



Beam Interlock System External Review 2009



B. Todd on behalf of TE/MPE/MI

11th November 2009

1. External Review Criteria

- Criteria
- Motivation

2. Outcomes

- Recommendations by CSL

3. Conclusions

- Summary Table
- Future Plans

1. External Review Criteria

- Criteria
- Motivation

2. Outcomes

- Recommendations by CSL

3. Conclusions

- Summary Table
- Future Plans



What is the aim of this work?



Beam Interlock System was Internally Reviewed in 2006

Very well received

1. The 2006 internal review used only accelerator professionals.
2. no means of referencing the Beam Interlock System design to other interlock systems in industry
3. VHDL (software/firmware) safety is difficult to quantify.
4. CERN has other systems which would benefit from generic review methods
5. Comparison of the system to international standards, such as DO-178B

This review is to continue and enhance that work



What is the aim of this work?

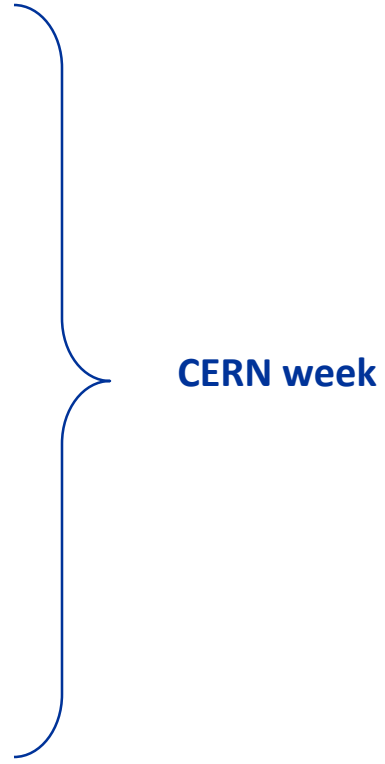


Remember the following points are the aim of this review

1. identify possible weaknesses in the mission-critical BIS before LHC reaches high intensity beam operation
2. assess the adequacy of the external and internal mitigations for critical component failure in the BIS
3. provide a general comparison of the BIS with approaches in industrial systems.
4. suggest potential improvements of the BIS
5. review and comment on the pre/during/post operational software sequences that verify the integrity of the BIS
6. provide CERN with a model for future assessments of mission-critical systems

18th August – 7th September
Study of pre-review material

- Monday 7th September**
presentations
- Tuesday 8th September**
demonstrations
- Wednesday 9th September**
open-house
- Thursday 10th September**
VHDL
- Friday 11th September**
AM: open-house
PM: outgoing remarks



11th September – 2nd October ++
Post-visit report



Canadian Firm...

Military Safety

Automotive Safety

Train Safety

Contribute to Writing Standards

Chaired the International System Safety Conference 2008

++

Very well placed to judge our work

My personal ambition

certification for our systems

These are the **certification experts = push us the right way**

Start **next projects** with this in mind

1. External Review Criteria

- Criteria
- Motivation

2. Outcomes

- Recommendations from CSL

3. Conclusions

- Summary Table
- Future Plans



R 1: The **rationale** to make a **user permit maskable / non-maskable** should be **documented**. If no systematic rationale exists then the justification to make any specific user permit maskable should be documented.

R 2: The origin of the value of **1.6 μ s** used in the **glitch filter** should be **documented and reviewed**.

BIS filters 'glitches' from USER_PERMIT signals

R 3: **Every user condition** that contributes **to** a **user permit** input should be **justified**, in particular, the inputs that come from the experiments and other sources which are outside the BIS. In particular, **the safety relevance of each such condition should be documented**.

Why are users connected / what specifically are they protecting LHC against?



R 4: Continue to follow the recommendations made following the **UJ33 incident** and **ensure that these recommendations are incorporated** into **life cycle processes** for maintenance of the LHC.

Critical blind failure last year in UJ33

R 5: CSL recommends that a **member of the BIS team** participates in the **review of the optical beam permit detector** developed by the **LBDS team**. In particular this person should identify whether any **assumptions** were made by the LBDS team for the development of this function.

Interface BIS to LBDS

R 6: A **verification process** for changes to the **BIS configuration database** should be **defined**. This verification process could be a review of the changes log between two versions.

R 7: A means to **check the integrity of the database** before the pre-operational sequence is recommended.



R 8: A procedure should exist to **ensure** that the BIS portion of the **preoperational program run by the Control group is identical** to the program handed-over by the BIS group to the Control group.

must run pre-operational checks as defined

R 9: The short-term “**re-arm**” (**without checks**) button provided to the system operator is a source of risk that **should be removed**

R 10: The **test frequency of each user input** should be **specified**.

How often should we test?

1. External Review Criteria

- Criteria
- Motivation

2. Outcomes

- Recommendations from CSL

3. Conclusions

- Summary Table
- Future Plans

#	Description	Action: who?
1	Maskable / non-maskable partition	R.S. , J.W. + <i>MPP</i>
2	Glitch filter definition	<i>MPE/MI</i>
3	User connection justification	R.S., J.W. + <i>MPP</i>
4	Follow-up UJ33 recommendations	<i>MPE/MI</i>
5	LBDS BEAM_PERMIT detection	<i>ABT + MPE/MI</i>
6	Database change verification	<i>MPE/MI + CO/DM + MPP</i>
7	Database integrity check	<i>MPE/MI + OP (V.K.)</i>
8	Enforce pre-operational check execution	<i>MPE/MI + OP</i>
9	Remove "rearm"	<i>OP (Alick)</i>
10	Specify testing interval	<i>MPP</i>

Very complete set of work undertaken by CSL
11 pages of comments / questions / critique about VHDL alone
51 pages of discussions over their initial findings
N.B. Report /= certification of function!

Final report at CERN by next week
Will be presented to LMC on Wednesday 18th by Jeff Joyce

MPP & TE/MPE/MI must clarify deadline for addressing the recommendations

TE/MPE/MI are now satisfied with the BIS
+ reviewers did not find anything of concern in the design
+ We have guidelines for future systems
+ We would encourage others to follow similar exercises

Better the devil you know



FIN