BIS Availability during Run 1 and Run 2

15-11-2018

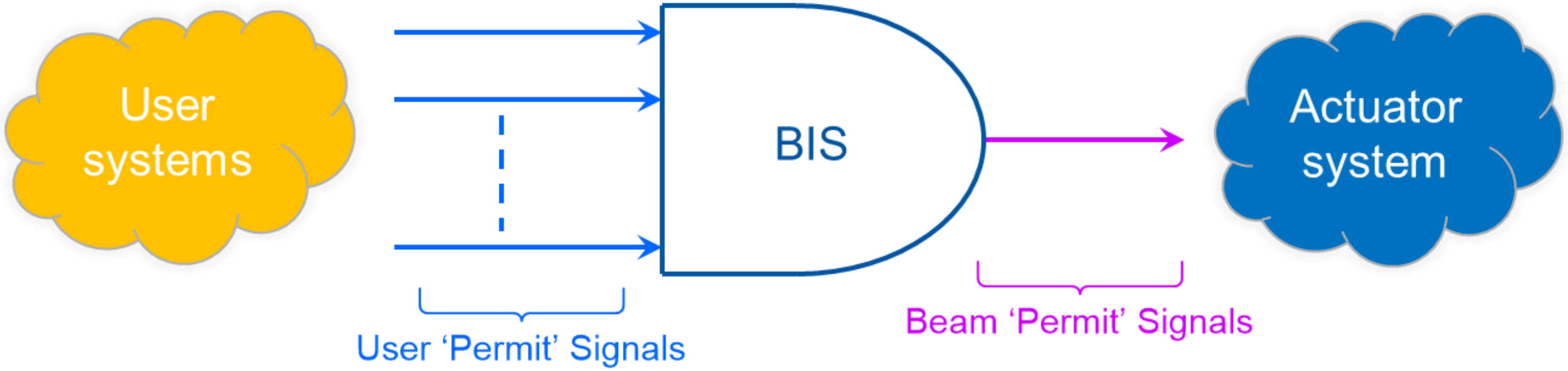
A. Apollonio (TE-MPE-PE)

