CERN,

Chamonix

26th January 2016

BEAM INSTRUMENTATION GROUP DEPENDABILITY APPROACH

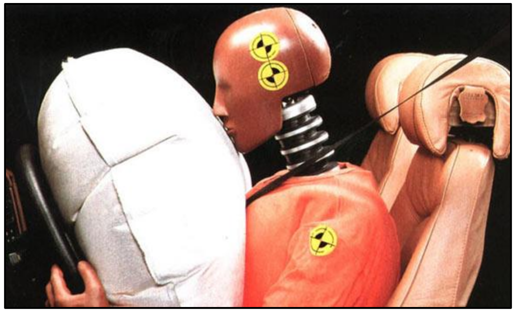
William Viganò (william.vigano@cern.ch)

Beam Instrumentation equipment

- The Beam Instrumentation Group is in charge of equipment installed in all CERN accelerators, some are solely for observation but others function as protection system.

- There is a huge difference between a Safety Critical System and an "Observation System",
  - The difference starts with the architectural design, followed by an entirely different implementation procedure.

Safety Critical System



Observation System

Critical systems involved in Dependability

- Dependability
  - Measure of a system's availability, reliability & maintainability

- The criteria used in this presentation for selecting beam instrumentation considered “critical” are LHC systems that:
  - Generate interventions or preventive maintenance that reduce beam availability.

  - Generate false dumps.
  - Can be responsible for blind failures.
    - ❖ Where the machine should be protected but the system is not operational and / or not monitored).

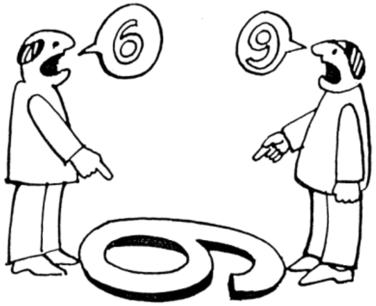
William Viganò (william.vigano@cern.ch)

List of BI Critical systems

- Beam Loss Monitor System [BLM]
- SW Interlocked Beam Positioning Monitors for orbit observation [Standard BPM]
- HW Interlocked Beam Positioning Monitors for the dump line in LSS6 [Interlocked BPM]
- Synchrotron Light Abort Gap Monitor [BSRA]
- DC Beam Current Transformer [BCTDC]
- Fast Beam Current Change monitor linked to the Fast Beam Current Transformer [BCTF]
- Tune measurement system [BBQ]
- Orbit and Tune feedback system [OFC/OFSU]

