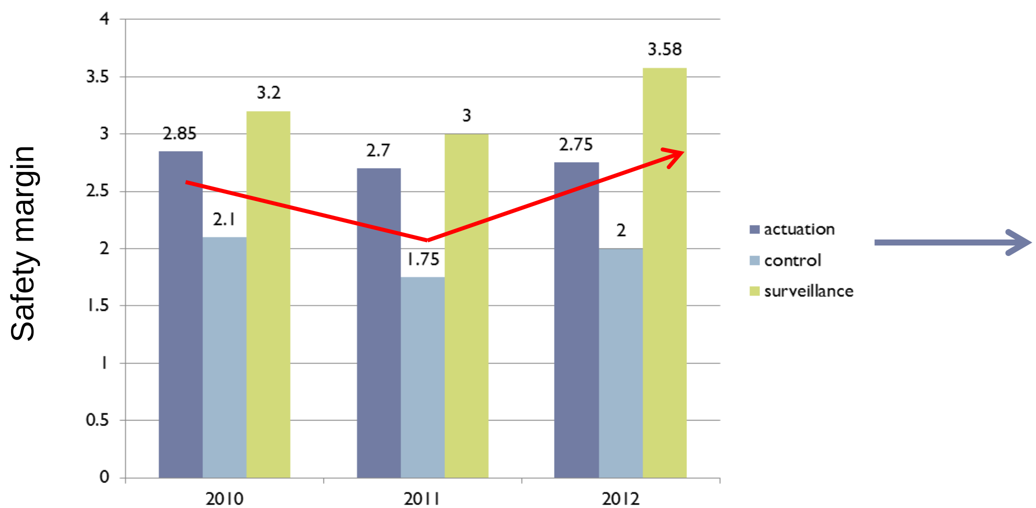


2 - Filtering
- Only LBDS false beam dumps in the phases injection and stable beam
- No repetition of the same internal dump request



LBDS safety 2010-2012

- Calculation of the safety margin at a dump request → loss of safety margins in 2011, and a recover in 2012, almost back to the initial levels of 2010
- SIL3 at least is met (hypothesis test)



Remark → too much safety margin leads to an unnecessary reduction of availability

The safety gauge

Tools and Methodologies - insights

Failure statistics
Statistical framework and inference tools

Tracking availability

Safety trade-off

Availability figures

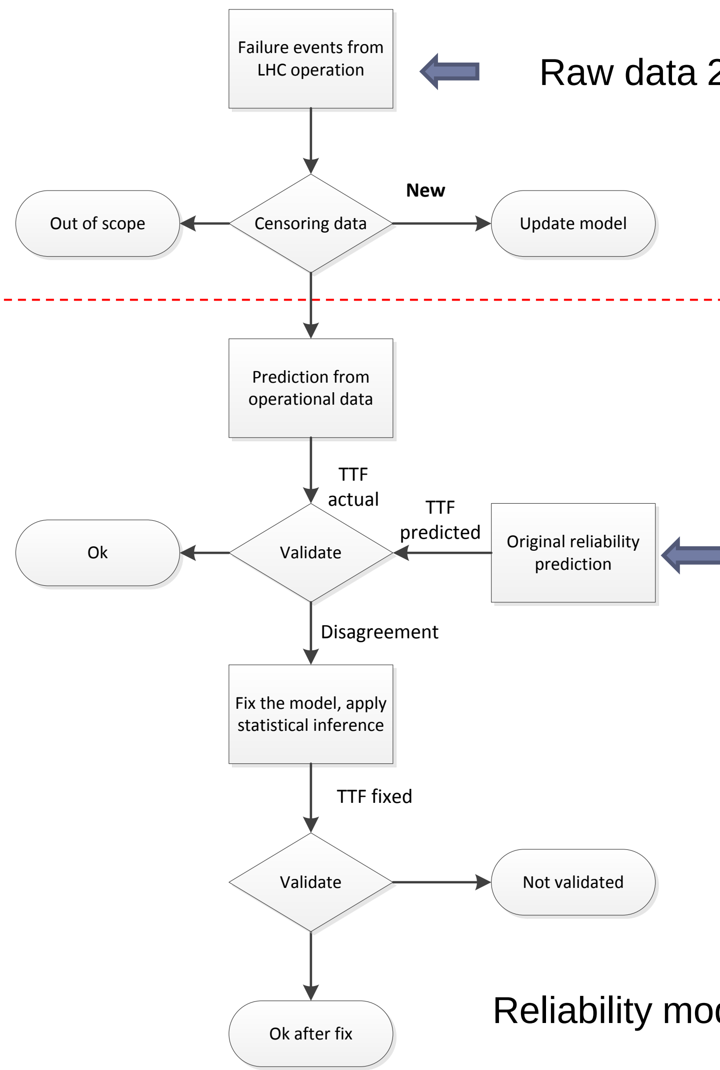
Tracking reliability
Advanced reliability prediction models

The statistical analysis framework

Raw data 2010-2012 IN

PHASE 1 – Censoring data

PHASE 2 – Statistics and validation



Predictions 2003-2006

Reliability models OUT

Failure modes and statistics – MKD system

Failure mode and identifier **# components** **Time to Failure** **Hypothesis test** **Time to recovery**

The underscored figure is the one validated. Population is counted for 2 LBDS. The raw estimate refers to [Years of operations] × [population] / [number of failures]. Hypothesis test is run with $\alpha = 0.05$.

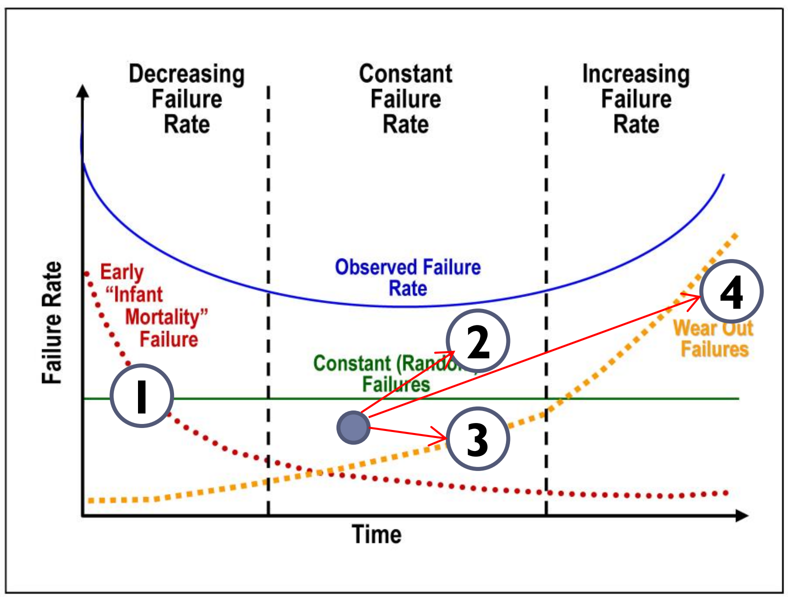
#	*Failure mode*	*Model*	*Population*	*TTF (years)* Raw	Corrected	Rel. pred.	H. test	*TTR (h:mm)*
1	MKD HV power supply breakdown	PSP1	30	3*30/7 = 12.8	β model	150		1:37
2	MKD PTU HV PS	HV	60	3*60/10 = 9	1-count 26	16	TRUE	2:18
3	MKD Compensation PS breakdown	PSOS1	30	3*30/6 = 15	1-count 18	113	FALSE	3:05
4	PTC tracking error	PTC, PTC3	80	3*80/2 = 120	1-count 240	103	TRUE	3:40 (singleton)
5	MKD Power switch degradation	SP2	60	3*60/3 = 60	P_D model	633	n.a. [1]	2:20
6	MKD PTC card failure	PTC1-3	80	3*80/1 = 240	-	1140	n.a.	1:44 (singleton)
7	MKB Power switch degradation	SW2	20	3*20/6 = 10	P_D model	633	n.a.	0:36
8	MKB HV power supply breakdown	PSH	20	3*20/1 = 60	-	152	TRUE	No data
9	MKB HV power supply degradation	Not in the model	20	3*20/3 = 20	1-count 60	114	TRUE	1:18
10	MKD PTC power supply	PTC	80	3*80/1 = 240	-	114	TRUE	2:03 (singleton)
11	MKB Magnet sparking	Not in the model	20	3*20/1 = 60	-	-	n.a.	No data
12	MKD Peltier cooling element	Not in the model	30	3*30/4 = 22.5	Removed	-	n.a.	No data

Validation
most conservative value is kept

Advanced models for reliability prediction

- Goal → How to capture anomalies from observations
  1 Reliability growth models
  2 Interaction-dependency models (CCF)
  3 Inaccurate diagnostics
  4 Stress models
  5 Failure on demand

Component Failure rates should always stay in the flat region



5

Failure on demand
Model apart

Tracking Availability

- Narrow scope
  - Faults that only manifest in operation → false beam dumps

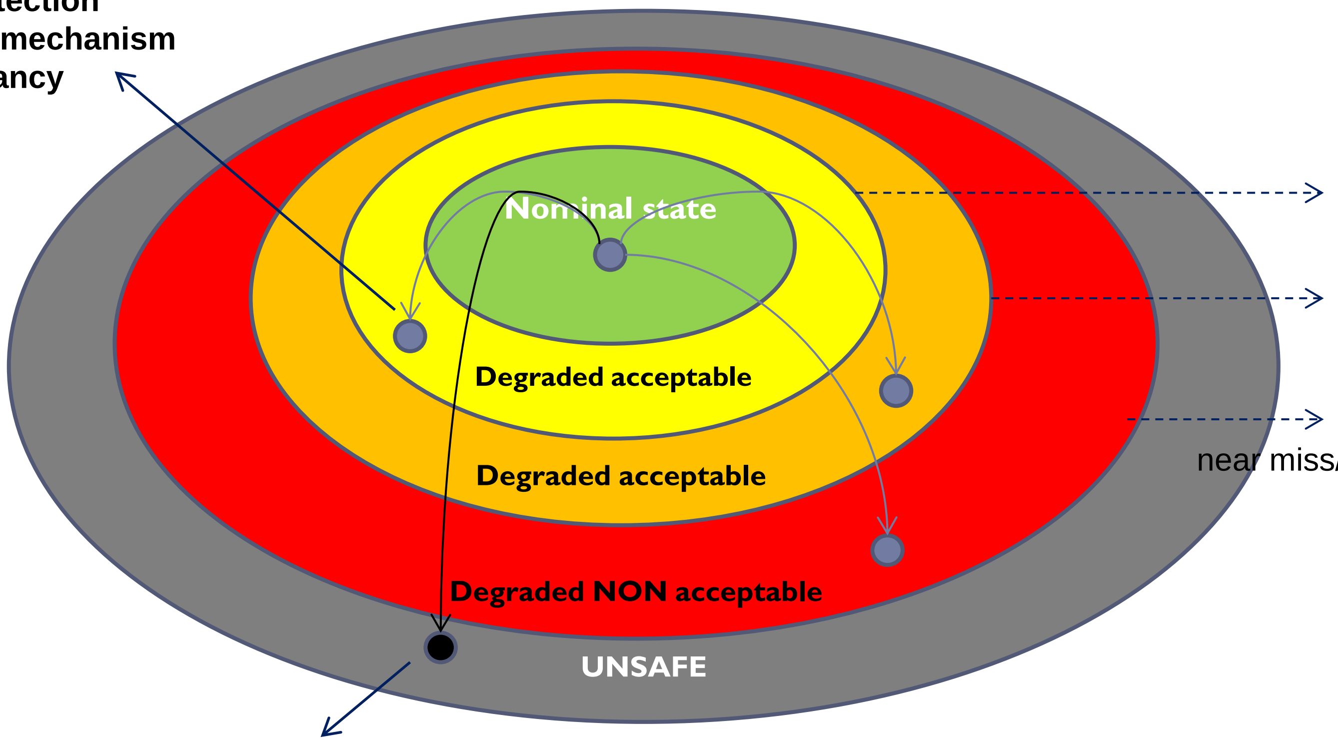
- Large scope
  - Any fault that impacts (and retards) on the operation schedule

