EUROPEAN
SPALLATION
SOURCE

Design Concepts for the Beam Interlock System

Annika Nordt et al.

European Spallation Source ERIC

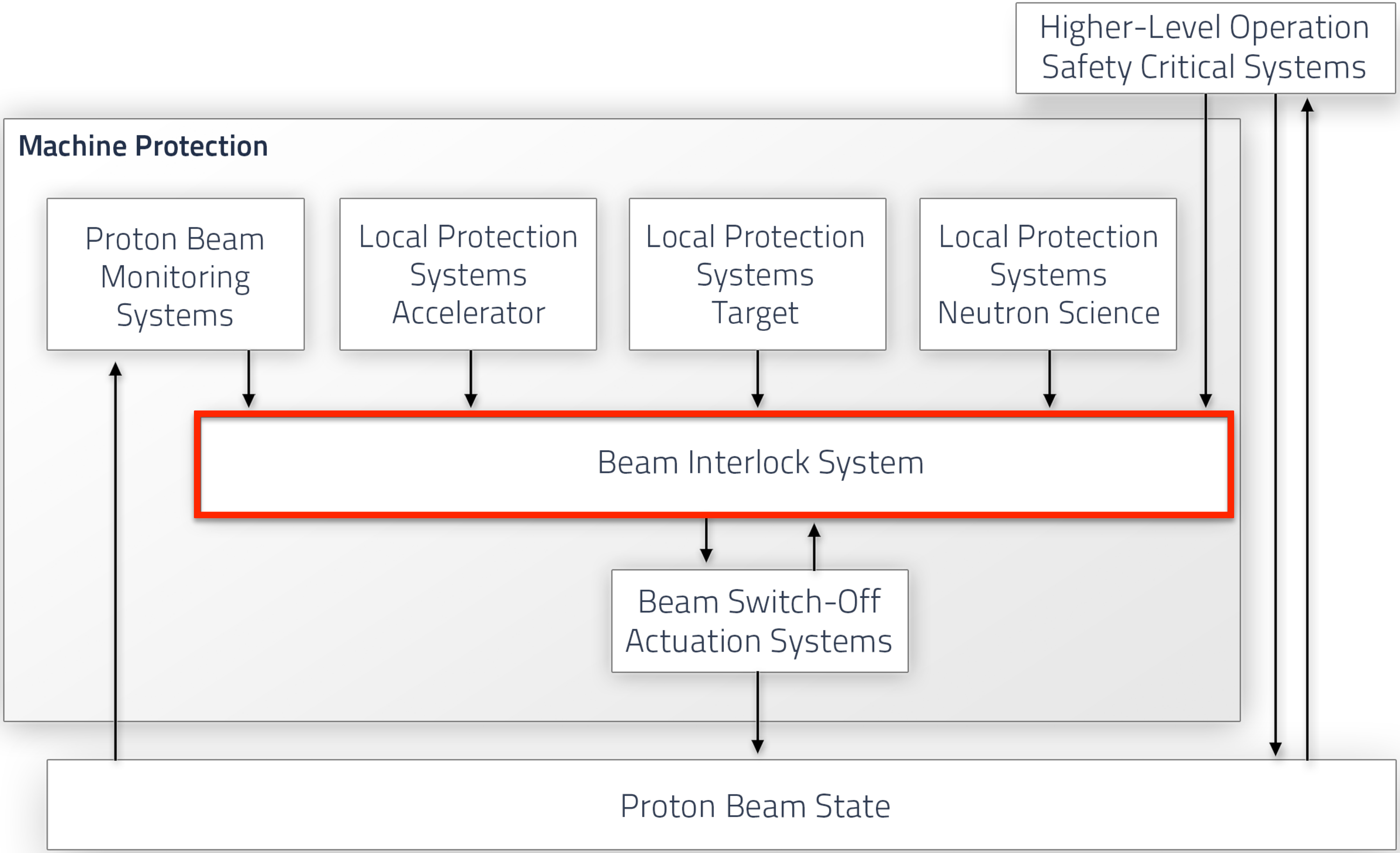
Machine Protection Review, December 2015