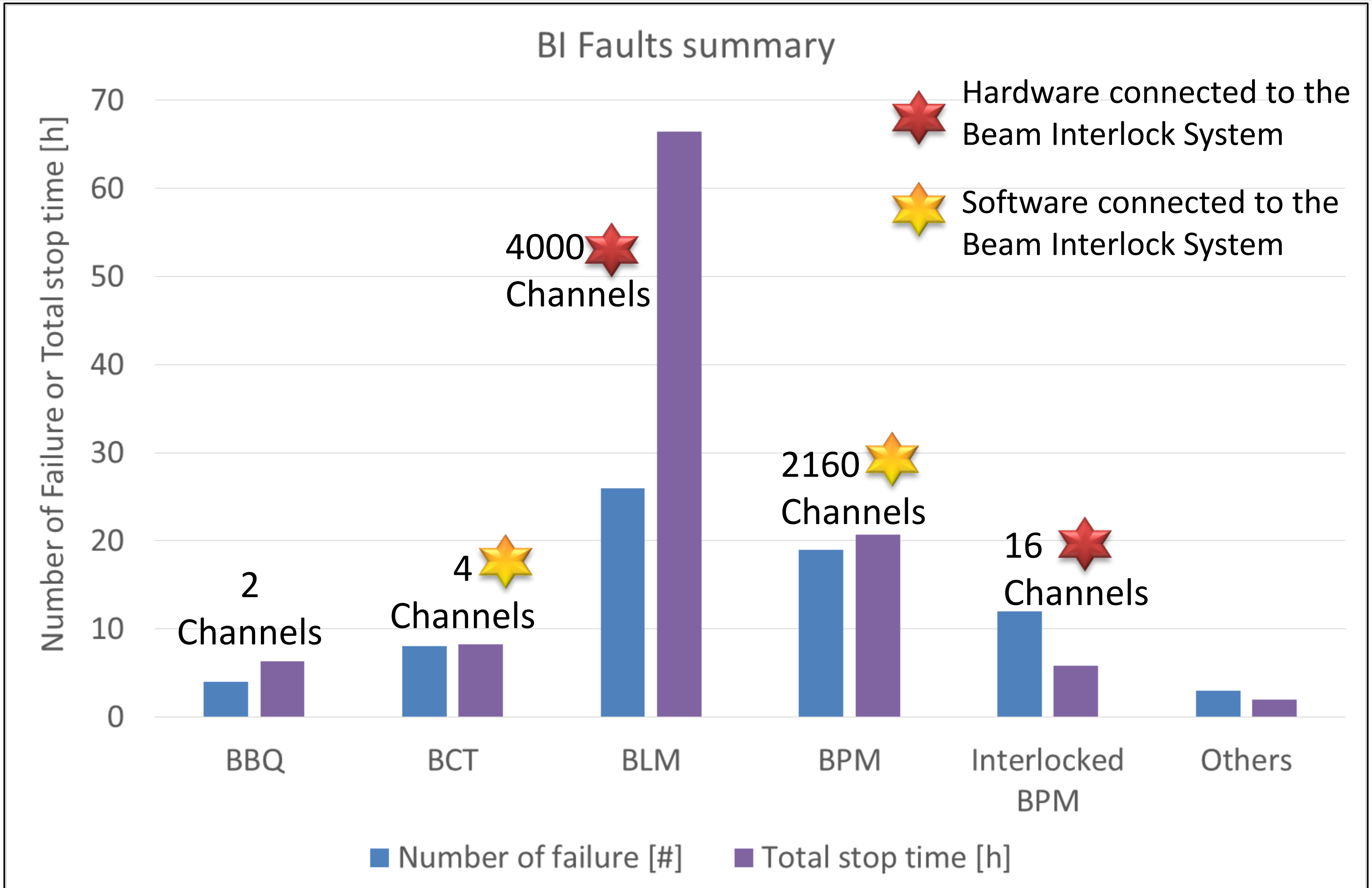
Failures in 2015

- The failure analysis presented on the next few slides is based on data from the Accelerator Fault Tracking [AFT] Tool which gives the overview from the Operation point of view.



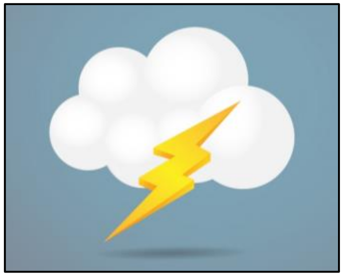
- More than 70 faults of Beam Instrumentation have been analyzed.
- From the Expert point of view, the number of faults is larger than the AFT result, but invisible to Operations due to factors such as: redundancy, recovery strategies, etc…
  - These are difficult to analyse as they are catalogued by each system using their preferred fault tracking method.

Failures - 2015 Summary



Fault categorization

Faults have been categorized into 4 sub-categories:



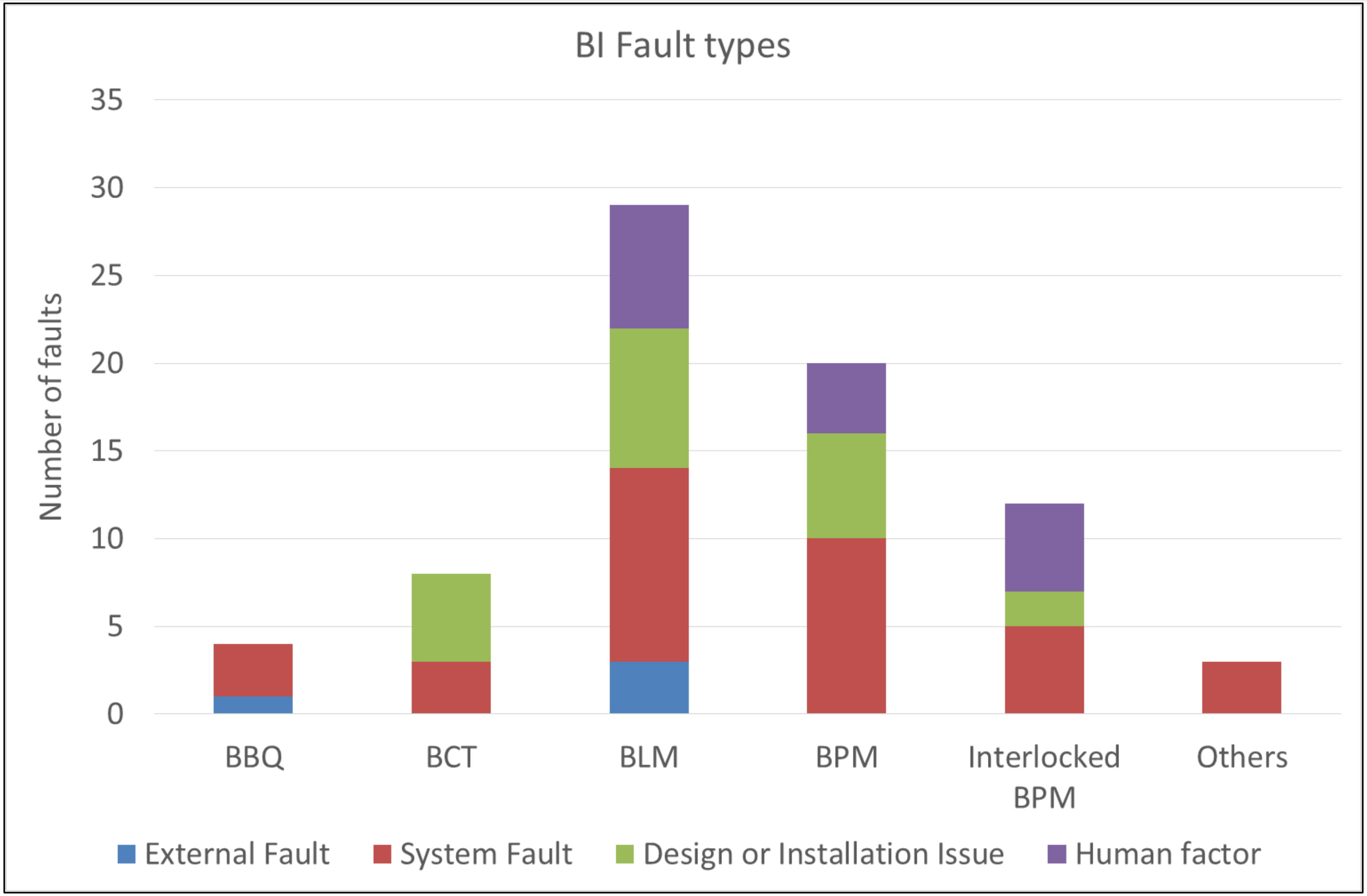
- "External fault": represents external interference leading to a failure, such as the surge current discharge that damaged the BLM system.