- Systemic → balance safety and availability
  - Is the system protected or overprotected?
  - Safety margins and safety policies
  - Trade-off and optimization

Safety margins

- **A state based approach →** safety by design guarantees that failures do not develop further and let the system operate at sufficient safety margins

1 - Fault detection
2 - Failsafe mechanism
3 - Redundancy



2 safety margin

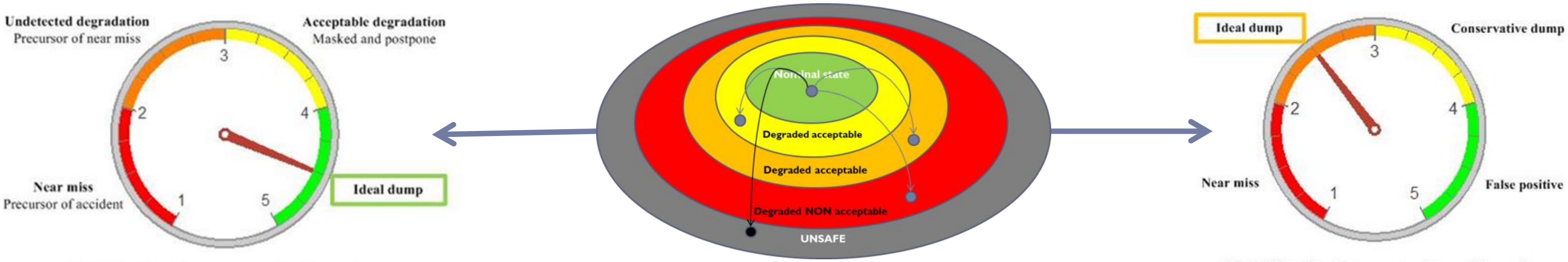
1 safety margin

Zero safety margin
near miss/single point of failure

Single point of failure

The safety gauge

- **Balance safety and availability**
  - Which ideal safety policy?
  - Quantify the safety margins at every beam dump → black box model



(i) LBDS safety distance at nominal beam dump

(ii) LBDS safety distance at an internal beam dump

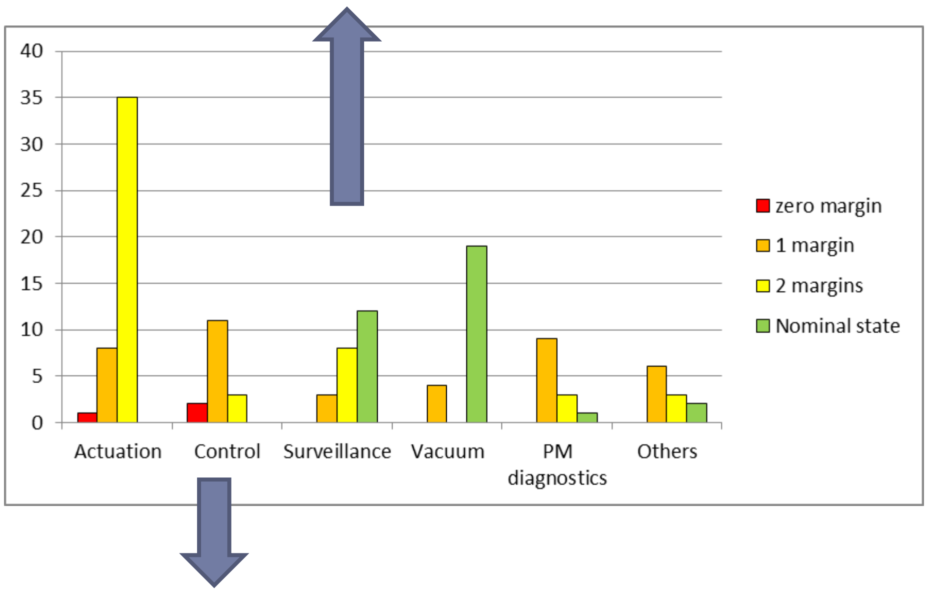
Nominal beam dump
The system is fully available or in an acceptable degraded state

False beam dump
The internal dump must be justified → safety margin about to be eroded

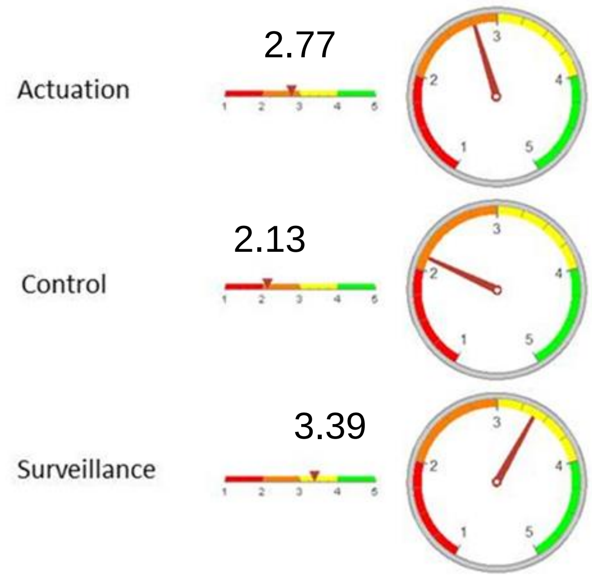
Example: Safety margins for the LBDS

1. Every system was calculated a safety margin at the beam dump
2. The **average safety margin** was calculated over 2010-2012

Surveillance function is unbalanced against availability (over-protection)



Control function (TSDS) is the closest to the safety margins



Average safety margins at an internal beam dump

Design upgrades during LS1

Additional re-trigger from BIS
Upgrade of TSU cards
Distribution TSU over three crates

Electronics

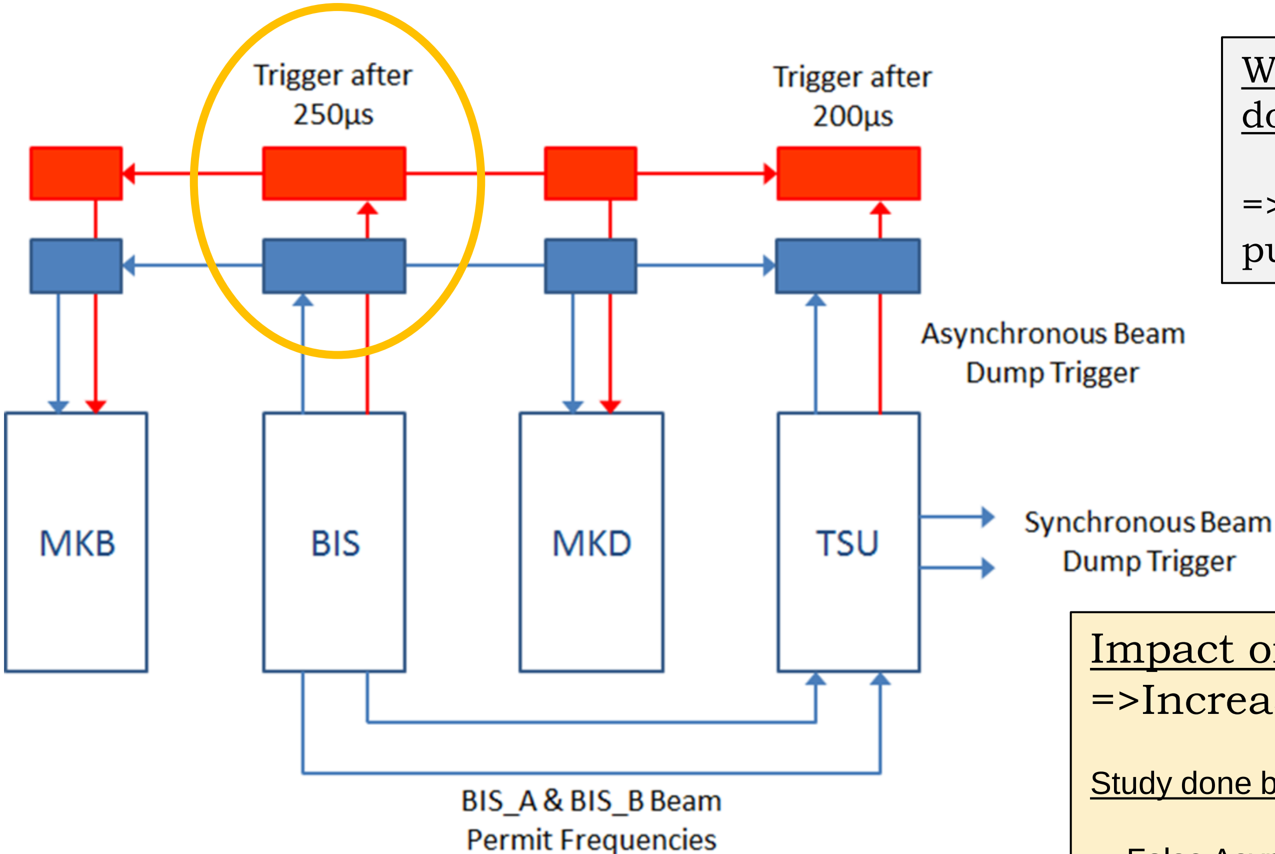
Magnets

Powering

Changes to HV generators
Upgrade of PTUs
UPS configuration

Add 2 MKB magnets per beam
Add shielding in MKD MKB cable ducts
MKB vacuum

Design update during LS1: Additional re-trigger from BIS



What happens if TSU cards do not send the triggers ?