Lund, Sweden

Overview

1. The idea of one Beam Interlock System
2. The idea of splitting: have 2 Beam Interlock Systems
3. Pros and Cons
4. Summary

Reminder: Functional MP Architecture Concept



Higher-Level Operation Safety Critical Systems

Machine Protection

Proton Beam Monitoring Systems

Local Protection Systems Accelerator

Local Protection Systems Target

Local Protection Systems Neutron Science

Beam Interlock System

Beam Switch-Off Actuation Systems

Proton Beam State

Question

How could this

Beam Interlock System Box

look like?

First Concept Idea for a BIS

Build 1 Beam Interlock System

Connecting ALL MP related systems!

That BIS has to be:

Fast… with a reaction time of 3 µs!

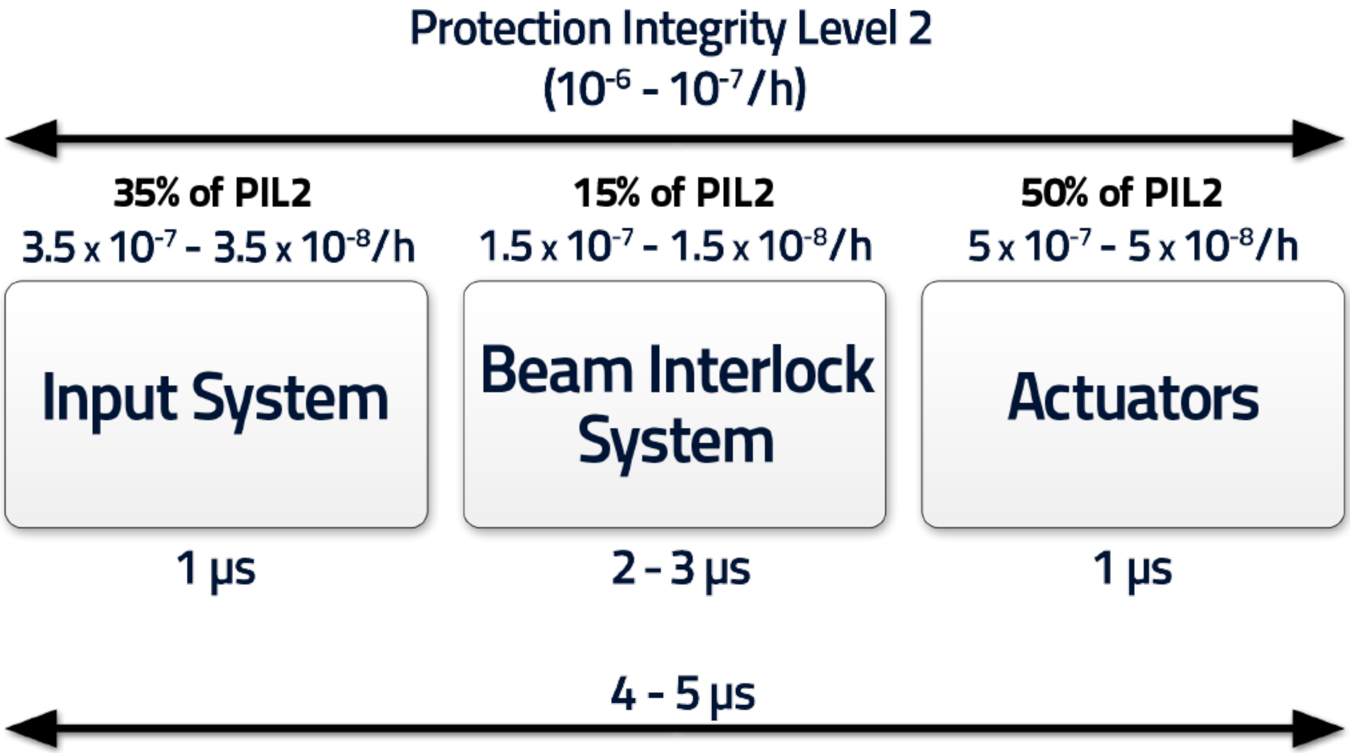
Reliable… with a failure rate of

$1.5 \cdot 10^{-7}$/h - $1.5 \cdot 10^{-8}$/h

(no matter what)

How Fast/How Reliable?