- "System Fault": Fault of a Hardware/Software nature.

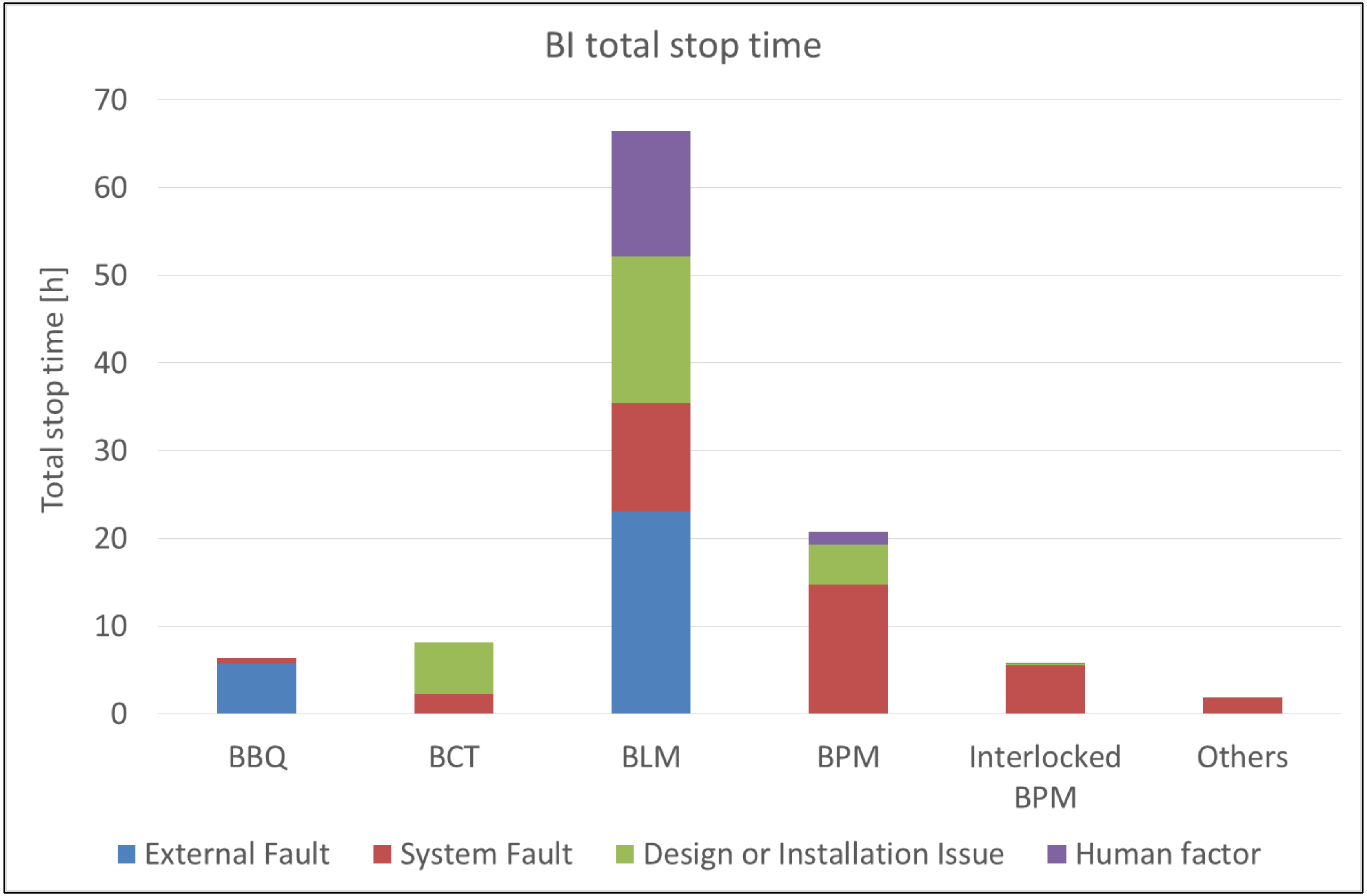
- "Design and installation issues": mainly due to missing test-benches or additional functionality added to systems after design completion.