=> BIS sends retrigger pulses after 250 us.

Goal:
Increase SAFETY

Impact on availability:
=>Increase of async dump rate ?

Study done by V.Vatansever:

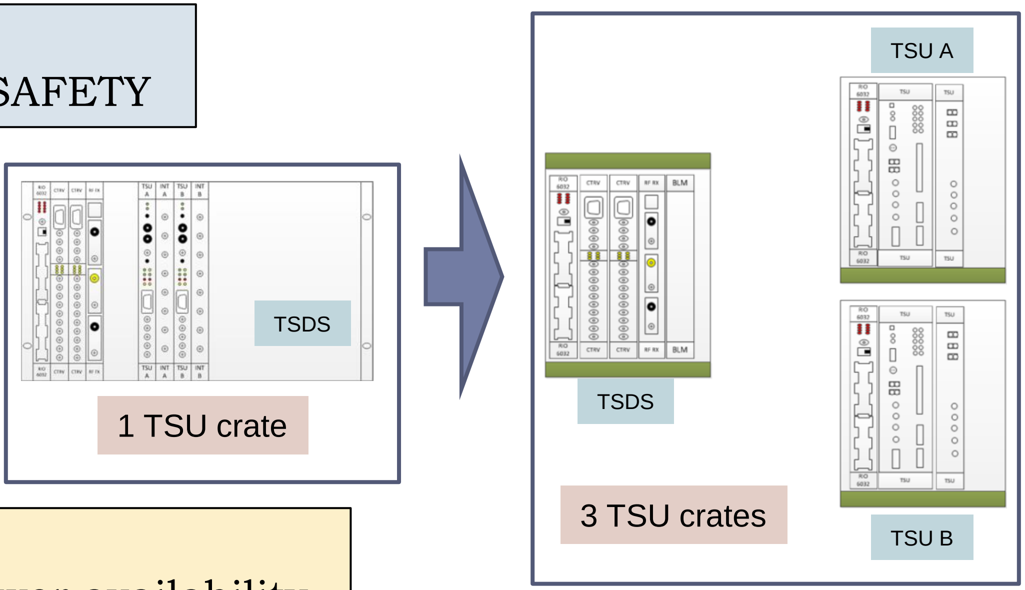
- False Asynchronous beam dumps in 10 years:
  ⇒Specified: **2** / Calculated: **0.025**
- False Synchronous beam dumps per year:
  ⇒Specified: **2** / Calculated: **0.011**

Design update during LS1: Upgrade of TSU cards

Motivation:
- External review of TSU v2 card (2010);
- CIBU power filter problems (2011);
- Internal review of LBDS Powering (2012);
- +12V problem in TSU VME crate (2012);
- Improvement of surveillance & diagnosis needed.

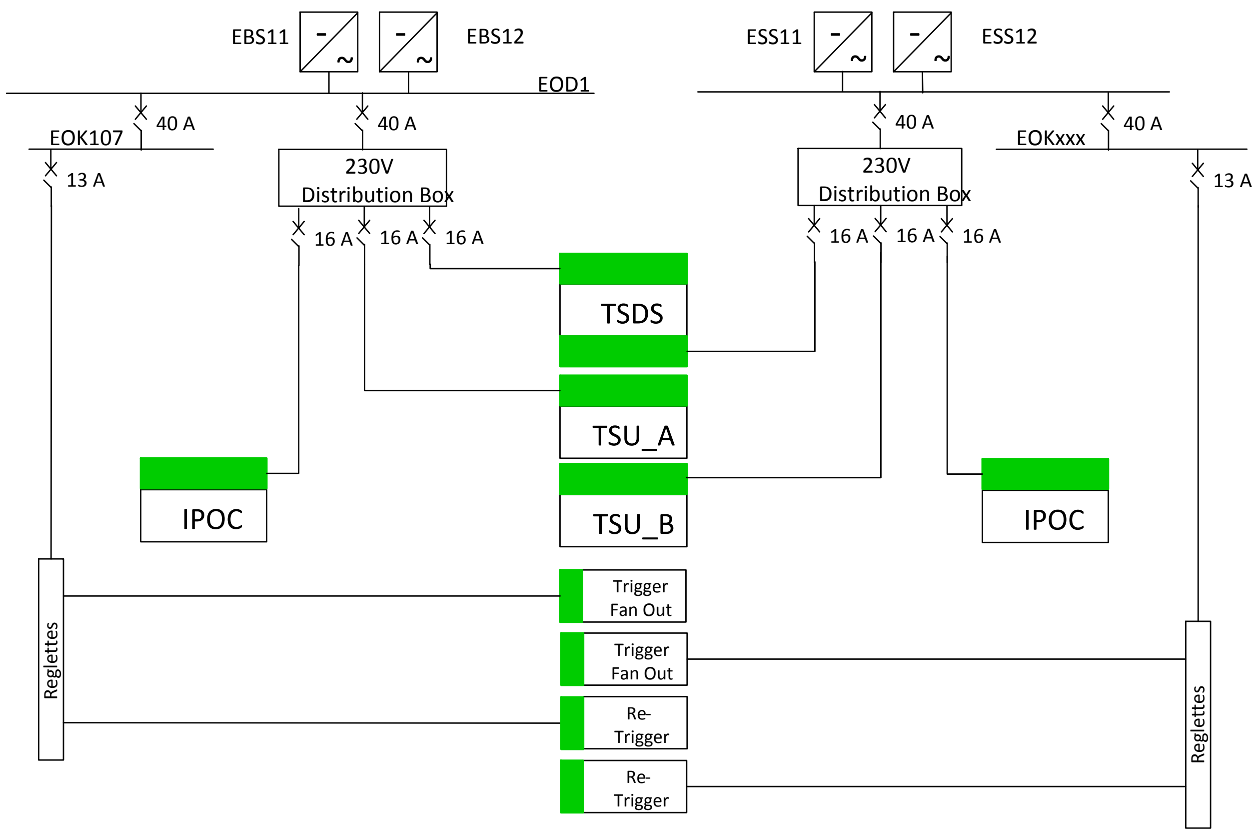
Implementation:
- Design of a new TSU card (v3)
- Deployment of the TSU cards over 3 separate crates

Goal:
Increase SAFETY



Impact on availability:
More surveillance systems => lower availability

Design update during LS1: LBDS powering modifications



- Add a separated connection to a second UPS (US65) for LBDS
- Individual circuit breaker for each crate PSU (Distribution Box)
- Software monitoring of all crate redundant PSU

Goal:
Increase SAFETY

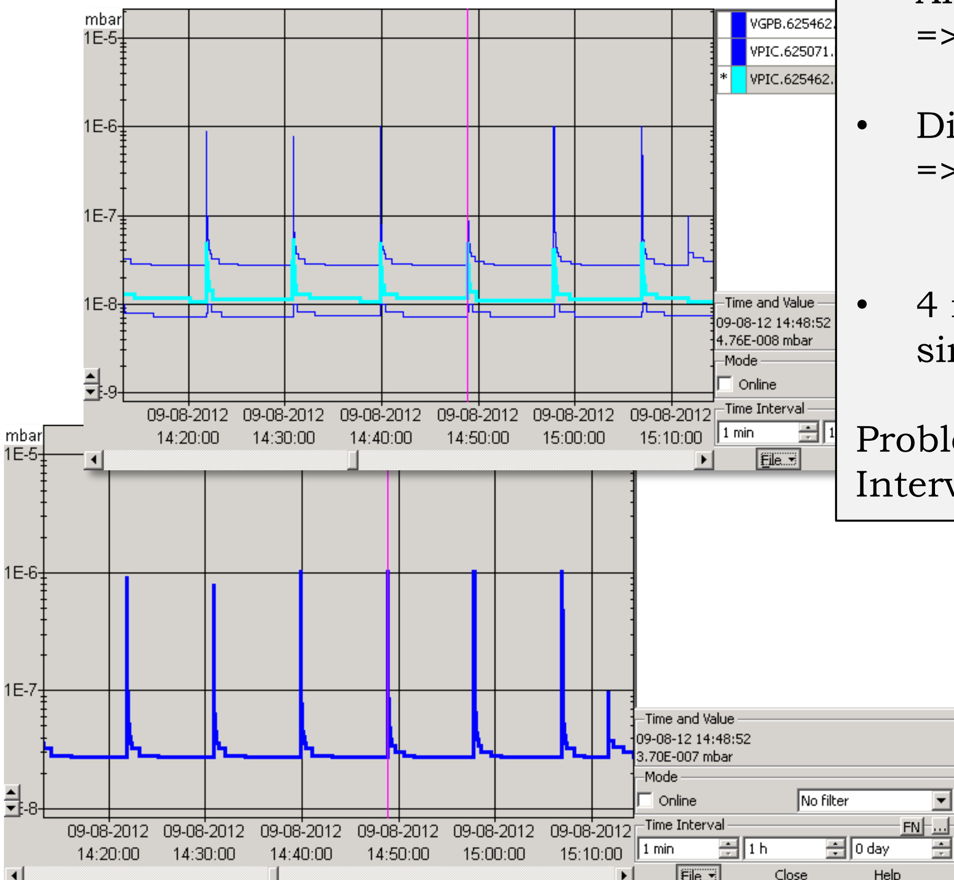
Impact on availability:
More surveillance systems => lower availability

Design update during LS1: Add 2 MKB magnets (1 tank) per beam

Goal:
Increase SAFETY

Impact on availability:
2 more MKBV (over 4 during LHC Run1):
- Increased risk of erratic triggering
- Increased risk of magnet flashover