Thanks to: Ivan, Raffaello, Christophe, Jan

https://indico.cern.ch/event/751827/

BIS in a Nutshell

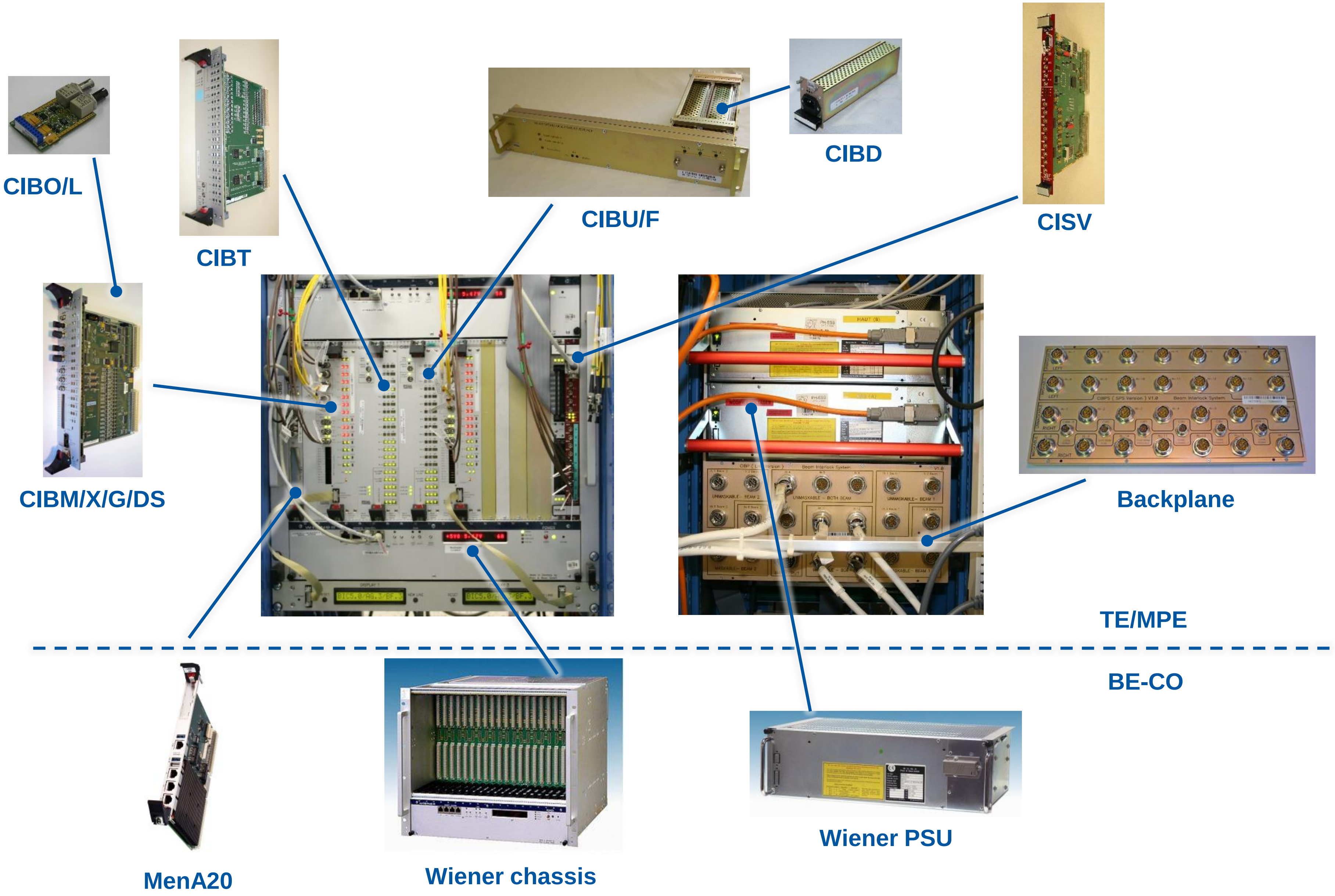
- Design to **protect** high energy accelerators
- High speed and **highly dependable**
- Deployed in LHC, SPS, SPS TLs, LINAC4 and PSB EXT
- Different topologies: **Ring** (e.g LHC, SPS) and **Tree** (e.g. SPS-EXT, LHC-INJ)



User Systems connected to the BIS

Linac4:	~95
PSB Ejection:	~14
SPS:	~50
SPS Extraction:	~100
LHC Injection:	~40
LHC:	~150