- "Human factor": due to wrong operation, lack of communication / understanding of the issue or modifications by untrained people.

BI Fault types - 2015 Summary

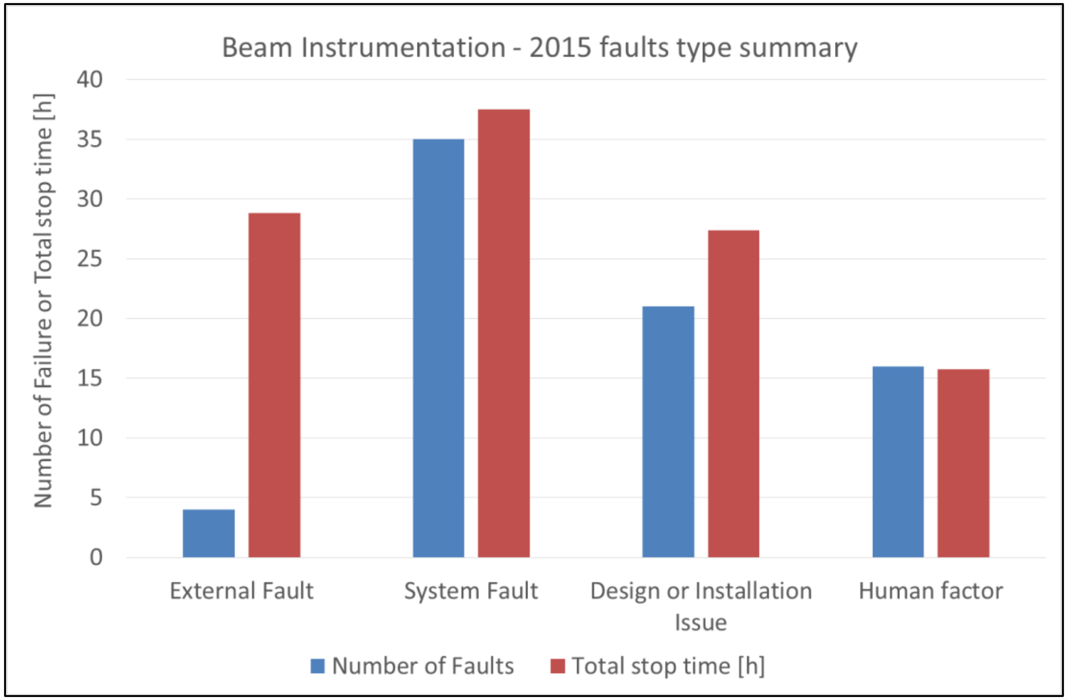


BI Intervention time - 2015 Summary



Lesson learned in 2015

Failure Type	Number of failures [#]	Total stop time [h]	Contribution Percentage
External Fault	4	28.8	26%
System Fault	35	37.5	34%
Design Issue	21	27.4	25%
Human factor	16	15.7	14%



