Christos Zamantzas for the BLM team.

SUMMARY: EXTERNAL REVIEW RESULTS FOR THE LHC BLM SYSTEM

Machine Protection Panel 24/06/2011

External Auditors

Critical Systems Labs
Strategic Insight for Safety

Critical Systems Labs, Inc.
#618 - 475 Howe Street
Vancouver, B.C.
Canada V6C 2B3

http://www.criticalsystemslabs.com/

Auditors:

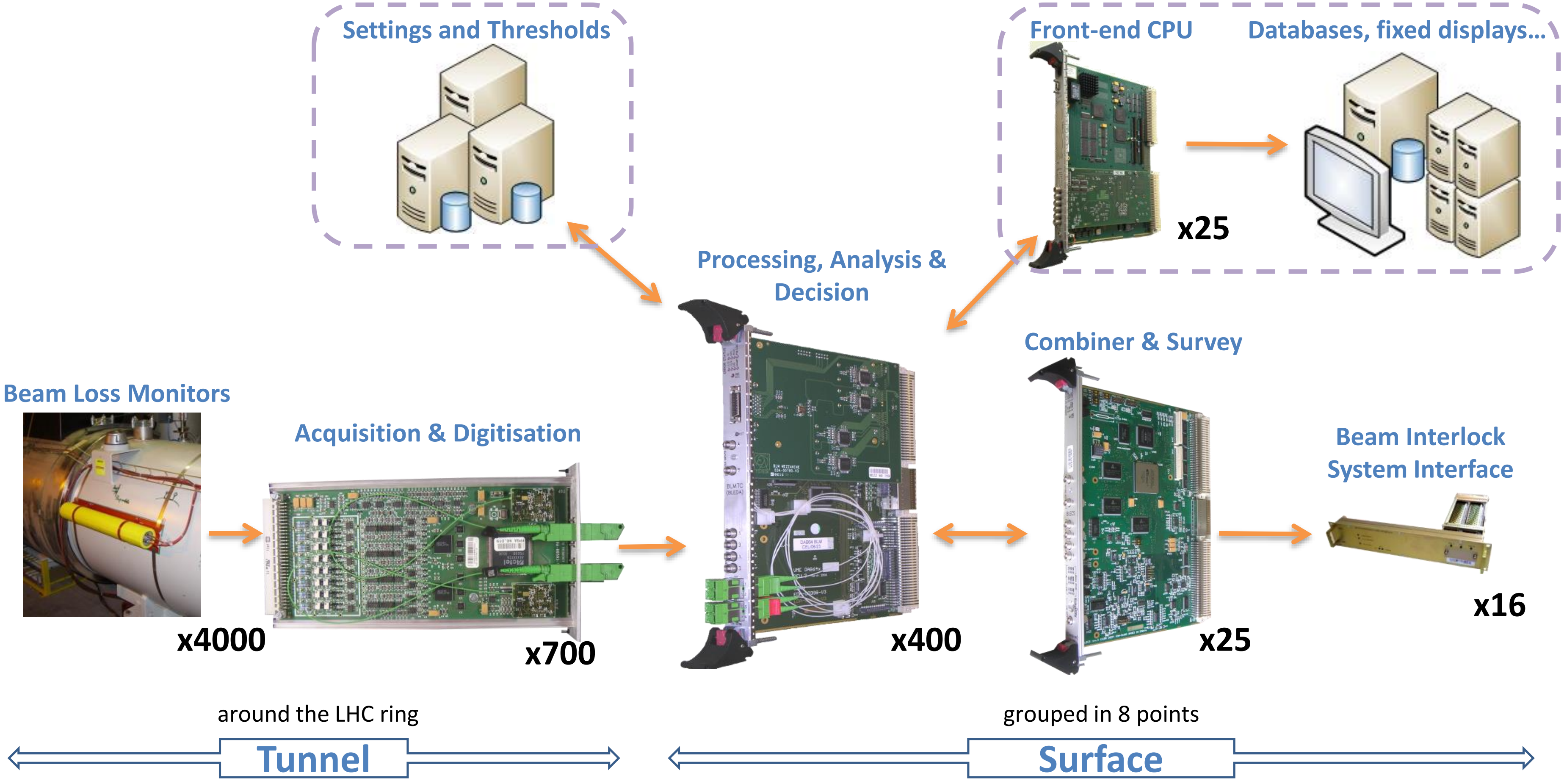
- Dr. Jeffrey Joyce
- Dr. Laurent Fabre
- Dr. Naghmeh Ghafari
- Dr. Lesley Shannon (external)
- Dr. Wolfgang Strigel (observer)