BIS Sub-Systems



CIBO/L

CIBT

CIBU/F

CIBD

CISV

CIBM/X/G/DS

Backplane

TE/MPE

BE-CO

MenA20

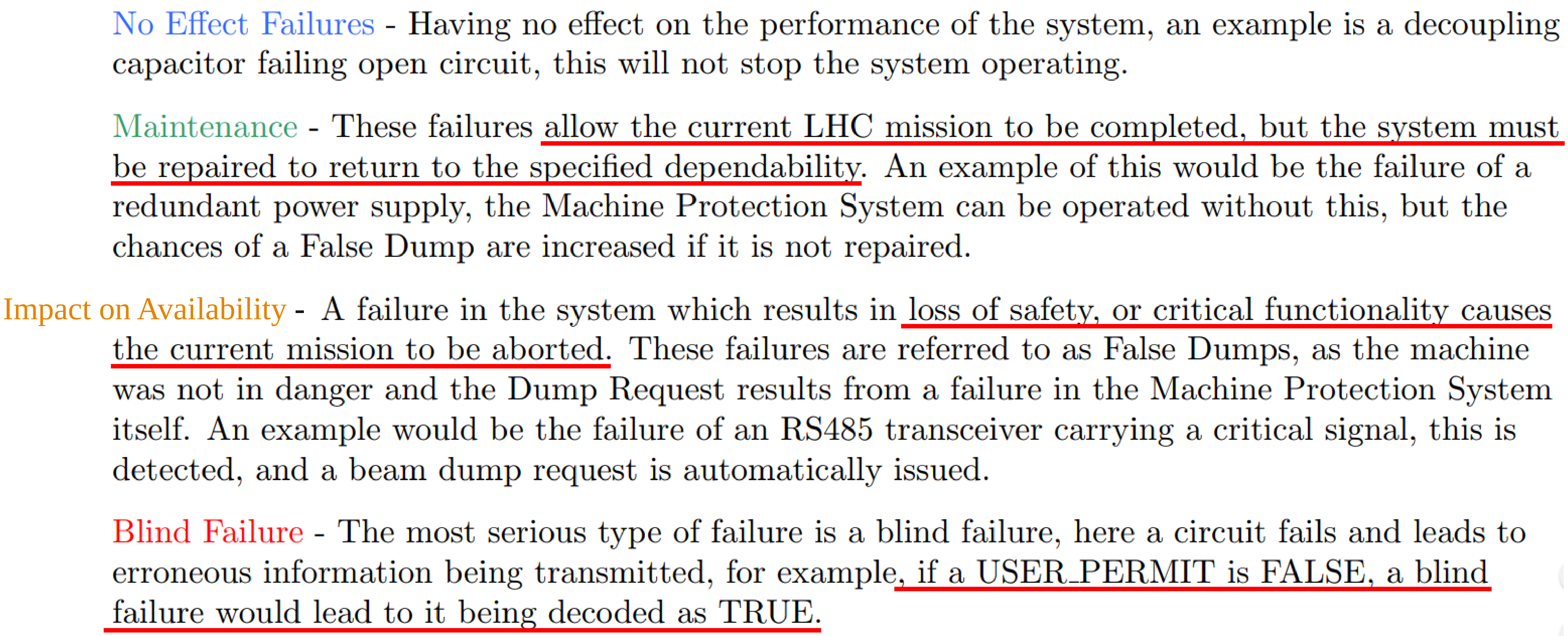
Wiener chassis

Wiener PSU

Fault Classification

Reference, thesis B. Todd: http://cds.cern.ch/record/1019495/files/thesis-2007-019.pdf

Classification:



No Effect Failures - Having no effect on the performance of the system, an example is a decoupling capacitor failing open circuit, this will not stop the system operating.

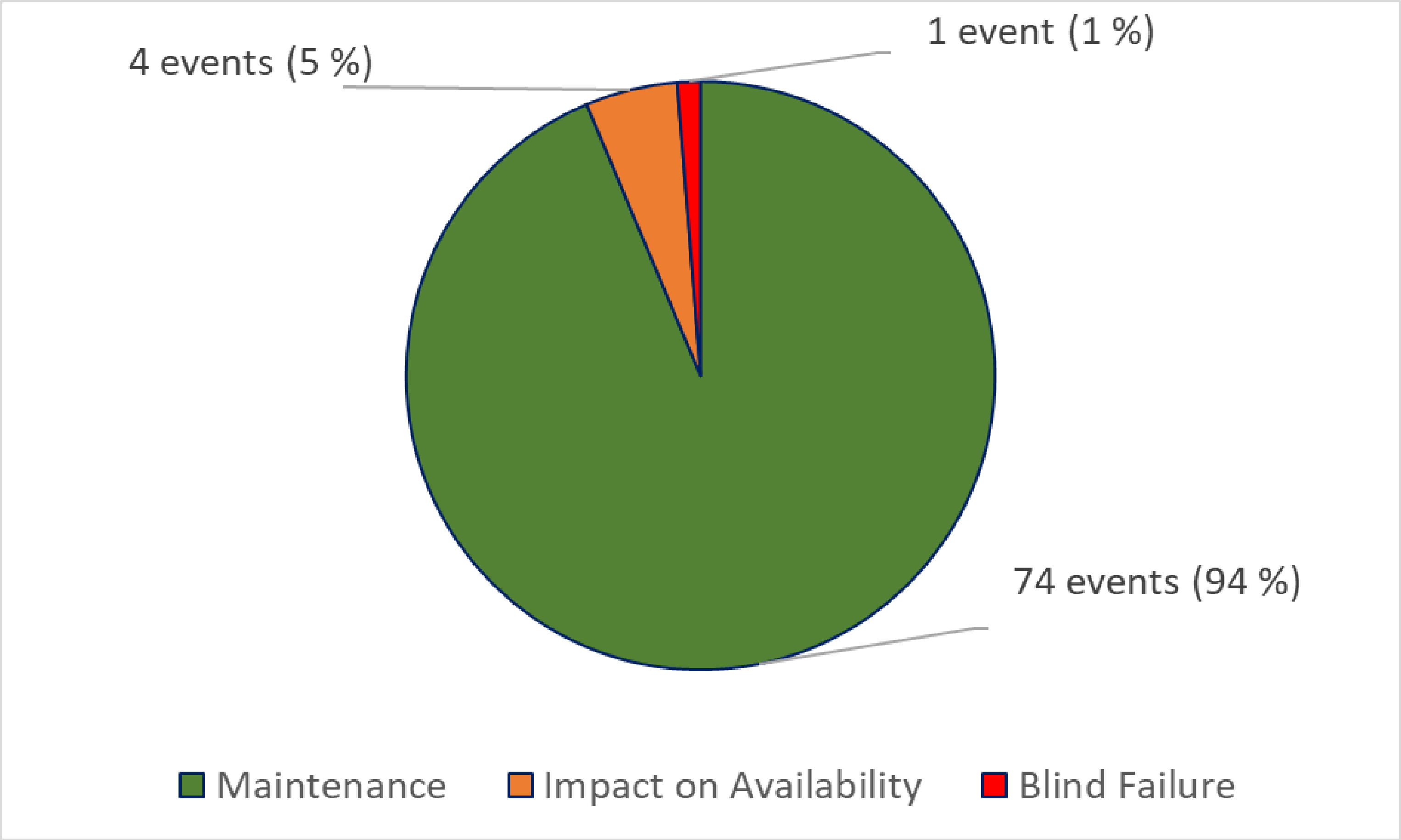
Maintenance - These failures allow the current LHC mission to be completed, but the system must be repaired to return to the specified dependability. An example of this would be the failure of a redundant power supply, the Machine Protection System can be operated without this, but the chances of a False Dump are increased if it is not repaired.