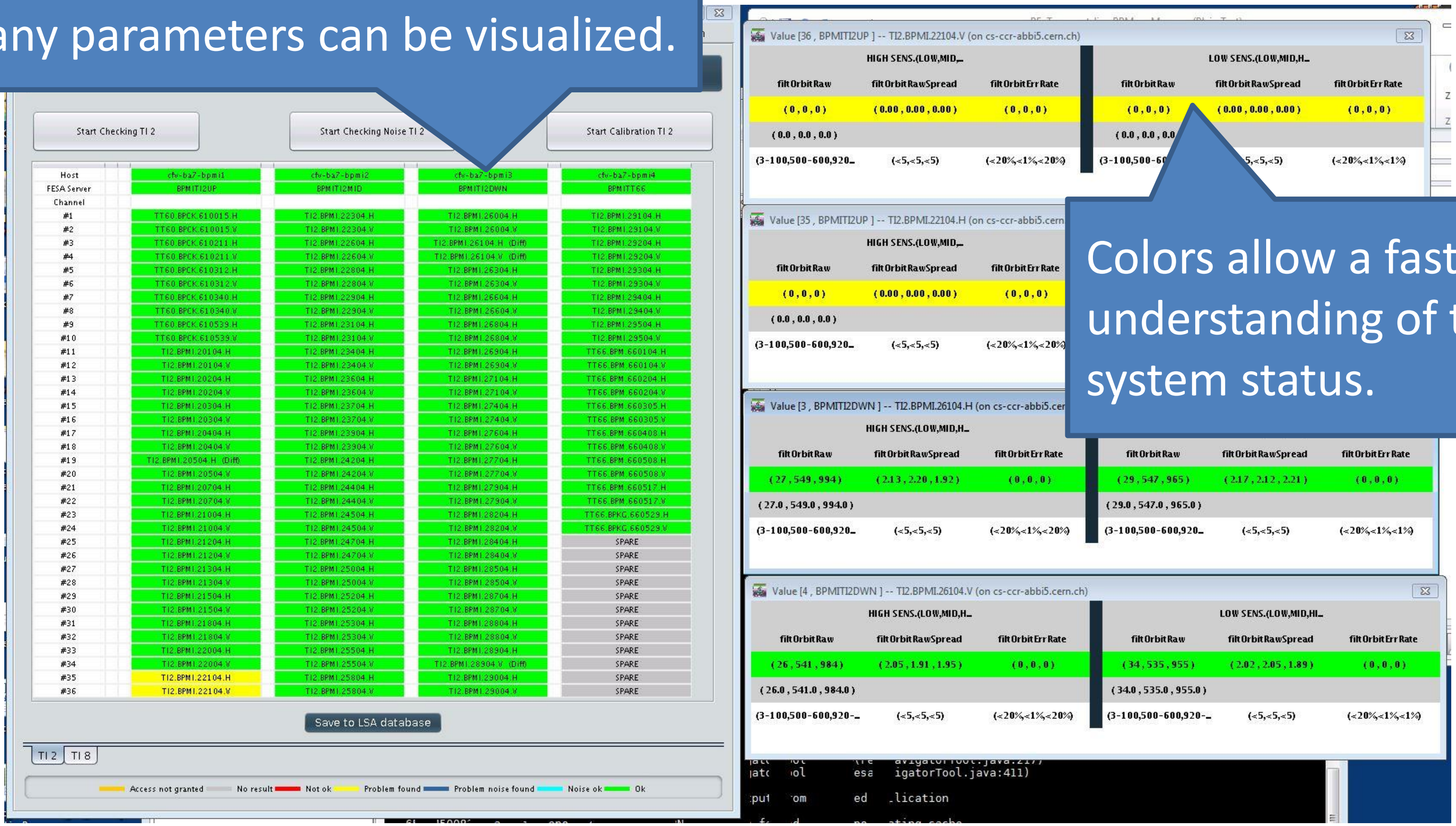
- Total stop time in 2015 => 109.4 hours (<2%)
- No R2E failures thanks to heavy testing of BLM & BPM systems at design stage.
- We need to better understand the nature of the faults for optimizing their mitigation.
- Improving the beam availability means for BI working on several aspects.

WHAT HAS BEEN DONE TO FORESEE AND REDUCE FAILURES

Diagnostics: Online monitoring

- BPM calibration screenshot for the SPS-LHC transfer lines.

Many parameters can be visualized.



Colors allow a fast understanding of the system status.

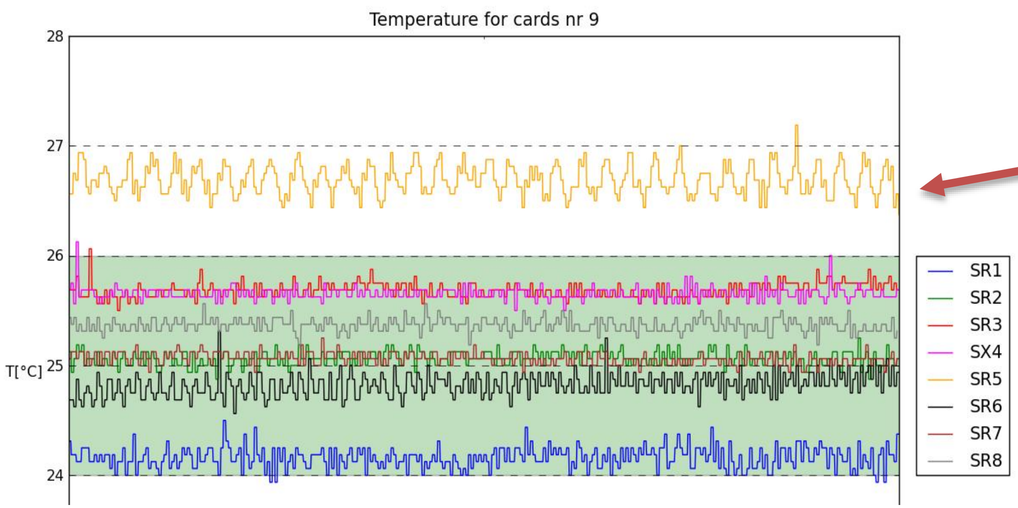
- <u>These tools do not prevent faults but they help save time understanding issues.</u>

Diagnostics: Offline monitoring

- Several offline monitoring functions added during 2015.
- Daily checks introduced with the aim of detecting parameter degradation.

Daily report on number of errors per Optical link

Card	BLECF Serial	BLETC Serial	BLECS Serial	CRC COMP		LK1 ERRORS		LK2 ERRORS		LK1 LOST		LK2 LOST		FID COMP	
				A	B	A	B	A	B	A	B	A	B	A	B
SR5-L 8	0473 0546	144115249047404545	3026419007996394497	0	0	0	0	0	0	0	3	0	0	0	0
SR7-L 10	0047 0017	16140901125476397313	16429131499061498881	0	0	0	0	0	0	0	1	0	0	0	0



Daily Temperature monitoring for all crates in all Points

Diagnostics: New event warning

- BLM Threshold changes – automatic alert to experts in charge of Piquet service.