Based on preliminary risk
analysis (IEC61508, IEC61511)



Protection Integrity Level 2
(10^{-6} - 10^{-7}/h)

35% of PIL2
3.5 x 10^{-7} - 3.5 x 10^{-8}/h

15% of PIL2
1.5 x 10^{-7} - 1.5 x 10^{-8}/h

50% of PIL2
5 x 10^{-7} - 5 x 10^{-8}/h

Input System

Beam Interlock System

Actuators

1 μs

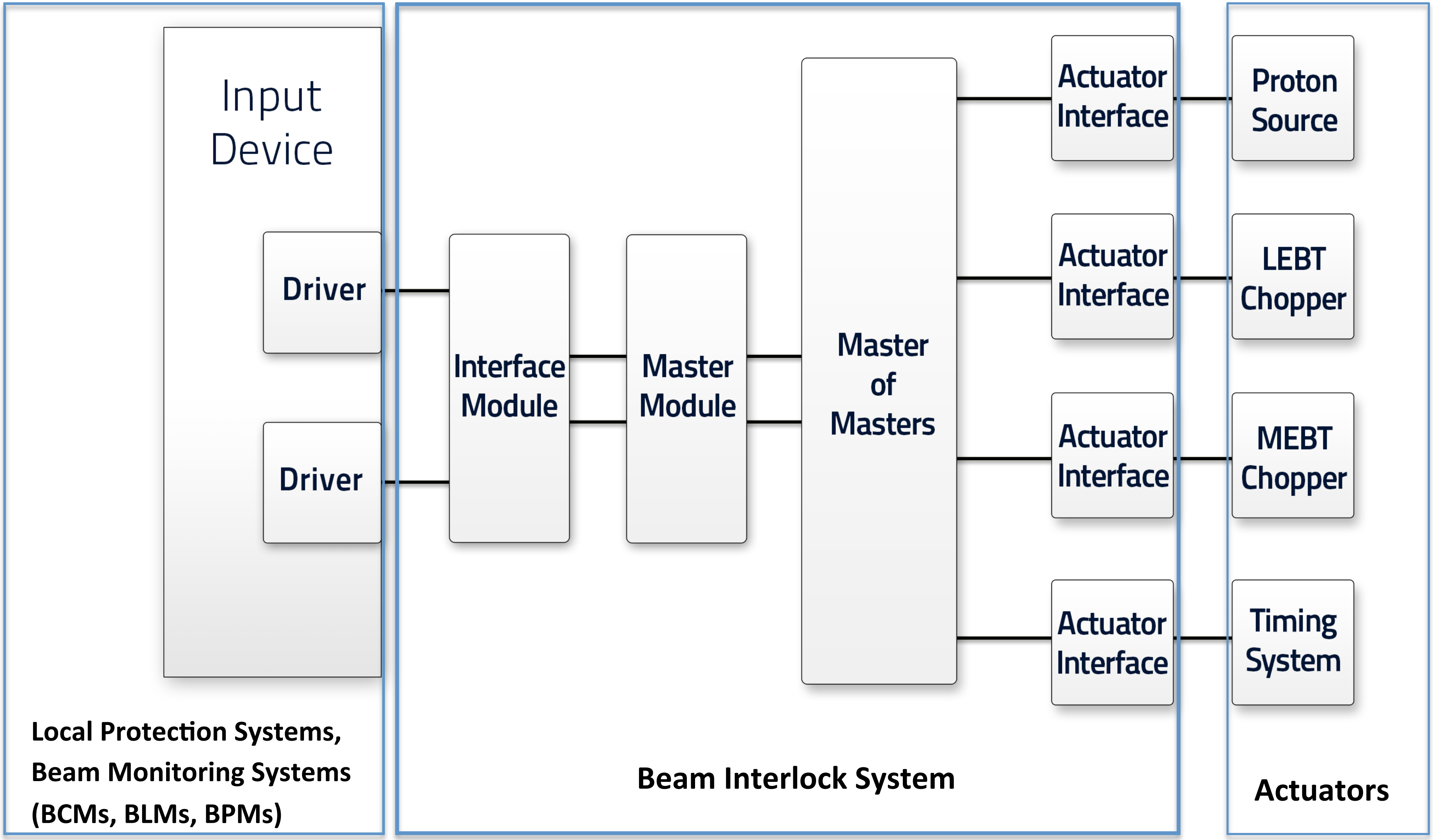
2 - 3 μs

1 μs

4 - 5 μs

These are the most stringent requirements in terms of response time and PIL level.

Modular Design Concept (adapted from CERN)



Advantages of Such Modular Design

This modular design approach:

1) Allows for a clear assignment of responsibilities

- ICS/WP5 is in charge to deliver the Beam Interlock System
- Stakeholders for MP related systems in AD, Target, NSS are in charge to deliver the MP relevant systems (to be compliant with MP requirements)
- Stakeholders for MP related systems in AD, Target, NSS are in charge to implement the drivers on their system (the driver is provided by ICS/WP5)
- Stakeholders for actuator systems are responsible to deliver the actuation systems (to be compliant with MP requirements)

2) Eases and speeds up the detection of faults, erroneous configuration, etc.

To be Thought of, When Going for 1 BIS

To build 1 BIS, implies to come up with a design that allows to connect (almost) any system to it, no matter what technology is being used by the systems connected to it (i.e. the BIS design needs to cope with that), examples:

- we have PLC based Local Protection Systems (rather slow/ms range).

  An example is the target Local Protection System

- we have FPGA based Local Protection Systems (fast/ µs range)

  An example is the RF Local Protection System