Impact on Availability - A failure in the system which results in loss of safety, or critical functionality causes the current mission to be aborted. These failures are referred to as False Dumps, as the machine was not in danger and the Dump Request results from a failure in the Machine Protection System itself. An example would be the failure of an RS485 transceiver carrying a critical signal, this is detected, and a beam dump request is automatically issued.

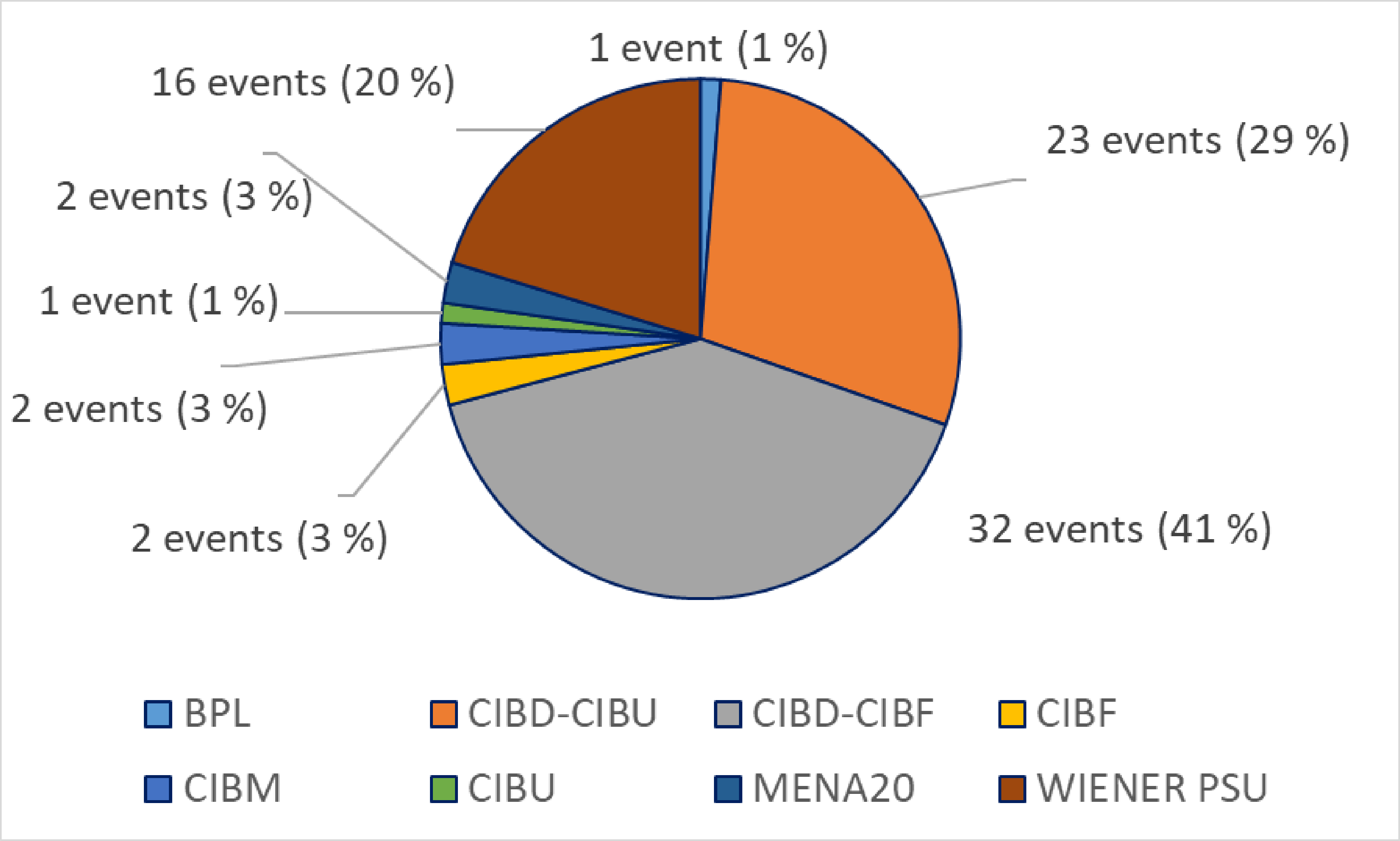
Blind Failure - The most serious type of failure is a blind failure, here a circuit fails and leads to erroneous information being transmitted, for example, if a USER_PERMIT is FALSE, a blind failure would lead to it being decoded as TRUE.