Design update during LS1: MKB vacuum



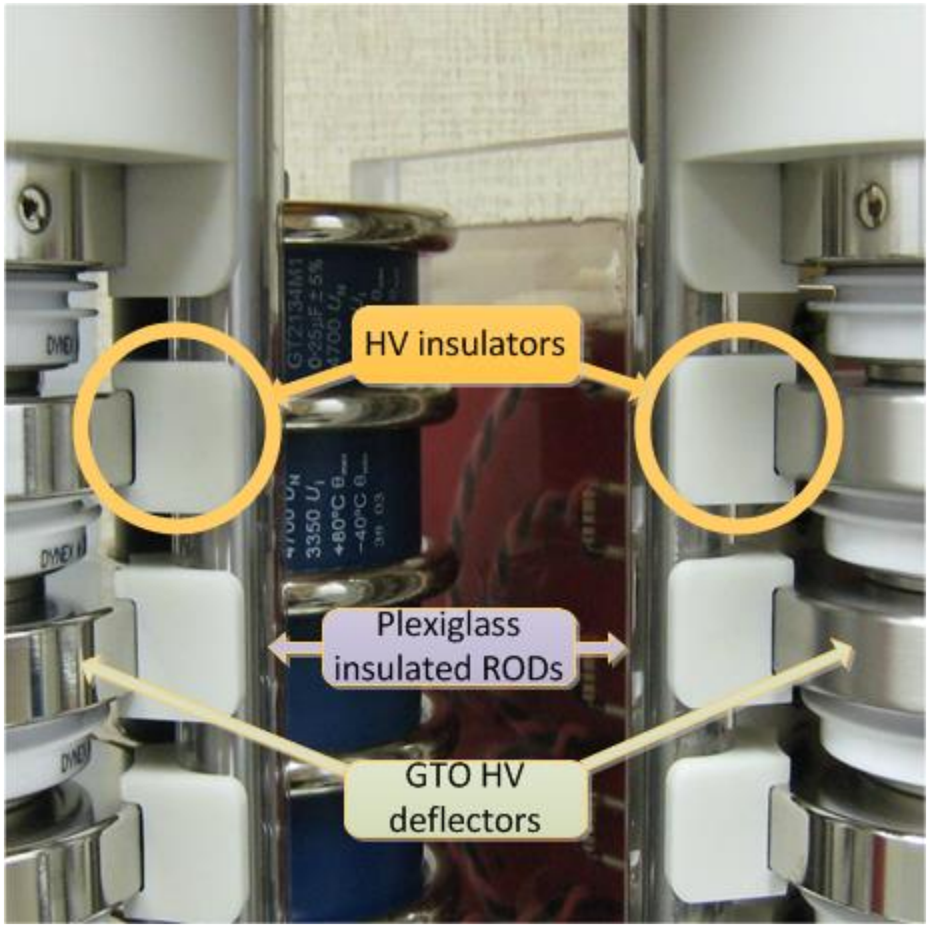
Courtesy of Fabien ANTONIOTTI

- Analogue signal very noisy
  => Masked since the beginning !
- Digital signal experienced glitches/spikes
  => Many dumps due to this problem !
  (**13 during LHC Run 1**)
- 4 noisy vacuum probes masked in XPOC since the beginning

Problems identified by TE/VSC:
Intervention is planned.

<u>Goal:</u>
Increase AVAILABILITY

Design update during LS1: Changes to HV generators



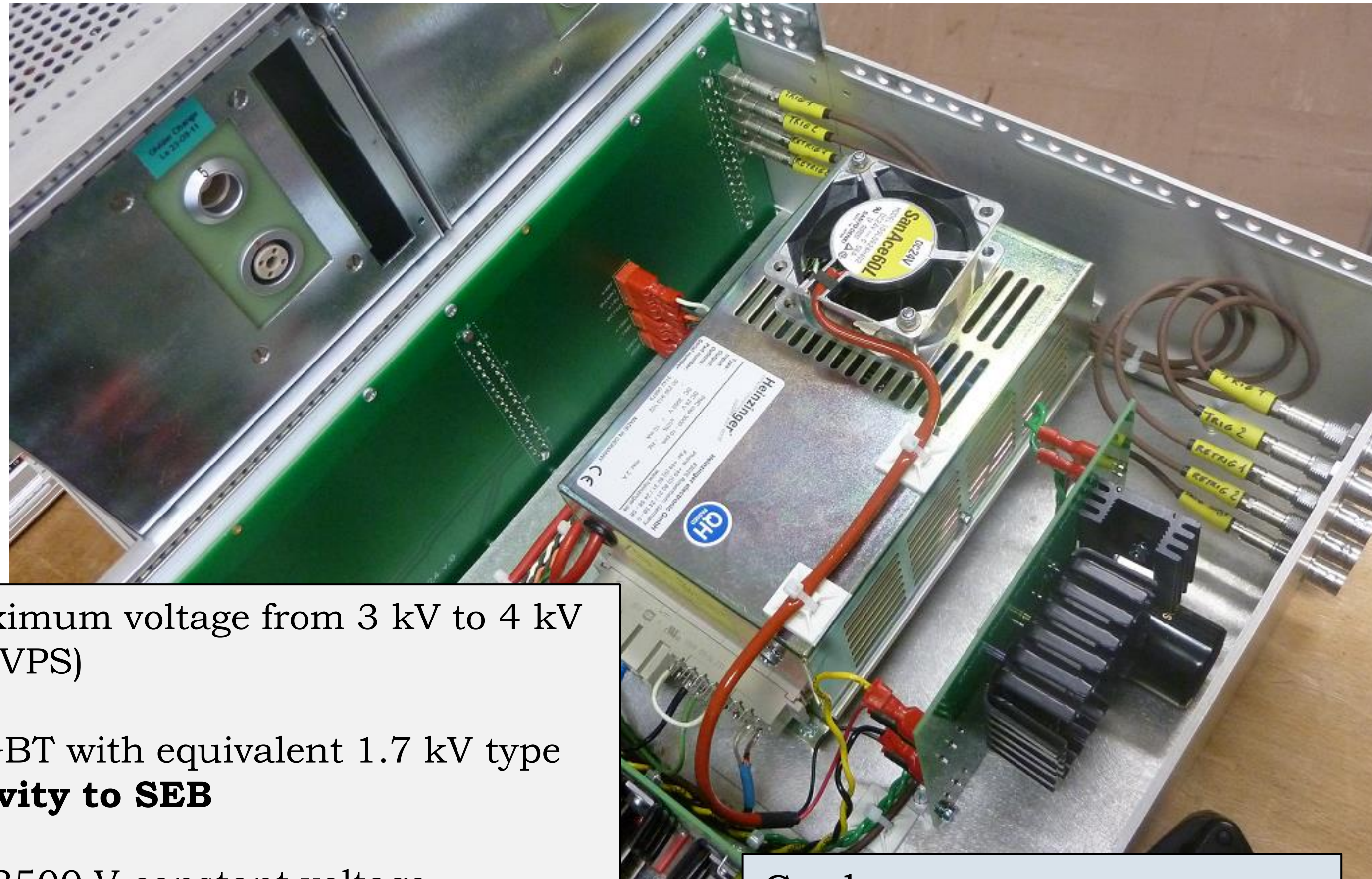
Sparking in the GTO stacks causing self-triggers: (operation limited to 5 TeV)

=> **HV insulators** are added between:

- Return current Plexiglas isolated rods;
- GTO HV deflectors.

Goal:
Increase AVAILABILITY

Design update during LS1: Upgrade of PTUs



- Increase PTU maximum voltage from 3 kV to 4 kV (replacement of HVPS)
- Replace 1.2 kV IGBT with equivalent 1.7 kV type => **better sensitivity to SEB**
- Operate PTU at ~3500 V constant voltage
  => Increased GTO gate current
  => **less GTO wear out**

<u>Goal:</u>
Increase AVAILABILITY

Design update during LS1:
Add shielding in MKD & MKB cable ducts

Add shielding in all MKD & MKB cable ducts between UA and RA:

=> less SEB problems

<u>Goal:</u>
Increase AVAILABILITY

System analysis and recommendations (1)

- Safety by design → implementation issues
  - Prevent the generation of erratic triggers (MKD)
  - Loss of redundant chains and Common Cause of Failure (all)
  - Overlap between control functions and safety functions (TSDS)

- Safety by design → functional, systemic issues
  - Analysis of rare events (e.g. "Swiss cheese" models)
  - Safety measures as possible source of hazards
  - Functional dependencies and domino effects

- Tools
  - Safety standards
  - System analysis qualitative and probabilistic methods
  - Fault tracking → monitor that every components stays in the flat region and identify anomalies (aging? dependencies? stress?)

System analysis and recommendations (2)

- Scale up risks → operating at higher energies may demand tighter margins of safety and impact on availability

1. Review of the existing safety chains
   - Review SIL in the light of possible increased risks
2. New hazards or existing hazards that become safety relevant
   - New safety chains and interlocks after LS1 changes
   - New failsafe mechanisms as sources of false beam dumps

- Tools
  - Risk analysis
  - Real-time estimate of safety-availability balance → the safety gauge

… <u>export the safety gauge (safety margin) concept</u> to every system that has a non trivial safety-availability trade-off - it returns a metric easy to understand and that can be shared throughout designers and operators

Conclusions

- Analysis of LBDS over 2010-2012 returned overall satisfying statistics
  - Availability and safety improved along the operational period.
  - Anomalies sorted out.
  - Theoretical models in line with observations
- Experience in methodologies is encompassing
  - Hazards → system analysis → safety by design
  - Innovative methodologies → safety gauge
- All design upgrades are safety-availability informed

…

Conclusions (2): design upgrade during LS1

SAFETY is our main concern !

Most of important changes for **SAFETY improvement**…

…Perhaps **reducing AVAILIBILITY** !

Nonetheless, many changes are performed to **improve AVAILIBILITY**…
…where **SAFETY is not impacted**.

...question time

Roberto Filippini
email: rob.filippini@tiscali.it

Spare slides - recommendations

Sensitivity to unknowns

- Some failure modes were not foreseen in the theoretical model (7 over 26 recorded)
- Their impact is significant in the overall safety figures
  - They reduced the safety margin or impacted on availability

Function	*With new failure modes*	*Without new failure mode*
Actuation	2.77	2.86 ↑
Control	2.13	2.58 ↑
Surveillance	3.39	2.85 ↓

R. Filippini, J. Uythoven Review of the LBDS safety and reliability analysis in the light of the operational experience 2010-2012, CERN-ATS-Note-2013-042 TECH. 2013

Recommendations (1)

- Further investigations on failure mechanisms
  - Common Cause Failure suspected in a few components such as the failure of three High Voltage power supplies in the MKD generators, two Triggering Units not responding, and the spurious firing of two Trigger Fan Out units. Further analysis on CCF and consequences on reliability is recommended.

- Availability concerns
  - 7 false beam dumps are from the vacuum
  - 12 failures from post mortem and diagnostics => cause of delays in re-arming
  - Diagnostics was not always accurate, faults fixed after several interventions
  - Some functions might be over-protected, e.g. LBDS surveillance

- Safety concerns
  - SIL3 is largely met for LBDS, SIL4 possible but further analysis is recommended
  - The control functions of the LBDS (TSDS) is estimated to have the smallest safety margin.
  - HW changes during LS1 in TSDS (controls) and powering.

Recommendations (2)

- Data quality
  - Good and large quantity, but inconsistencies existed as well as non-homogeneities in the data reporting, time stamps, consequences from diagnostics and intervention
  - Improvements during the years should be consolidated by the definition of standard procedures of data reporting and tools for the automatic information retrieval

- Product assurance
  - Several components did not meet the reliability specification because of design flaws, and were returned to the manufacturer (e.g. Asibus®, Power trigger power supply).