- we have FPGA based Beam Instrumentation Systems (fast/ µs range)

  An example are the Beam Loss Monitors

- we have PLC based Beam Instrumentation Systems (slow/ms range)

  An example are the Wire Scanners

To be Thought of, When Going for 1 BIS

If this one Beam Interlock System fails, ***it fails***, and we have (currently) no second layer of protection! i.e. no backup system that can stop beam operation!

A blind/dangerous failure[1] of the BIS can potentially lead to really severe damage leading to long downtime and costly repair actions or **worse[2]**.

[1] blind/dangerous failure: in case the BIS should stop beam but it does not because of an internal failure

[2]

"NOW THIS IS NOT THE END. IT IS NOT EVEN THE BEGINNING OF THE END. BUT IT IS, PERHAPS, THE END OF THE BEGINNING."

WINSTON CHURCHILL

SO WE IGNORE EACH OTHER, AND PRETEND THE OTHER PERSON DOESN'T EXIST BUT DEEP DOWN, WE BOTH KNOW IT WASN'T SUPPOSED TO END LIKE THIS

Second Concept Idea

Split!

Build two Beam Interlock Systems:

One for the slow systems that are connected to a slow BIS

One for the fast systems that are connected to a fast BIS

Background thoughts:

We have an almost equal amount of signals that can be categorized into being slow and fast (200 fast and 200 slow)

Therefore…Why not connecting:

All slow signals/devices to a "slow" BIS (SBIS)

All fast signals/devices to a "fast" BIS (FBIS)?

Counting…

Categorization of signals/devices/systems regarding their response times (slow/fast) is given in:

https://ess-ics.atlassian.net/wiki/download/attachments/60031539/BIS-SAS-v0.7.docx?version=1&modificationDate=1449354043697&api=v2

(Table 4 and 5).