Scope of the external audit

CERN internal reviews have been performed in the past and these reviews focused primarily on the analogue parts of the system design. **Therefore the CSL review will focus more on the digital parts and particularly on the programmable parts of this system.**

The essential and foremost question that will drive the CSL technical review is: “Are the digital and programmable parts of the BLM system going to perform as they are intended to in the context of the BLM system?”

LHC Beam Loss Monitoring System



Review participants: B. Dehning, E. Effinger, J. Emery, C. Zamantzas

Additional things checked

- The propagation of a signal from the monitor input up to the interlock output
- Existing documentation
- Choice of technical options
- System verification techniques
- Performance of the Successive Running Sums
- Possible future changes

Successive Running Sums

Investigated:

- Dynamic range, accuracy and speed requirements
- Simulation and calculation models we've used for validation

Verified:

- Formal methods simulation model
- Collaborated with Cambridge university
  - Results will be presented this August at the **"16th International Workshop on Formal Methods for Industrial Critical Systems"**

Executive Summary

> **“With one minor reservation, we have found no reason to be concerned that the current configuration of the BLMS might fail to request a beam dump in response to a dangerous beam loss.**
>
> This conclusion is based on the following assumptions:
>
> (1) appropriate threshold settings are used;
>
> (2) the current operating procedures, including regular execution of the “connectivity test”, are maintained;
>
> (3) no element of the BLMS, such as an individual detector, is disabled without a decision by the appropriate authority that the safety risk is acceptable;
>
> (4) known limitations of the BLMS are adequately addressed before the machine is used at higher energies; and
>
> (5) the risk associated with the dependency of the BLMS on other systems for an accurate indication of bean energy is deemed to be acceptable by the appropriate authority.
>
> Changes to any aspect of the design may invalidate this conclusion.”

The Reservation

“The *one minor reservation* associated with the above conclusion is the fact that the critical real-time datapath responsible for generation of a beam dump request is **not fully redundant**.

Hence, there are single points of failure in the design of this critical portion of the BLMS.

In this regard, we are concerned mostly about non-redundant elements of this datapath within the **Threshold Comparator Field Programmable Gate Array (FPGA)**.”

All comments from CSL – emphasis mine

SUMMARY OF FINDINGS

Summary of findings 1/4

1. The design of the BLMS is **conservative**, except where novel solutions are needed to overcome limitations of known solutions.
2. The design of the BLMS includes very **substantial** provision for **error detection**. Fault tolerance is used appropriately.
3. The critical path for beam dump requests includes some **single points of failure**.
4. The BLMS serves **other purposes** besides machine protection. This might bring other interests into conflict with the safety objective of the BLMS.

Summary of findings 2/4

5. **Separation of critical parts** of the design from non-critical parts is not an explicit feature of the design.
6. Very **high utilization** of the logic elements in the BLECF and BLMTC FPGAs could be problematic as it evolves over the lifetime of the LHC.
7. The algorithm and circuit design for the BLMTC **Successive Running Sums** (SRS) calculation is **very complex**.