- Other issues
  - Maintenance, and diagnostics had a relevant impact on operation
  - A number of faults/errors are procedural (human factor) and should be taken into account for a more detailed analysis

Spare – Failure models

Control and surveillance functions (spare)

Not validated

#	Failure mode	Model	Population	TTF (years)				TTR (h:mm)
				Raw	Corrected	Rel. pred.	H. test	
1	TSDS TSU spurious trigger	O, PL, S2, CLK	4	3*4/3 = 4	1-count 12	320	n.a.	No data
2	SCSS voltage tab. corrupted	Not in the model	2	3*2/1 = 6	-	-	n.a.	No data
3	BEM anybus error	TX1,TX2, TX3	50	3*50/5 = 30	1-count 150	380	TRUE	0:37:00
4	TDSD fan out spurious trigger	TO2	100	3*100/2 = 150	β-model	16000	n.a.	1:20:00 (singleton)
5	TSDS TSU fail in both LBDS	C1, DR1, TO1	4	3*4/4 = 3	β-model	157	n.a.	0:36
6	SCSS PLC Dout board failure	Not in the model	150	3*150/1 = 450	-	-	n.a.	3:05 (singleton)
7	TSDS VME crate PS breakdown	Not in the model	2	3*2/1 = 6	-	-	n.a.	No data
8	RTB out box, fail silent	OUT, DT1, C1	60	3*60/2 = 90	P_D model	726	n.a.	0:26 (singleton)
9	RTB in box, VD fail silent	IN	300[1]	3*300/1 = 900	Removed	162	n.a.	No data

#	Failure mode	Model	Population	TTF (years)				TTR (h:mm)
				Raw	Corrected	Rel. pred.	H. Test	
1	BEA power supply	Not in the model	50	3*50/3 = 50	-	-	n.a.	1:29:00
2	Voltage divider	VD	160	3*160/3 = 160	-	1140	n.a.	0:37:00 (single data)
3	BEI energy tracking table	ER1, ER3	50	3*50/1 = 150	-	386	TRUE	1:25:00 (single data)
4	BEA TX module stuck at timeout error	TX1	50	3*50/1 = 150	-	786	n.a.	No data
5	SCSS PLC Din board failure	Not in the model	108	3*108/1 = 324	-	-	n.a.	0:50:00 (single data)
6	SCSS PLC cabling failure	Not in the model	-	-	Removed	-	n.a.	No data
7	SCSS Asi Bus SEU	Not in the model	4	3*4/10= 1.2	1-count 6	-	n.a.	3:07
8	BEM anybus error	TX1, TX2, TX3	50	3*50/2 = 75	1-count 150	380	TRUE	3:20

Failure on demand

- The failure model on demand assumes that the contribution to the failure is twofold:
  - Constant failure rate □
  - Probability on demand P_D

Average failure rate $$\frac{P_D N}{T} + \lambda = \frac{1}{TTF_{data}}$$

- Example: MKD power switch
  - 60 components, predicted (633) and calculated (60) TTF disagree, a probability on demand model is applied and results in P_D = 3E-06.

- Failure mode validated with corrected model

Failure Dependency

- The beta model assumes that the behavior at failure of similar components is not fully independent
  - The dependency is quantified by a beta factor (math. steps omitted)

$$TTF_{data} = (1 - \beta)TTF$$

- Example: MKD HV power supply breakdown
  - 30 components, predicted (150) and calculated (13) TTF disagree. A **Common Cause Failure** beta-model is introduced in addition to the constant failure rate => beta = 0.9 which is high.

- Failure mode validated but further investigation suggested

Hypothesis test

- The **hypothesis test** verifies that the assumption on the predicted TTF is true on the basis of the observations
  - The test consists of calculating the probability that the number of observed failures k_1 over a time T is compatible with the assumed distribution => the null-hypothesis H_0

$$P_0(k \geq k_1) = 1 - \sum_{k=0}^{k=k_1} p_0(k,T) = \begin{cases} > \alpha = 0.05 \Rightarrow H_0 \text{ is true} \\ \leq \alpha = 0.05 \Rightarrow H_0 \text{ is false} \end{cases}$$

- Example: Power Trigger HV Power supply
  - 60 components, predicted (9) and calculated (16) => TTF slightly disagree.
  - The hypothesis test is True.

- Failure mode validated after hypothesis test

Safety metrics

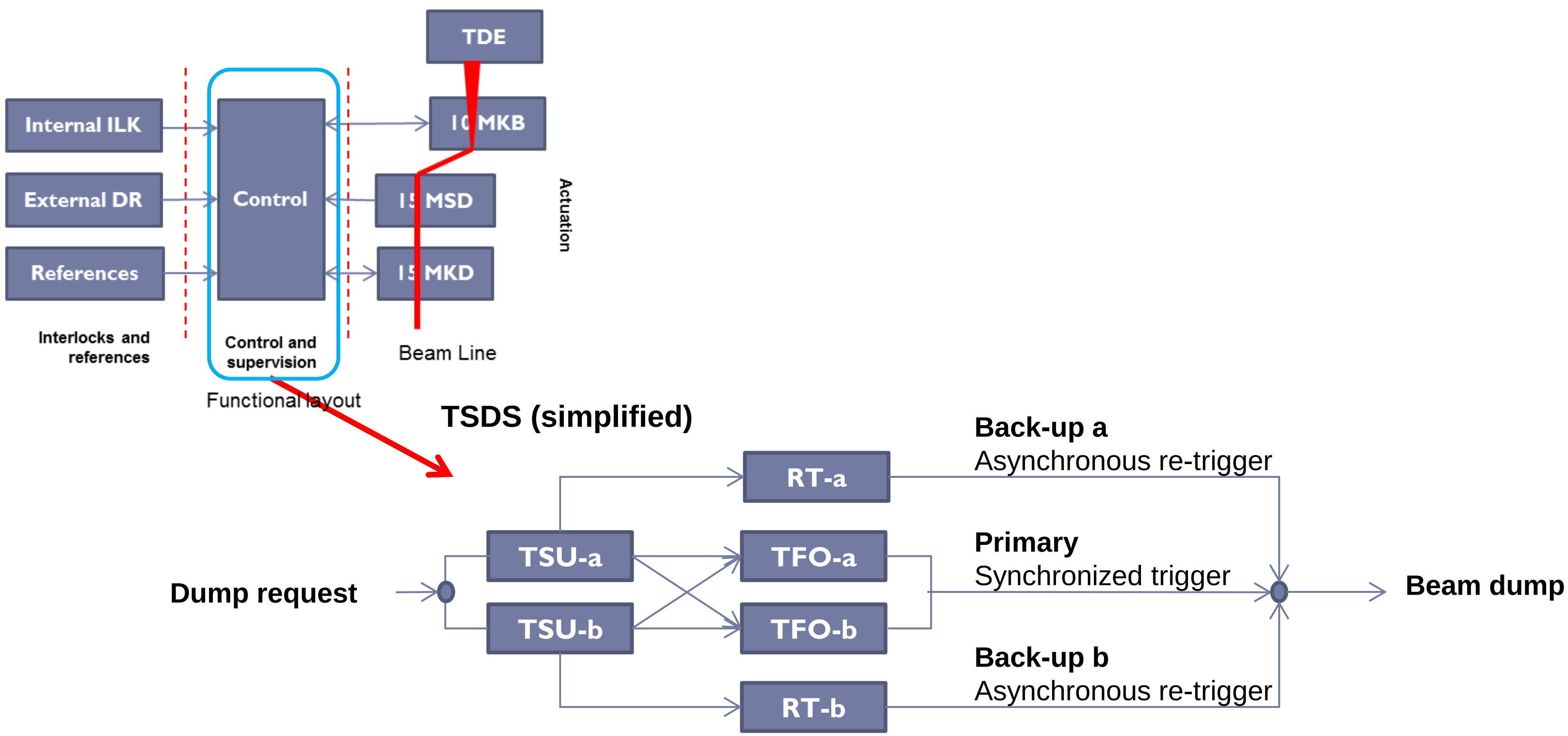
- The problem
  - The evidence that all beams were safely dumped at every beam dump request for LBDS is a necessary but not sufficient condition to state that the system is SIL3 at least

- Rare events are hopefully not recordable but… their early development can be observed
  1. Look for near misses and close to near misses
  2. Identify the event driven failure dynamics
  3. **Set a metric for safety → safety margin**
  4. Estimate SIL on the calculated safety margin

Spare - Safety

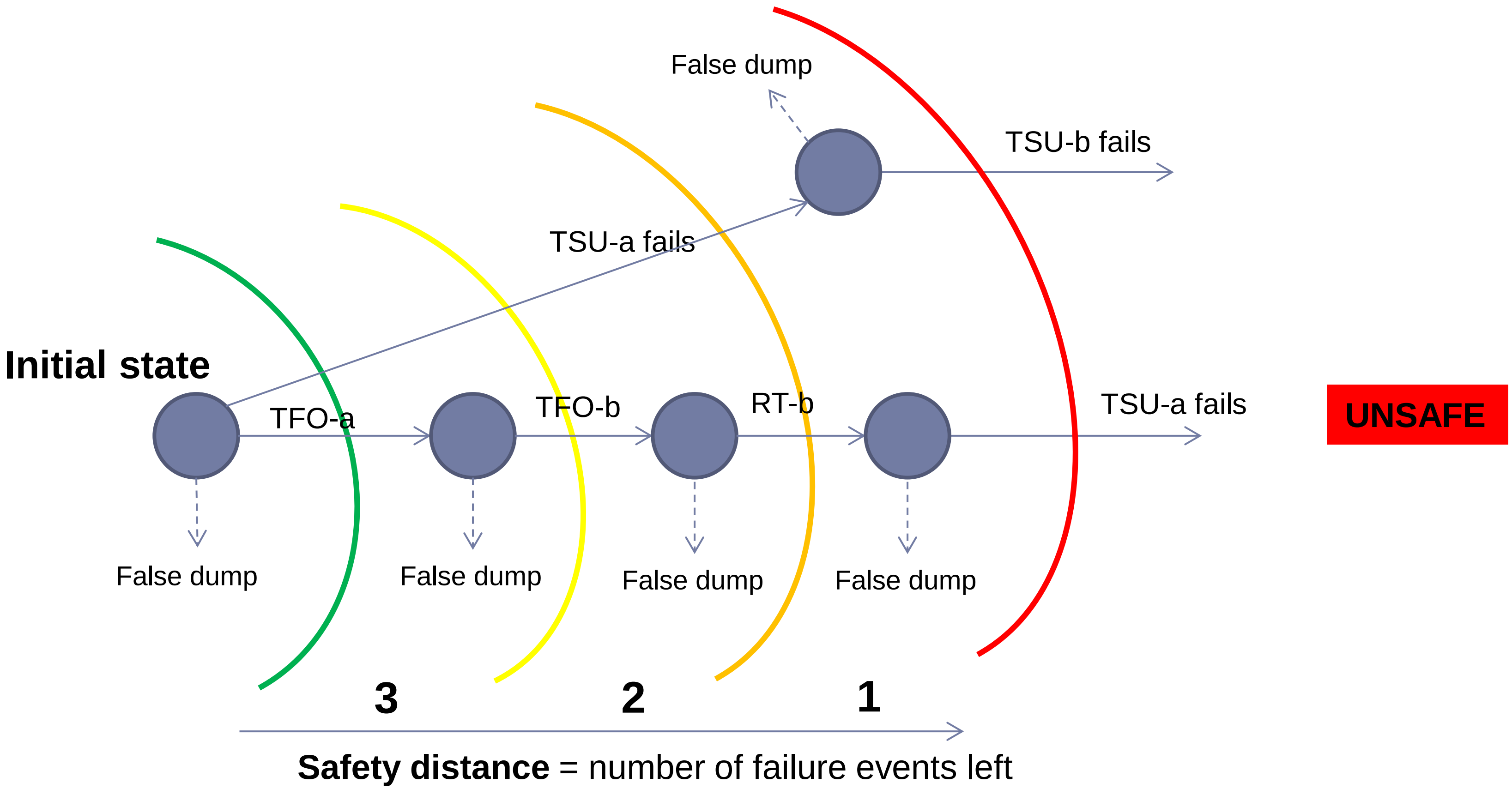
LBDS and safety by design

- The behavior at failure of the LBDS is conceived in order to …
  - Tolerate faults by redundancy => fault masking
  - Prevent faults by surveillance => failsafe