Faults by Consequence

Total: 79 events registered in various tools (AFT, Jira, BIS Database, Logbook)
No tracking of “no fault”
List might not be 100 % complete, but should well approximate reality



Faults by Sub-System



Most faults related to powering units (CIBD, Wiener PSU)

Main Failure Modes

Design/component-related

- CIBD no power: Exchange fuse T400mA/250V, effect: *maintenance*

Radiation-Induced (both in UJ56 in 2012 → relocation during LS1**)**

- Communication Lost, effect: *maintenance*
- Inconsistent monitoring signals, effect: *maintenance*

Random (?)

- BIS CPU (RIO3 before LS1, MENA20 after LS1) crash, effect: *impact on availability*

Ageing-related

- CIBD: exchange TRACO PSU (erratic), effect: *maintenance*
- Optical fibre attenuation (R2E or manipulation), effect: *impact on availability*
- No power: Exchange Wiener PSU, effect: *maintenance*

Maintenance-related

- No power: 3 Connection of 230V socket missing following EYETS, effect: *impact on availability*

User-related

- Missed beam dump: 1 event during commissioning (see slide 13 and reference), effect: *blind failure*

Availability Matrix

Machine Downtime [h]

Frequency

	Transparent	< 1h	1-4	4-8	8-12	> 12
1/week						
1/month	**CIBD: Fuse Exchange** 🔴	**Wiener PSU** 🔴				
1/year	🔴 **CIBD: TRACO PSU**		⚪ **BIS CPU crash**			
< 1/year			**Missing CIBD power supply (socket)** 🔴 🟢 **R2E**	⚪ **Fibre attenuation**		