Table 1: Changes of BLM info in LSA

Expert Name	Position		Family		Dcum	
	old	new	old	new	old	new
BLMBI.11L1.B0T20_MBA-LEFL	-	-	THRI.ARDS_MBMB	THRI.ARDS_MBMB_IQT15	-	-
BLMBI.11L5.B0T20_MBA-LEFL	-	-	THRI.ARDS_MBMB	THRI.ARDS_MBMB_IQT15	-	-
BLMBI.11R1.B0T20_MBB-LEHR	-	-	THRI.ARDS_MBMB	THRI.ARDS_MBMB_IQT15	-	-
BLMBI.11R5.B0T20_MBB-LEGR	-	-	THRI.ARDS_MBMB	THRI.ARDS_MBMB_IQT15	-	-

- Most of the diagnostic tools have been created or grown with the project development. Now systems are installed but many tools are needed for understanding issues.

➢ With the growing of the system complexity we need a simplification of software used for diagnostic purpose.

Test-benches

- Testing BI Software (e.g. Orbit Feedback software test-bench)

1. Prepare Software for Testing
   - Relax Constraints (RBAC etc)
   - Isolate Reliance on Other Systems

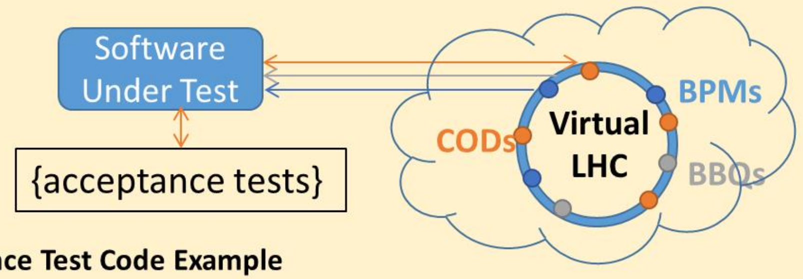
2. Plant Virtualization
   - Simulate Timing
   - Simulate Data I/O

3. Decide Test Objectives
   - FESA Mechanics (GET/SET/Subs)
   - I/O Processing
   - Control Loop Behavior

4. Assert Tests
   - Assert Pass & Failure Cases
   - Assert Boundary Cases

Plans in 2016 to Develop New Testbeds for LHC BLM &Tune Software

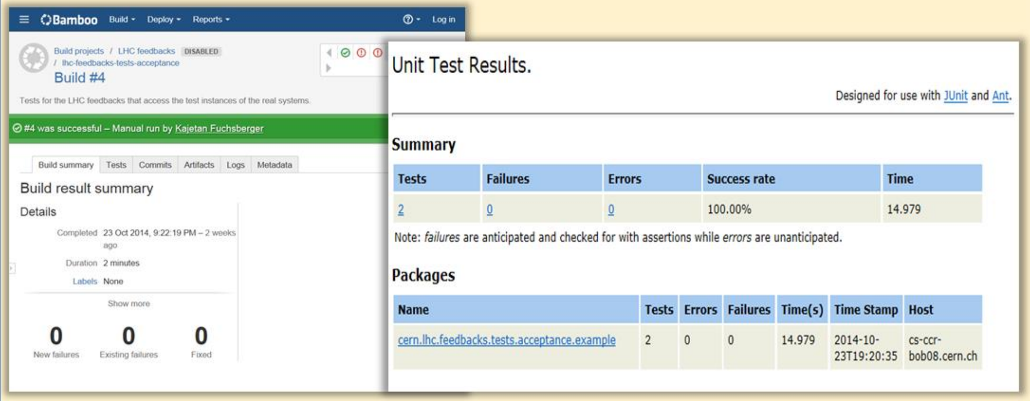
Example from Software Testbed Developed for LHC Feedbacks



Acceptance Test Code Example

```
prepareSendingOf(zeroOrbit()).andStart();
MultibeamOrbit acqOrbit = from(MultibeamOrbit.class).skip(1).and().awaitNext();
awaitLastSending();   /* assertion here */
```

Tests Run Regularly and Results Seen in Bamboo



Unit Test Results.

Designed for use with JUnit and Ant.

Summary

Tests	Failures	Errors	Success rate	Time
2	0	0	100.00%	14.979

Note: *failures* are anticipated and checked for with assertions while *errors* are unanticipated.

Packages

Name	Tests	Errors	Failures	Time(s)	Time Stamp	Host
cern.lhc.feedbacks.tests.acceptance.example	2	0	0	14.979	2014-10-23T19:20:35	cs-ccr-bob08.cern.ch

Intervention time reduction

- Creation of a Piquet service for BLM.
- Preparation of a Piquet Service Manual
  - Learning from past failures.
  - Reduction in time taken to resolve issues.