Example: TSDS and safety distance

- Simplified state transition diagram of the TSDS
  - Some failure events may be detected and trigger a false dump

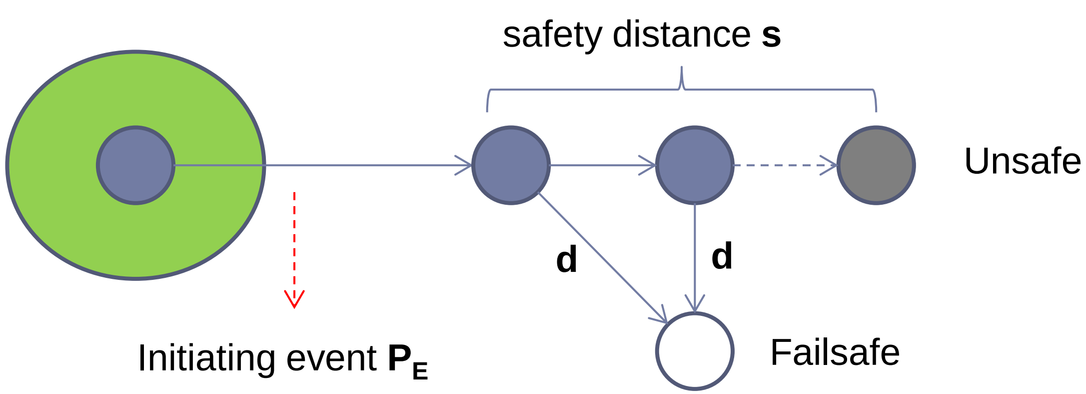


Actual safety (0)

- **Extreme outcomes and singularities**
  - failure events that moved the LBDS to a potentially unsafe state, or close to it (near miss) before this was discovered.
- 1 erratic trigger of 2 MKDs over three years, from 30 independent TFO outputs
  - The maximum failure rate threshold in order to be SIL3 at least is 7.2 E-05/h which is met.
- 2 failure at zero safety margin (detected) in the actuation and control functions, in 3 years
  - The maximum failure rate threshold for the control is 7.8 E-05. and the one for the actuation is 1.1 E-03, which are both SIL3 at least.

Actual safety (spare1)

- Problem statement
  - Given the average safety distance at failures for each LBDS function, over the period 2010-2012, the objective is to calculate the maximum component failure rate below which LBDS is SIL3, for 300 days per year (total = 21600 h) with an average machine fill of 10 hours
- Data…
  - P_E = probability of the initiating events (90/21600)
  - N = 1674 number of components at failures in the LBDS
  - s = safety distance
  - d = detection rate; 0.73 for LBDS, 0.6 (actuation), 0.87 (control) 0.96(surveillance)



Actual safety (spare 2)

- The average failure process is approximated to a Poisson process, initiated by the initiating event E
- The system is safe if the probability of failure over one machine fill is SIL3 at least => the following **test** is a sufficient but not necessary condition for being SIL3

Continuous Poisson CDF

$\square_{SIL3}$= 1xE-07/h

$$P = P_E \underbrace{[1 - F(d, N, \lambda, T, s)]}_{\text{residual safety margin}} < \underbrace{1 - e^{\lambda_{SIL3} T}}_{\text{SIL3 bounds}}$$

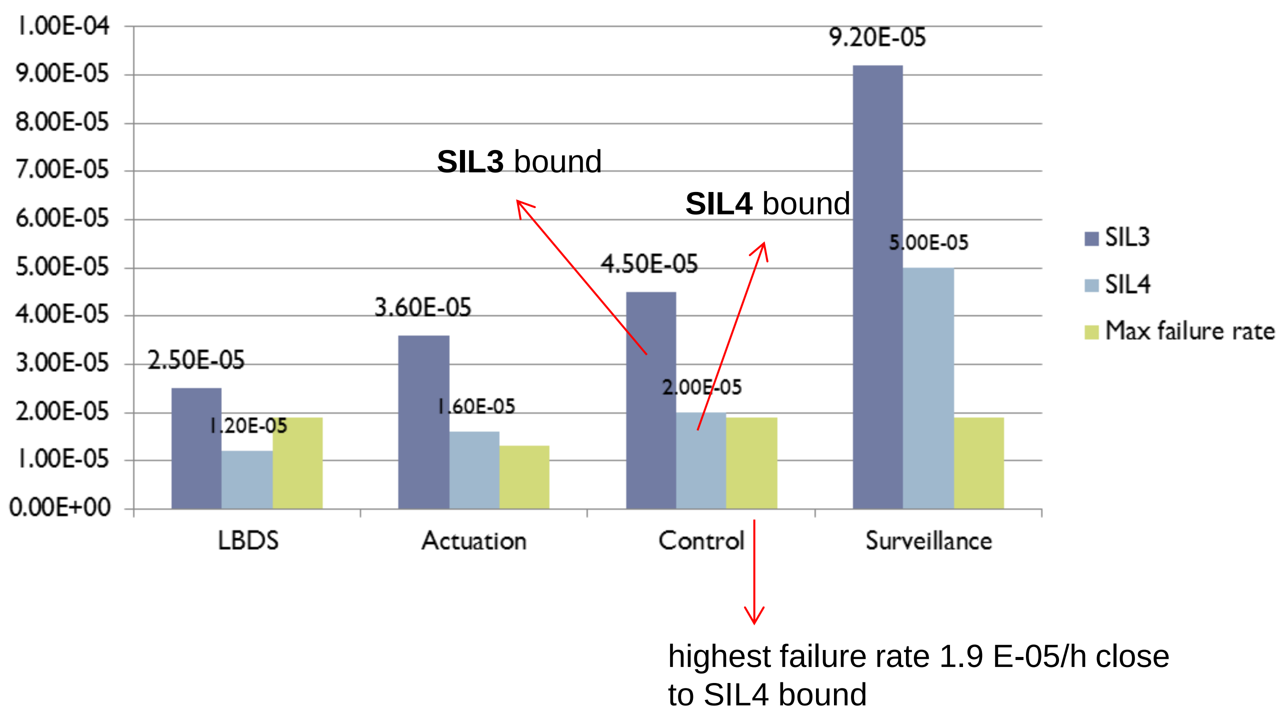
Initiating event

Probability of exceeding the safety margin s

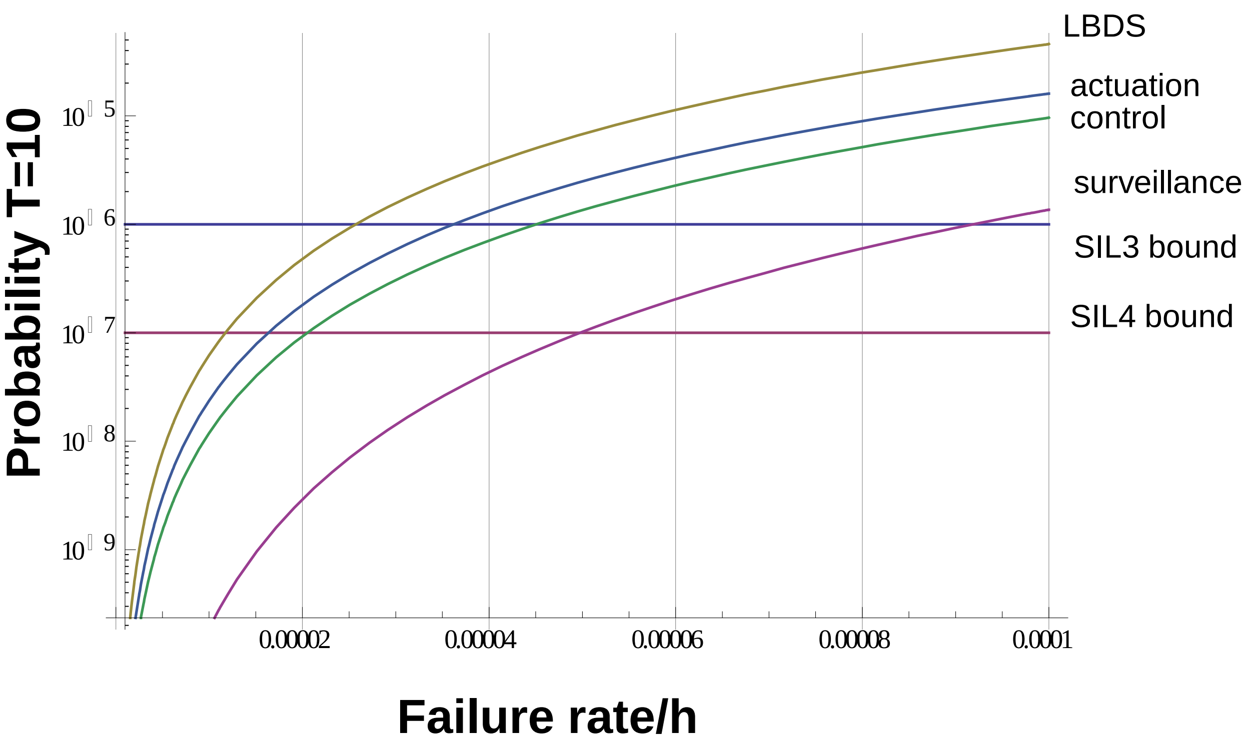
The failure rate threshold

Actual safety (3)

- Actuation, control, and surveillance functions **meet the safety requirements** individually and together as LBDS
  - Example: LBDS SIL3 bound is 2.5 E-05/h - the highest rate is from the TSDS VME crate power supply failure =1.9 E-05/h with all other components being more reliable.