Mitigated/not expected to re-appear

Not yet mitigated/mitigation not justified

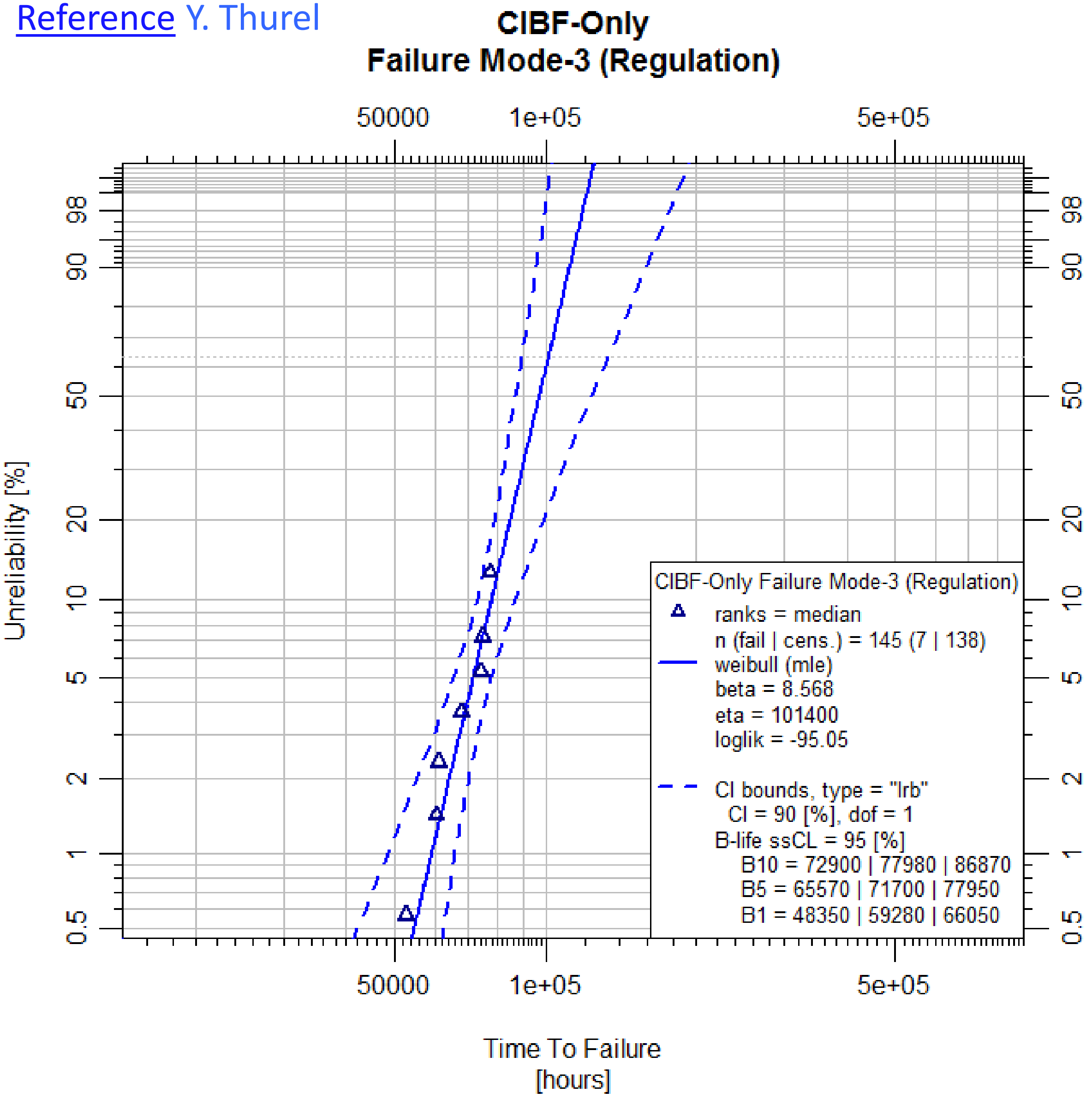
Partially mitigated

Most failures have a negligible impact on availability: considerations in this respect might be more on a strategic level (when is the ideal time to intervene, how to optimize manpower and spare parts)