Table of Contents

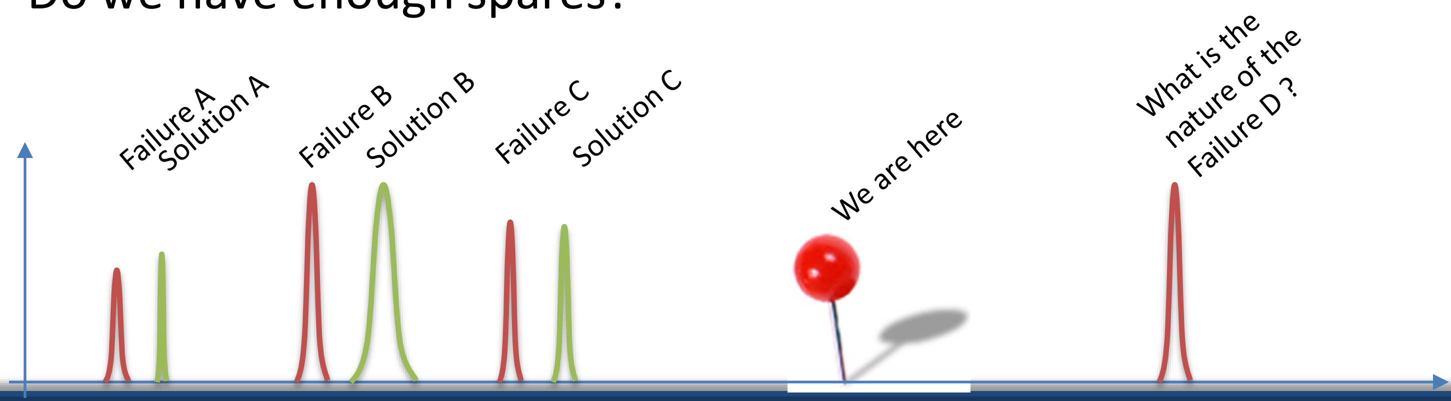
William Viganò (william.vigano@cern.ch)

WHAT BEAM INSTRUMENTATION NEEDS FOR FURTHER IMPROVING ITS DEPENDABILITY

William Viganò (william.vigano@cern.ch)

Reliability Analysis

- Apart from a few exceptions, such as the LHC and injector BLM systems, the normal way of proceeding is: “learn from the experience”.
- This approach can work in general, but means that we are often working to solve issues rather than foresee them:
  - Simple example:
    - A brushed fan has a lifetime of 7 years.
    - We have many fans installed everywhere.
    - What happens in case of multiple failures?
    - Do we have enough spares?



Common Analysis Method Required

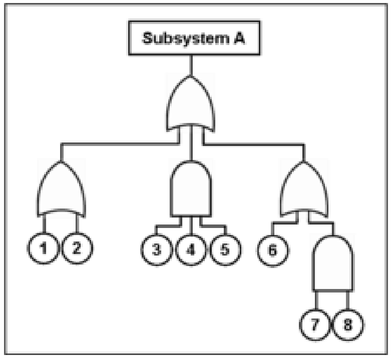
- Need a common method for running Reliability Analysis for all future critical systems (not just BE-BI?) composed of 3 main points:

  - Failure Prediction.

  - Failure mode and criticality analysis using the Risk Priority Number method.

S	x	O	x	D	= RPN
10		2		2	40
3		10		2	60
2		5		10	100

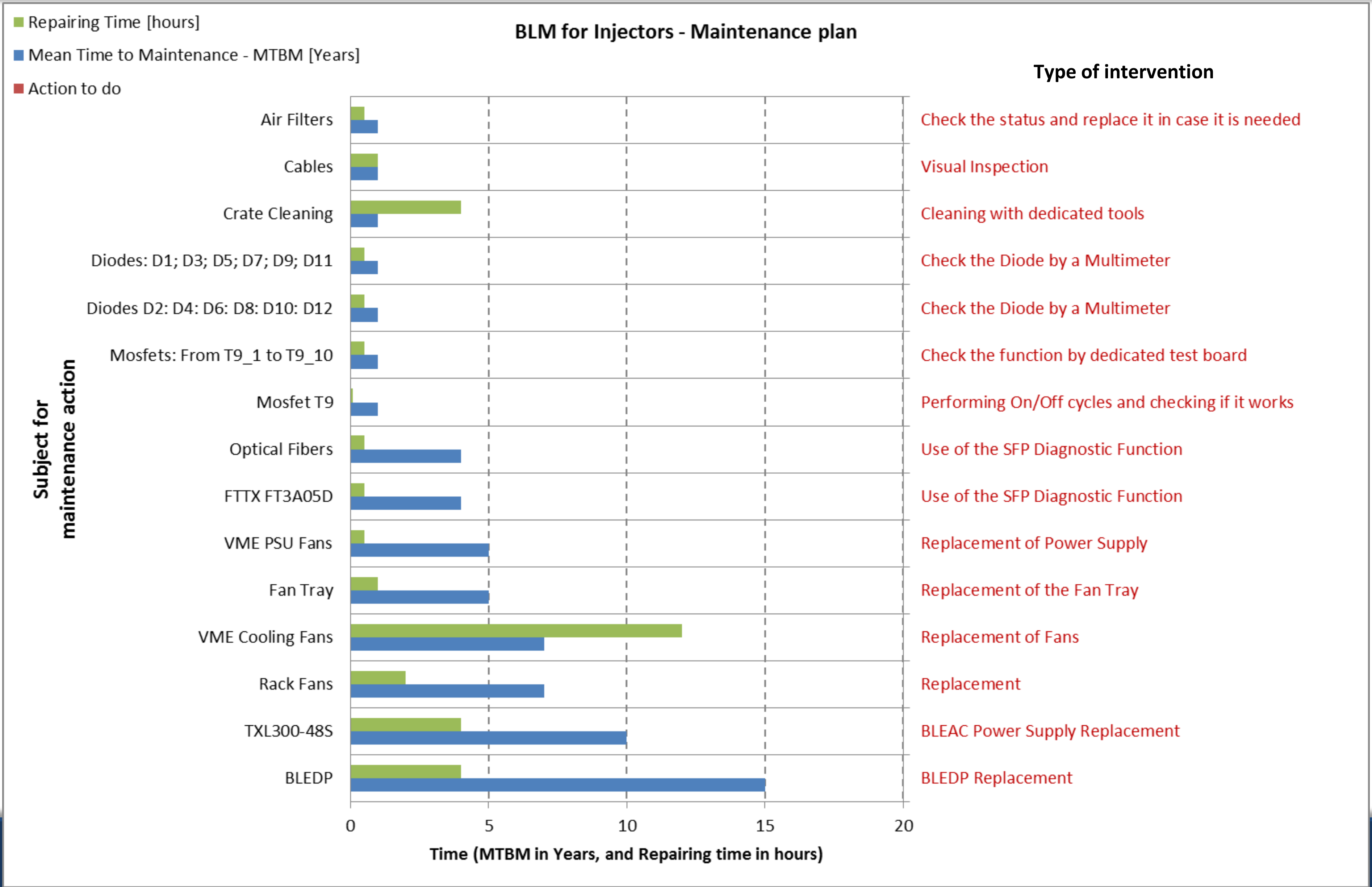
  - Fault Tree analysis.