Summary of findings 3/4

8. The **lack of a comprehensive specification** of the BLMS requirements will likely have an adverse effect on the maintainability of the system.
9. System maintainers could have difficulties **understanding the VHDL code** for several reasons, especially the lack of meaningful comments.
10. While impressively diverse, it is **difficult to** objectively **assess** the adequacy of the **verification results**.
11. Proof testing is very substantial, but **operational procedures** concerned with proof testing are **unclear**.

Summary of findings 4/4

12. There are known limitations of the BLMS that need to be addressed, e.g., insufficient dynamic range of the detectors near the injection sites.
13. There is a lack of safeguards to protect against human error when critical data such as threshold settings is modified.
14. There are a number of ways in which the maintainability of the system could be improved.
15. It is unclear how operators and system maintainers will become aware of problems that arise while the system is operating.
16. The safety of the BLMS depends on other systems including the BETS and GMT link.

All comments from CSL – emphasis mine

RECOMMENDATIONS

Recommendations 1/4

- #1: There should be a clear **policy statement** by the Director for Accelerators and Technology that **changes to the BLMS** design for the purpose of enhancing or modifying the capability of the BLMS to provide measurements of beam loss **must not compromise the safety** of the BLMS, i.e., its ability to reliably detect a dangerous loss.
- #2: The **engineering documentation** for the BLMS design should be enhanced to distinguish critical from non-critical elements of the design, and to record an evidence-based argument that the critical functionality is sufficiently isolated from the non-critical functionality (if such an argument can be made).
- #3: Any proposal to **modify the BLMS** in a manner that would increase the amount of utilization of the FPGAs should be strongly resisted unless some previous change to the BLMS has reduced the utilization to a level that easily accommodates additional functionality without increasing the utilization back to a very high level.

Recommendations 2/4

- #4: Options to **reduce the utilization** of the FPGAs should be identified and evaluated.
- #5: A comprehensive specification of the required **functional behaviour** of the BLMS should be created and maintained using a style and format that is amenable to modification as changes are made over its lifetime.
- #6: The understandability of the VHDL code should be significantly improved with the addition of **meaningful in-line comments**.

Recommendations 3/4

- #7: A **Master Verification plan** should be created to document the verification approach from a top-down perspective, e.g., what tests have been allocated to each component of the system. This document will guide system maintainers when changes are made to the system.
- #8: A formal policy should be established to impose limits on the ability of a single individual to modify the procedure for starting the accelerator in any way that would override, inhibit or otherwise interfere with the performance of the **connectivity test**.
- #9: A **schedule** for each form of proof testing should be defined along with a means by which operators would know if some form **of proof testing has not been performed** according to schedule, **or** if the results indicate an **unresolved problem**.

Recommendations 4/4

- #10: **Safeguards** should be added **to the tools** used to modify critical data to reduce the likelihood of simple human errors such as incorrect keystrokes.
- #11: A comprehensive procedure for **monitoring the status** of the BLMS should be defined to ensure that operators and system support maintainers will become aware of faults and other problems in a systematic and timely manner. This procedure should include review activities to be performed after each LHC run.
- #12: The LHC Machine Protection Committee should determine whether the risk associated with the **dependency of the BLMS** on other systems has been adequately controlled.

CONCLUSIONS AND FUTURE

Conclusions

- Lengthy and hectic procedure but provided excellent experience.
- CSL had multiple people (each having his own expertise) “attacking” the system from all fronts (specifications, documentation, testing, procedures, implementation,...).
- Helped to organise our multiple priorities.
- Accumulated knowledge that we can transfer on new projects.

Modifications List

Long-term:

- (complete) the Master Verification Plan

Short-term:

- Improve documentation
- Add functionality to inhibit the beam dump request on injection
- Add dedicated data for the automatic collimator beam-based alignment

As soon as possible:

- Full deployment of the “Study” buffer (part of the Capture function)
- Deploy the continuous high voltage check
- Add VME block transfer (DMA memory)

THANK YOU