Non-transparent failures mostly related to provided infrastructure

Details on TRACO Power Converter Failures - Erratic

Reference Y. Thurel



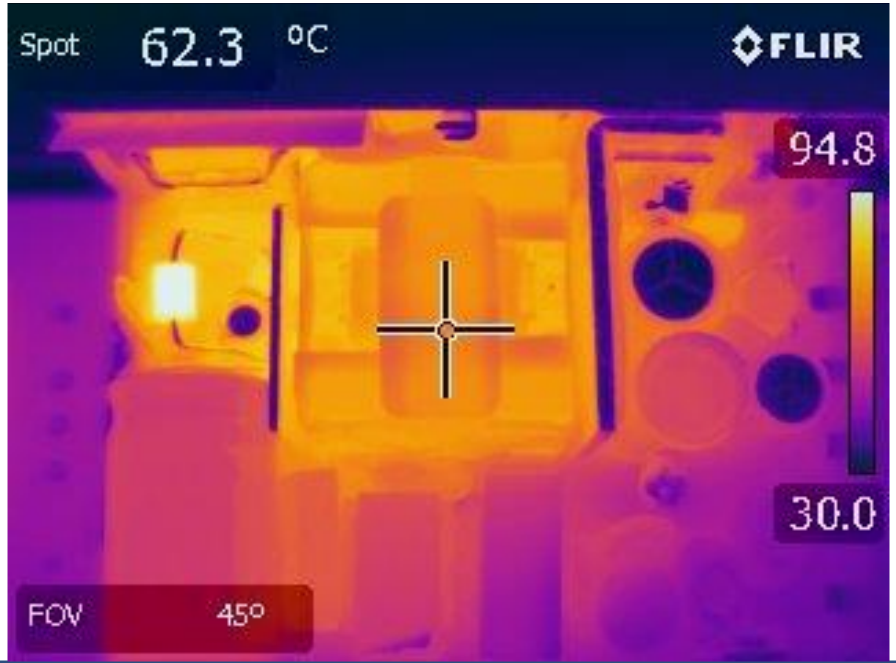
β=8.6 very high, moderated by a high η value.

Based on the projection

- 90% units would have been failed before 120 000 hours, which is around Mid-2023, for many of the considered units.

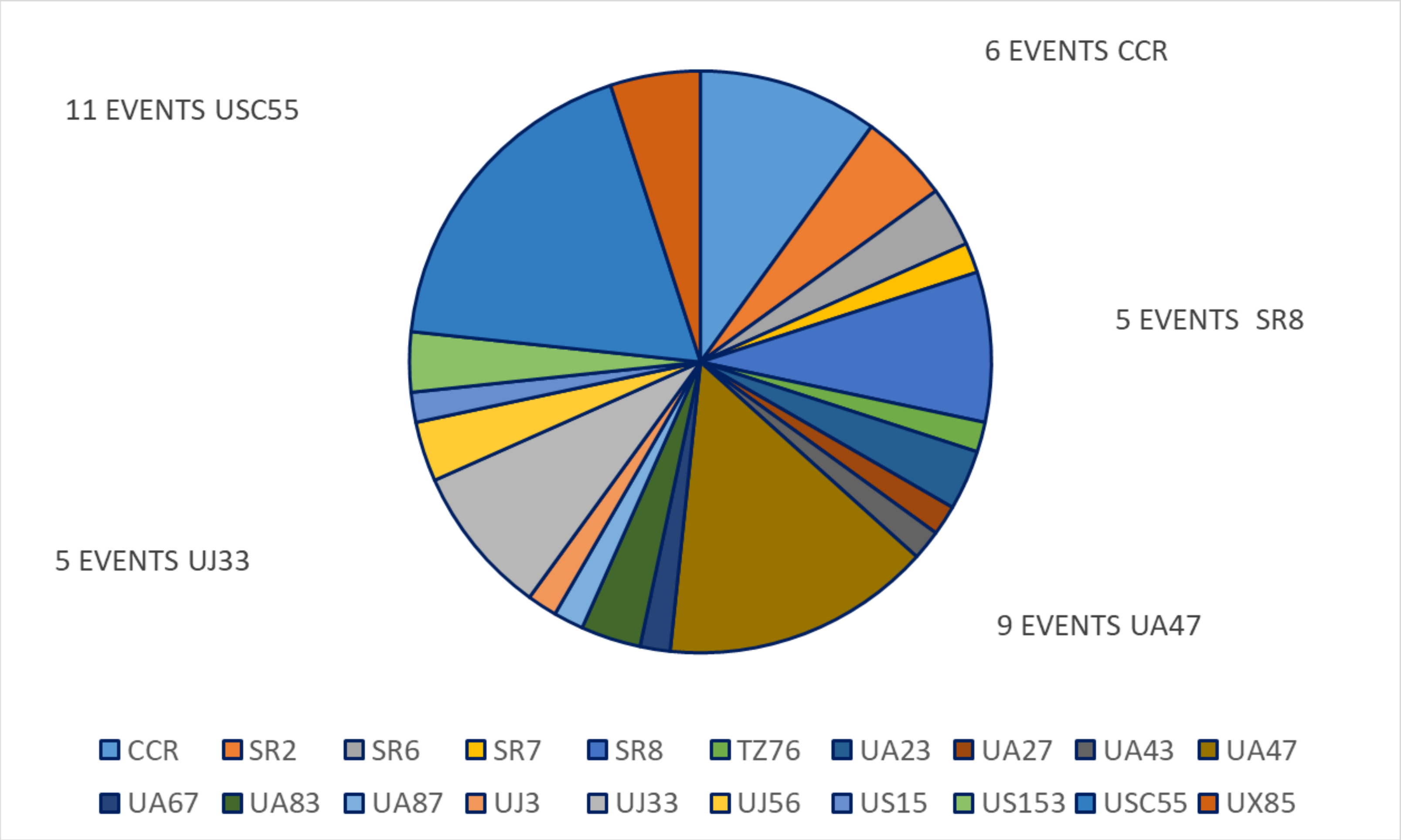
Root cause: degradation of electrolytic capacitor due to increasing ESR