(e.g. Using Military handbook as reference standards.)

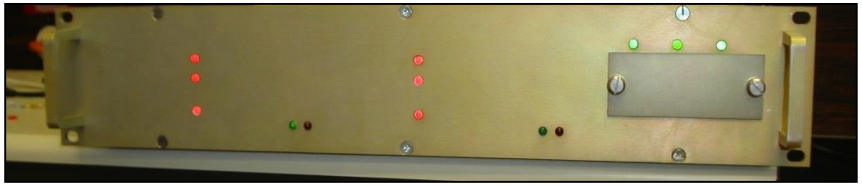
For projects with Prediction and Failure mode analysis done, a maintenance plan is automatically obtained as one of the results.

Maintenance plan



Connecting systems to the Interlock

- We have cases of equipment originally designed for observation or measurements only which are now being connected to the Beam Interlock System.

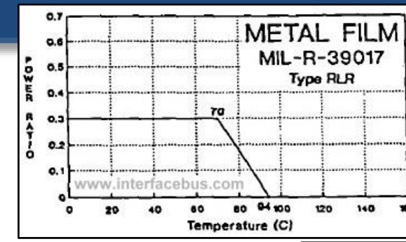


- Many systems have been designed, manufactured and installed following the measurement performance needs without performing a proper Reliability Analysis.

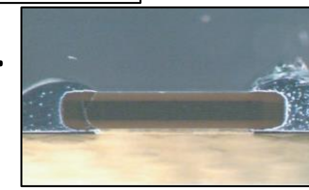
➢ BI propose that the decision to connect new systems to the Beam Interlock System should be limited to those that have undergone Reliability Analysis, and are compliant with BIS specifications.

William Viganò (william.vigano@cern.ch)

A structured approach to improve dependability



- Training of design engineers in best practice:
  - CERN guidelines for component “derating rules”?
  - What do we mean by failure modes?
  - How to guarantee high reliability manufacturing, assembling, etc.
    - ❖ How do we verify this?
  - What is the appropriate tool for fault tracking?
    - ❖ AFT, Jira, EAM, etc. ?



CERN Accelerator Fault Tracking

- Identifying critical systems early in the design phase:
  - Needs to be clearly included in specifications.
  - Systems should be audited during conception phase.

- Maintaining Reliability Analysis Expertise:
  - Often done solely by Temporary Personnel.
    - ❖ Overhead for starting each analysis.
    - ❖ Subsequent loss of knowledge when they leave.
  - **BE-BI Group would profit from a longer term (centralised?) Reliability Analysis team.**

Conclusions

- The reliability analysis of BLM system (over 4000 channels connected to BIS), has certainly contributed to its full reliability & low number of system faults. Currently addressing human factor & remaining design issues to further improve availability.

- Need to extend reliability analysis to other systems with all engineers aware of the importance of such an approach at the design stage (Consolidation & HL-LHC).

- Reliability, Availability and Maintainability (R.A.M.) analysis should be performed on all BI systems affecting availability.
  - To do this BI will need more support and would greatly profit from a dedicated team for guaranteeing the feasibility of this important and complex task.

Thanks for your attention!

And many thanks to the AFT team and BI colleagues for their contribution to this presentation!