Safety: SIL3,SIL4 graphical tests



LBDS safety gauge 2010-2012

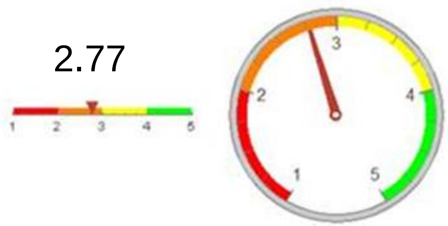
Table 1: Distribution of safety margins from operational failure data

	Zero-margin	*1-margin*	*2-margin*	*3-margin*	*Safety distance*	
					Average[1]	Variance
Actuation	1	8	35	-	2.77	0.23
Control	1	11	3	-	2.13	0.24
Surveillance	-	3	8	12	3.39	0.5
LBDS	2	22	46	12	2.82	0.5
Vacuum	-	4	-	19	3.65	0.57
PM diagnostics	-	9	3	1	2.38	0.39
Others	-	6	3	2	2.63	0.56

Ideal behaviour

Actuation

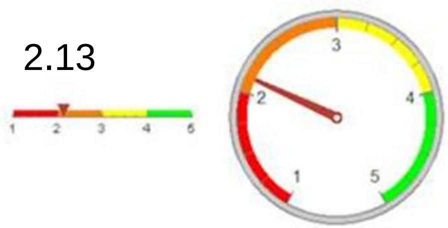
2.77



Ideal behaviour

Control

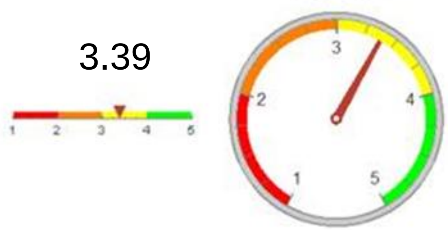
2.13



Poor safety margins

Surveillance

3.39

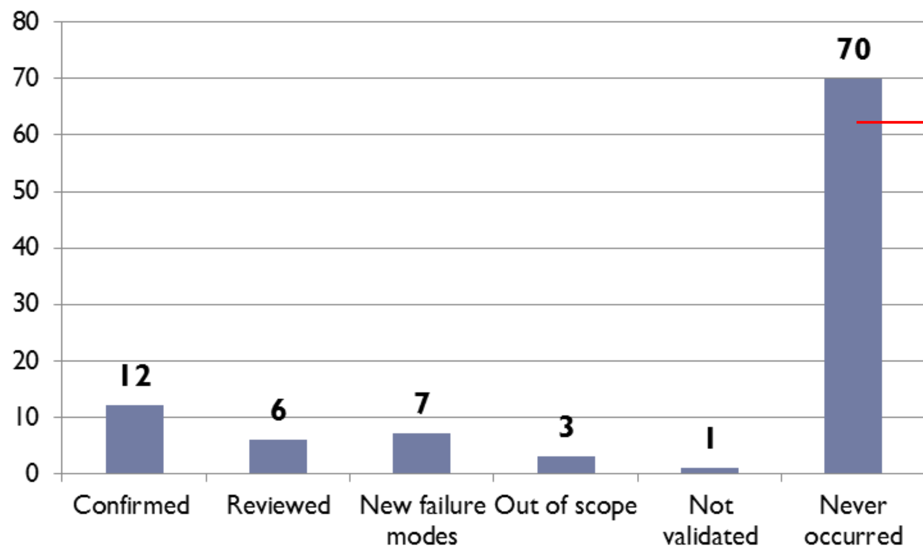


Over-protected at detriment of availability

Spare – various statistics

Failure modes

- 2518 LBDS components exposed to failures during 2010-2012 resulted in **90 failure events**, distributed in **29 different failure modes**…
- …but almost 70 failure modes never occurred

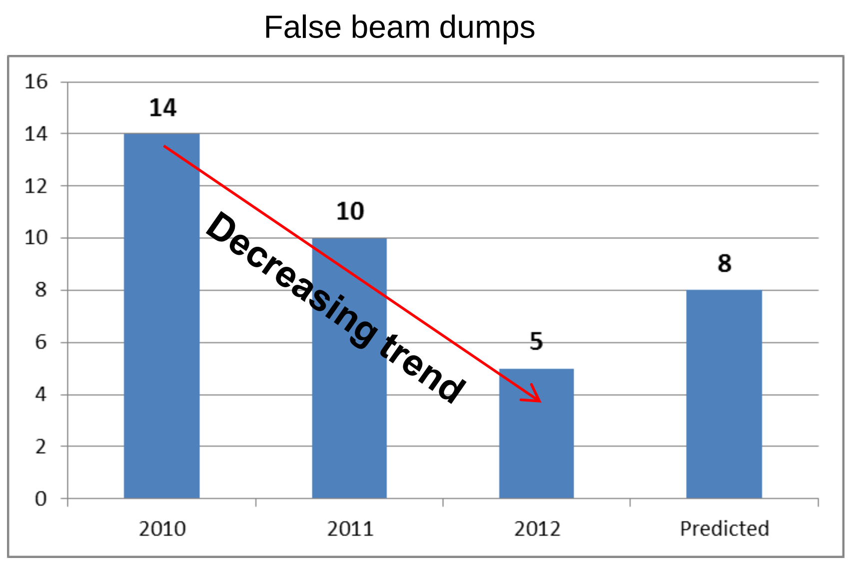


Hypothesis test always true with the exception of the PTM power supply that was expected to fail

The most conservative TTF was taken

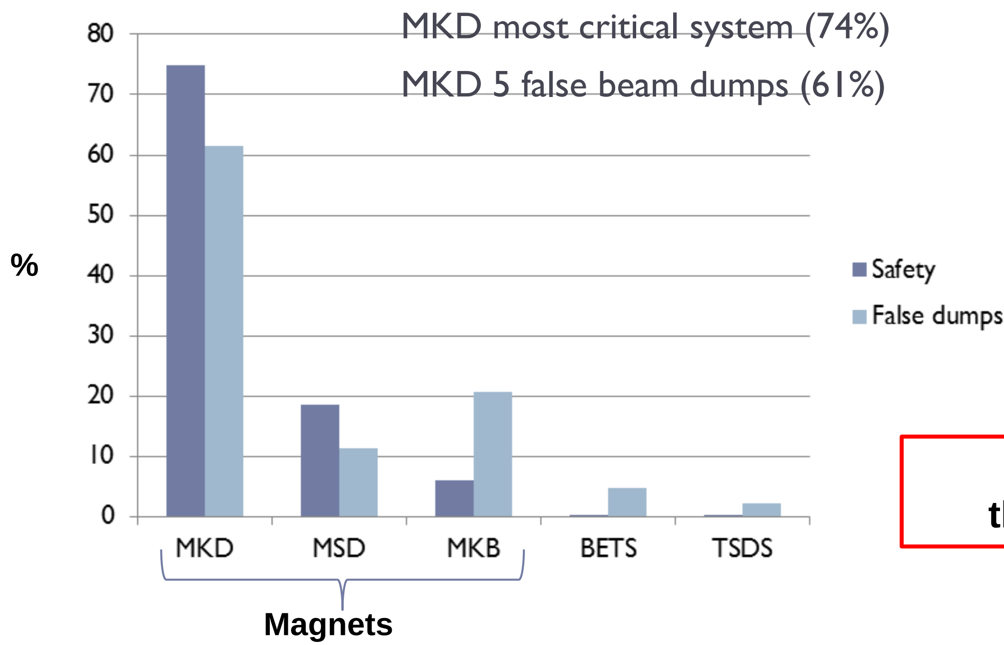
Actual availability

- Assumptions
  - Only LBDS false beam dumps in the phases injection and stable beam are considered
  - No repetition of the same internal dump request, i.e. occurrence of the same event (e.g. inaccurate diagnostics) after a short interval => 5 false dumps not considered.
- Results
  - The LBDS counted **29 false beam dumps**, against the 24 (on average) foreseen.
  - Actuation (15) then surveillance (12) and control (2)



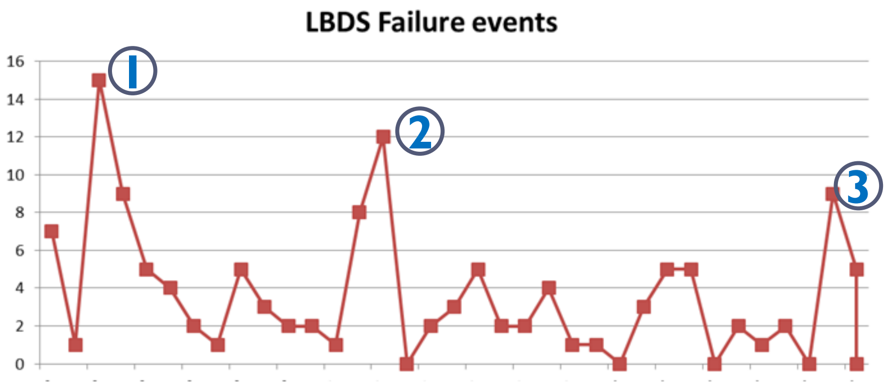
LBDS System analysis 2003-2006 (2)

- The probability of being not able to dump the beam on demand is estimated to be1.8E-07 per year of operation = largely **SIL4**
- The generated number of false beam dumps was **8** +/- 2



Predictions from theoretical models!