- Temperature of capacitor affected by close-by TVS, correlation?



Faults by Location

60 faults for LHC + LHC INJ



No evident correlation of fault occurrence with location

2005 Predictions…vs Reality

2005 – Reliability Sub-Working Group
Predicted false dumps and safety of Machine Protection System, reference R. Filippini

safety: no events
false dumps: used to determine whether predictions were accurate

System	Predicted 2005	Observed 2010	Observed 2011	Observed 2012	Observed 2015	Observed 2016	Observed 2017	Observed 2018
LBDS	6.8 ± 3.6							
BIS	0.5 ± 0.5	2	1	0	0	0	1	1
BLM	17.0 ± 4.0							
PIC	1.5 ± 1.2							
QPS	15.8 ± 3.9							

false dumps – in line with expectations…
safety –therefore in line with expectations… if ratio false dumps to safety is ok.

Lessons Concerning Safety/Protection

Blind Failure on 7th August 2008, reference B. Todd

No Beam In the Machine
Final Commissioning Vacuum System to Beam Interlock System

1. Vacuum Valves moved IN around IR3
2. Vacuum UJ33 USER_PERMIT_A stayed TRUE
3. Vacuum UJ33 USER_PERMIT_B stayed TRUE
4. BIC Test Mode showed ALL OK

Commissioning Fail

Between July and August
EIS (Elément Important de Sécurité)

1. Added to Interlock Logic
2. EIS controlled by Access System (Personnel Protection Device)
3. Access System connected to BIS via Vacuum System

MI were not aware of this cabling change

Several events = complete Blind Failure

1. Two Equipment systems sharing the same channel
2. PLC Voltage against rules
3. TVS Blocked Short-Circuit
4. Inputs were not redundant
5. Not re-commissioned by MI after a significant change

In addition…

a) Cable length against rules
b) EMC would have been a show-stopper anyway!

Shows weaknesses in the interconnection conception:

1. No redundancy = No SIL
2. Can a GND short be mitigated?
3. Human Error can never be 100% eradicated – Testing before each fill should be possible if in doubt!

For each User System

1. Change to use full redundancy
2. Change so a GND fault doesn't fail blind
3. Automated Test from User Side A /= B

Conclusions

- BIS has been one of the most dependable systems during the first 2 LHC Runs

- Most failures were completely transparent for accelerator operation

- Some known – minor - problems:
  - TRACO power supplies ageing
  - Optical fibres
  - Wiener power supplies
  - BIS CPU

- No obvious reason for major changes (architecture, protection strategy)

- However, possibly review general strategy concerning user inputs and critical interfaces – ensure that the protection integrity level is preserved through the chain:

  detection → user electronics → **user interface → interlock system** → actuator
- Today many users are non-conform to specifications (in all machines)

- Improvements for BIS fault tracking could be considered (e.g. AFT + INFOR EAM)