The number of signals from slow and fast devices is listed to be:

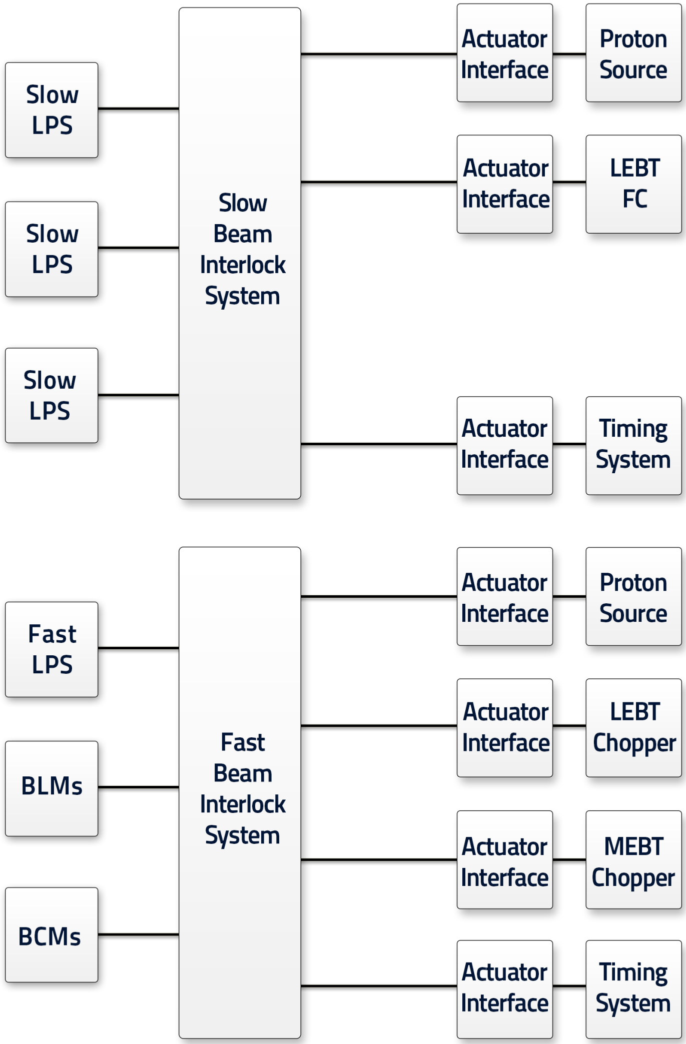
Sum slow signals (no aggregation): 576

Sum slow signals (aggregation): 156

Sum fast signals (no aggregation): 427

Sum fast signals (aggregation): 213

Different approaches for Concept #2



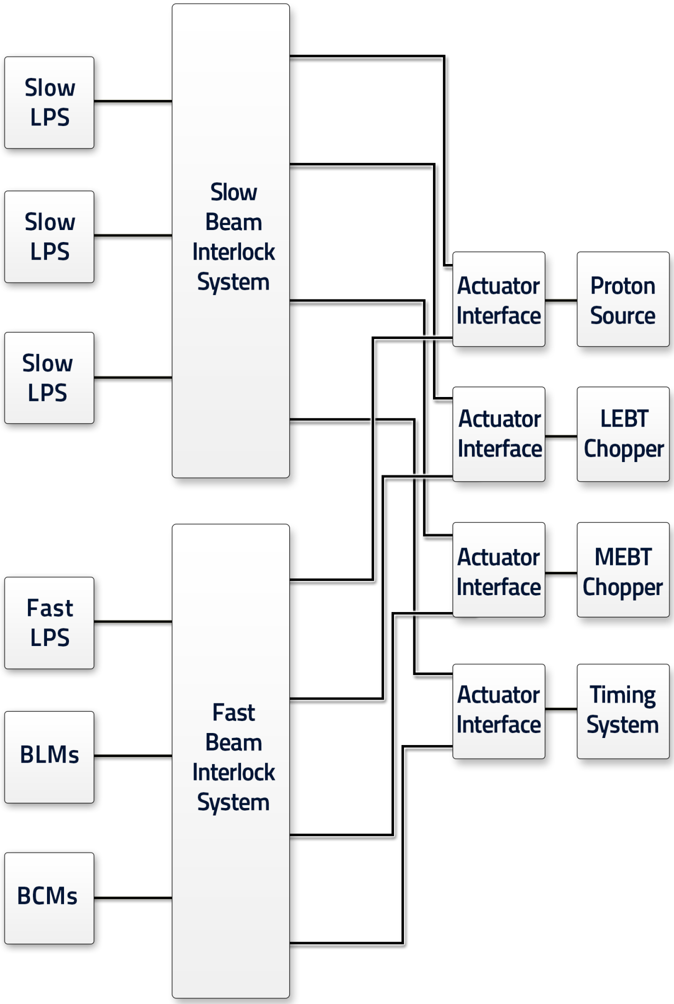
Have two fully separated Beam Interlock Systems