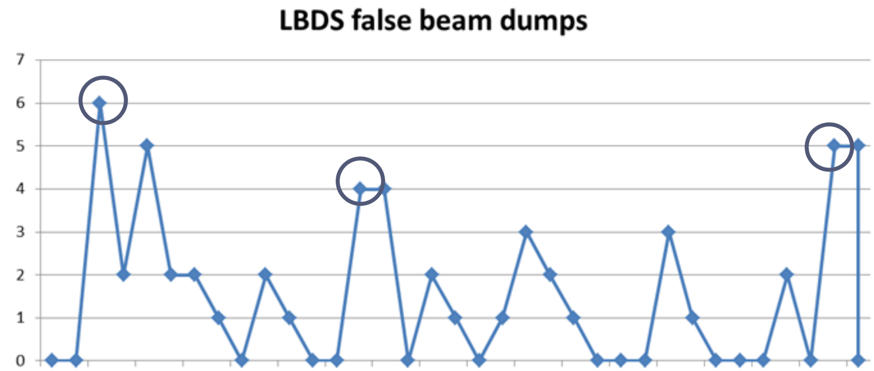
Raw data by time series 2010-2012
Put together 8, 9 and 10



Jan 2010 Dec 2012

Anomalies
1 Vacuum and BEM Anybus®
2 Vacuum and diagnostics
3 SCSS Asibus®

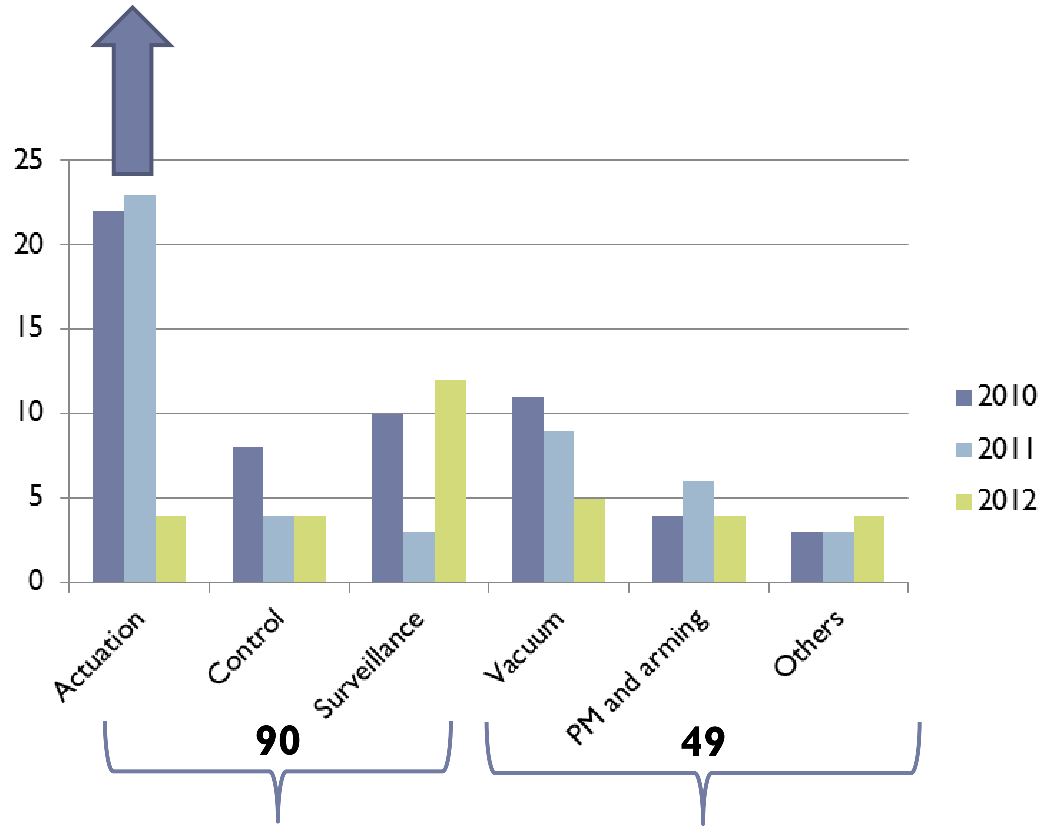
Statistics per month



Jan 2010 Dec 2012

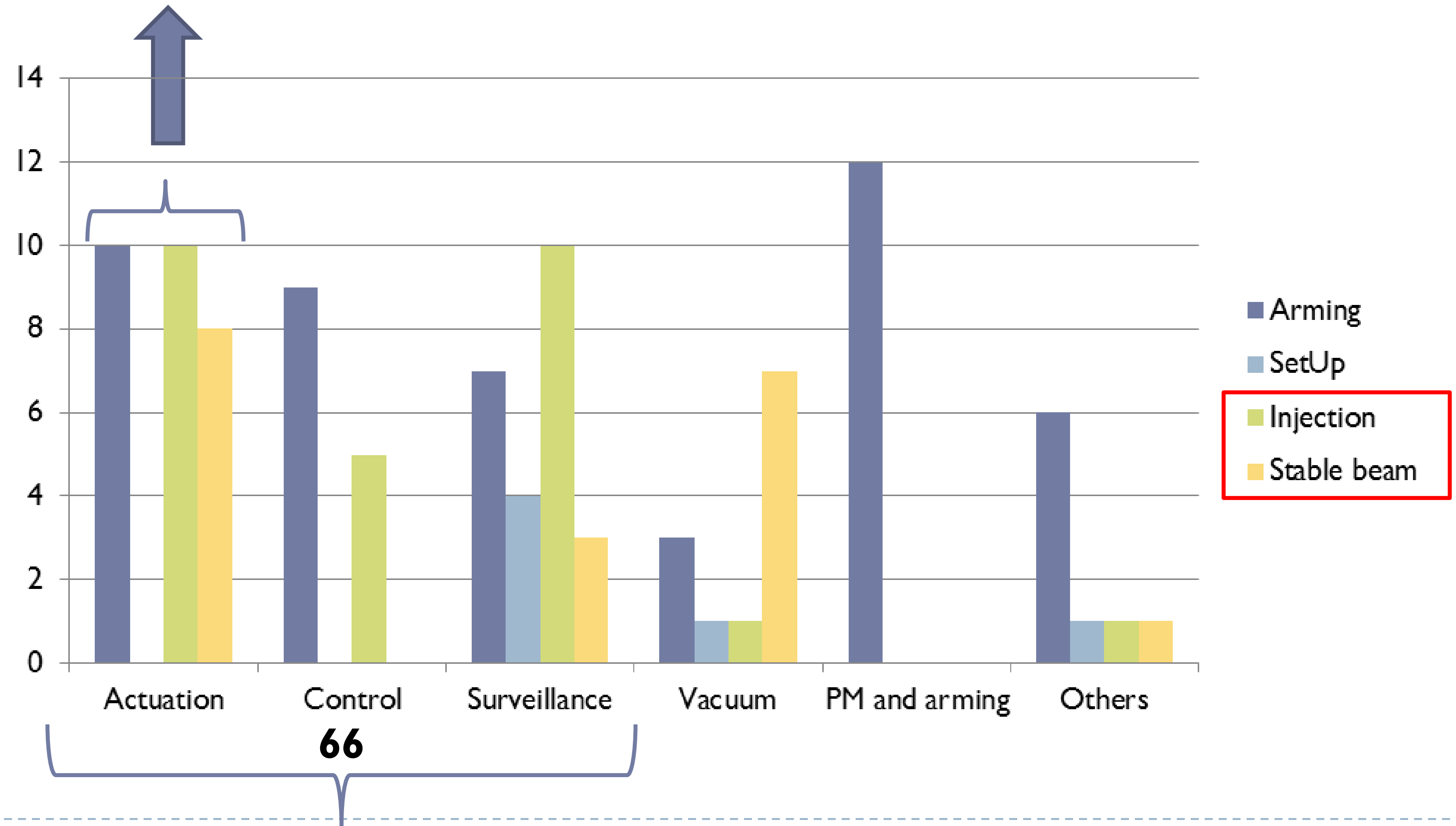
Failure distribution vs. functions

- 139 failure events recorded of which 90 in the LBDS
  - Actuation (MKD, MKB) is the largest contributor (60%)



LBDS false dumps vs. machine phase

- A total of 97 events during 2010-2012 triggered a false dump (with or without the beam) of which 66 from the LBDS, i.e. 73% of the total
  - The most important contributor is the actuation (MKD, MKB)

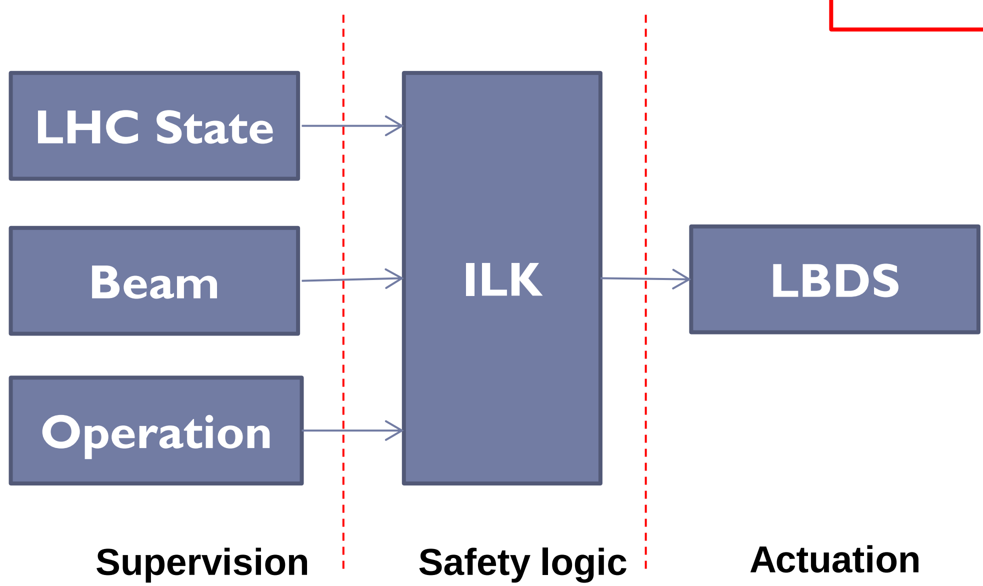


Spare - MPS

Machine Protection and LBDS

- The **LHC machine protection system** MPS allows operation with the beams only if the LHC is cleared from faults/errors, and it supervises its functioning in order to prevent that a failure may develop into a critical accident.

Is it reliable, safe?



Machine Protection System 2003-2006

- The **reliability sub-working group** of the machine protection system working group was charged to perform the analysis of safety and availability of the most critical systems of the MPS
- The scope
  - All active devices, supervision and interlocking elements including the Beam Loss Monitors, Quench Protection System, Beam Interlocking Systems, Power Interlock System, LBDS.

Reliability w.g. 2006

System	Unsafety/year	False dumps/year	
		Average	Std. dev.
LBDS	$2.4 \times 10^{-7} \times 2 = 4.8 \times 10^{-7}$	$4 \times 2 = 8.0$	2.0
BIC	1.4×10^{-8}	0.5	0.5
BLM	1.44×10^{-3}(BLM1) / 0.06×10^{-3}(BLM2)	17.0	4.0
PIC	0.5×10^{-3}	1.5	1.2
QPS	0.4×10^{-3}	15.8	3.9
MPS	2.3×10^{-4}	41.0	6.0

B. Todd, MP Workshop Annecy 2013

Most results confirmed, with a few exceptions

	2010	2011	2012	Totals
Qualifying Fills [#]	355	503	585	1443
MPS Equipment Failure [#]	43 [12.7%]	71 [14.1%]	82 [14.0%]	196 [13.6%]
Quench Protection	24	48	56	128
Beam Loss Monitors	4	4	18	26
Beam Dumping System	9	11	4	24
Software Interlock System	4	2	4	10
Powering Interlocks	-	5	-	5
Beam Interlock System	2	1	-	3