Potentially even using different actuator systems

The usage of different actuator systems strongly depends on the response times required for the implemented protection functions

Such approach allows to build fully diverse redundant Beam Interlock Systems

Different approaches for Concept #2



Have two fully separated Beam Interlock Systems

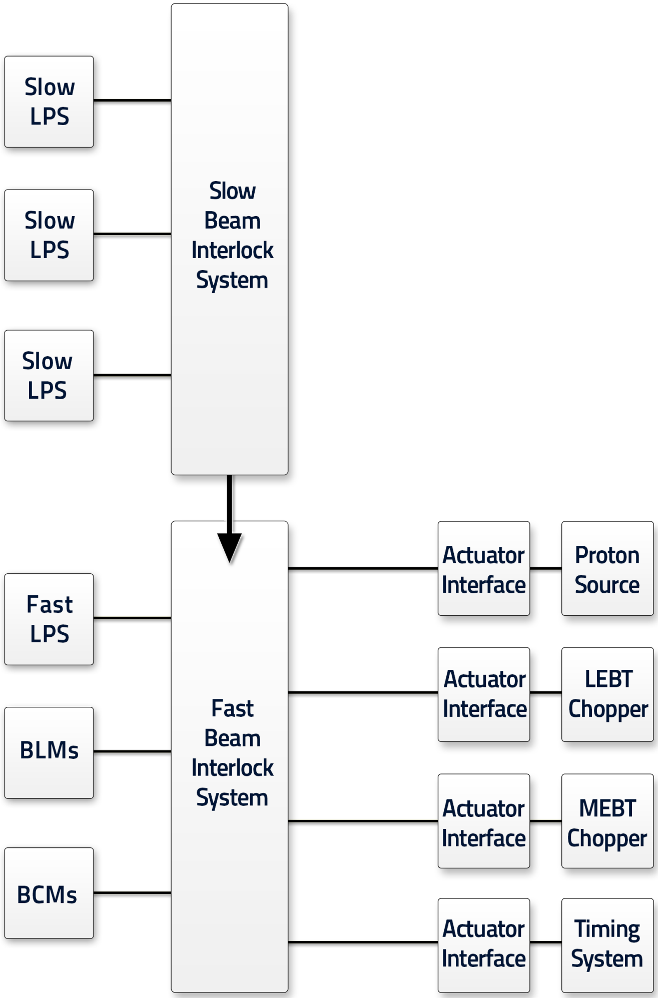
But use the same actuator systems

Potentially share the same actuator interface modules to communicate to the actuator systems.

Single point of failure:

Actuator interface modules.

Different approaches for Concept #2



Have two fully separated Beam Interlock Systems

But simply send a BEAM_PERMIT signal from the Slow BIS to the FAST BIS

Like this, the single point of failure is still the Fast BIS

Check

More details on the Fast BIS design can be seen in Angel Monera’s talk

More details on the Slow BIS design can be seen in Manuel Zaera-Sanz’ talk

Summary

Two major design concepts were presented and we need your feedback on

whether its worse to follow up more the idea of concept idea #2

(ie splitting the BIS into 2 such that we add diverse redundancy)

Let’s discuss