Zurich University
of Applied Sciences

School of
Engineering

IAMP Institute of Applied
Mathematics and Physics

FBIS Driving Requirements and Architectural Design Constraints

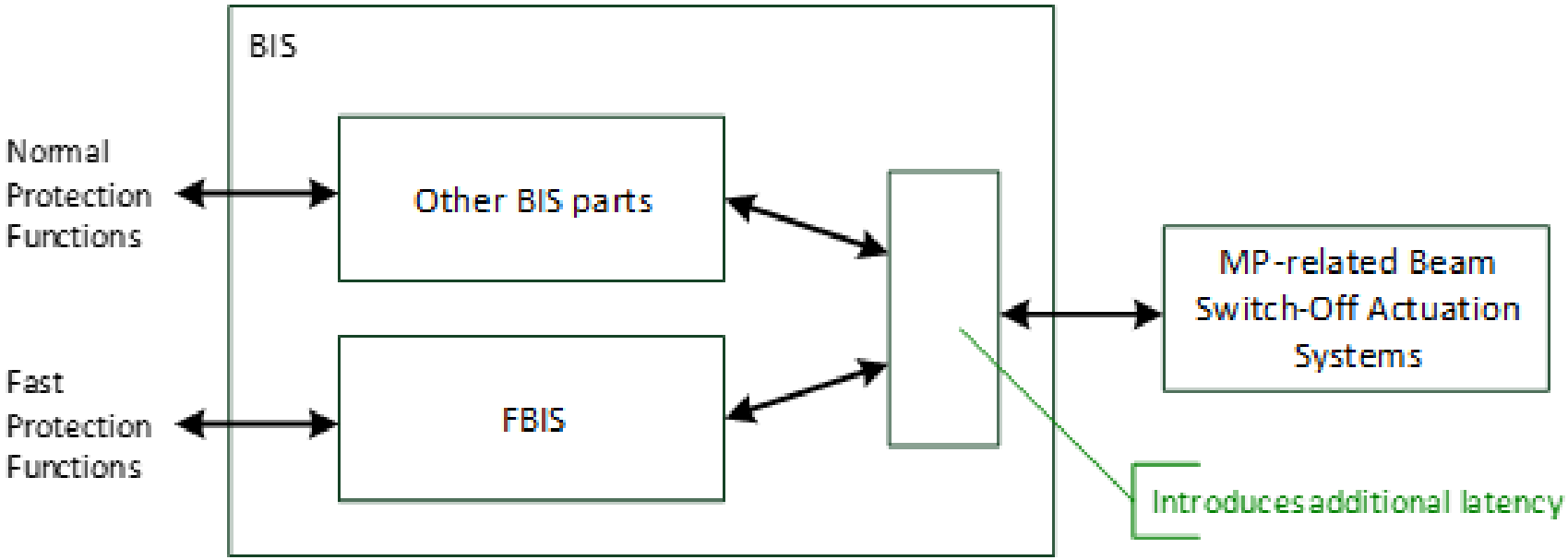
14.08.2017

1. Minimize Latency

- *latency* is defined as the time needed by the FBIS to generate an output once a state change has occurred at any FBIS input
- FBIS latency contributes to reaction time of all Protection Functions involving the FBIS
  - the time to detect the hazard and communicate this to the FBIS
  - FBIS latency
  - the time the MP-related Actuation Systems need to achieve a Protected State.

1. Minimize Latency

Not favorable:

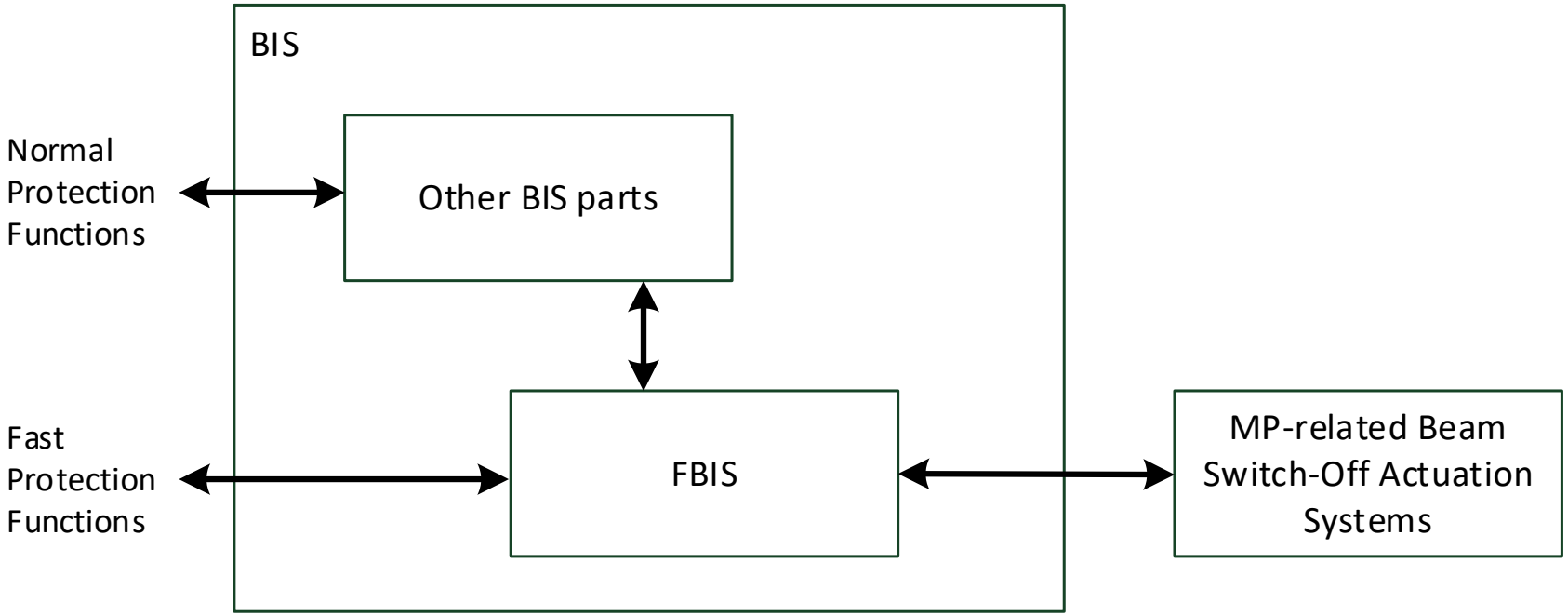


Architectural Design Constraint:

The FBIS has to be implemented such as to allow other parts of the BIS to access to the MP-related Beam Switch-Off Actuation Systems.

1. Minimize Latency

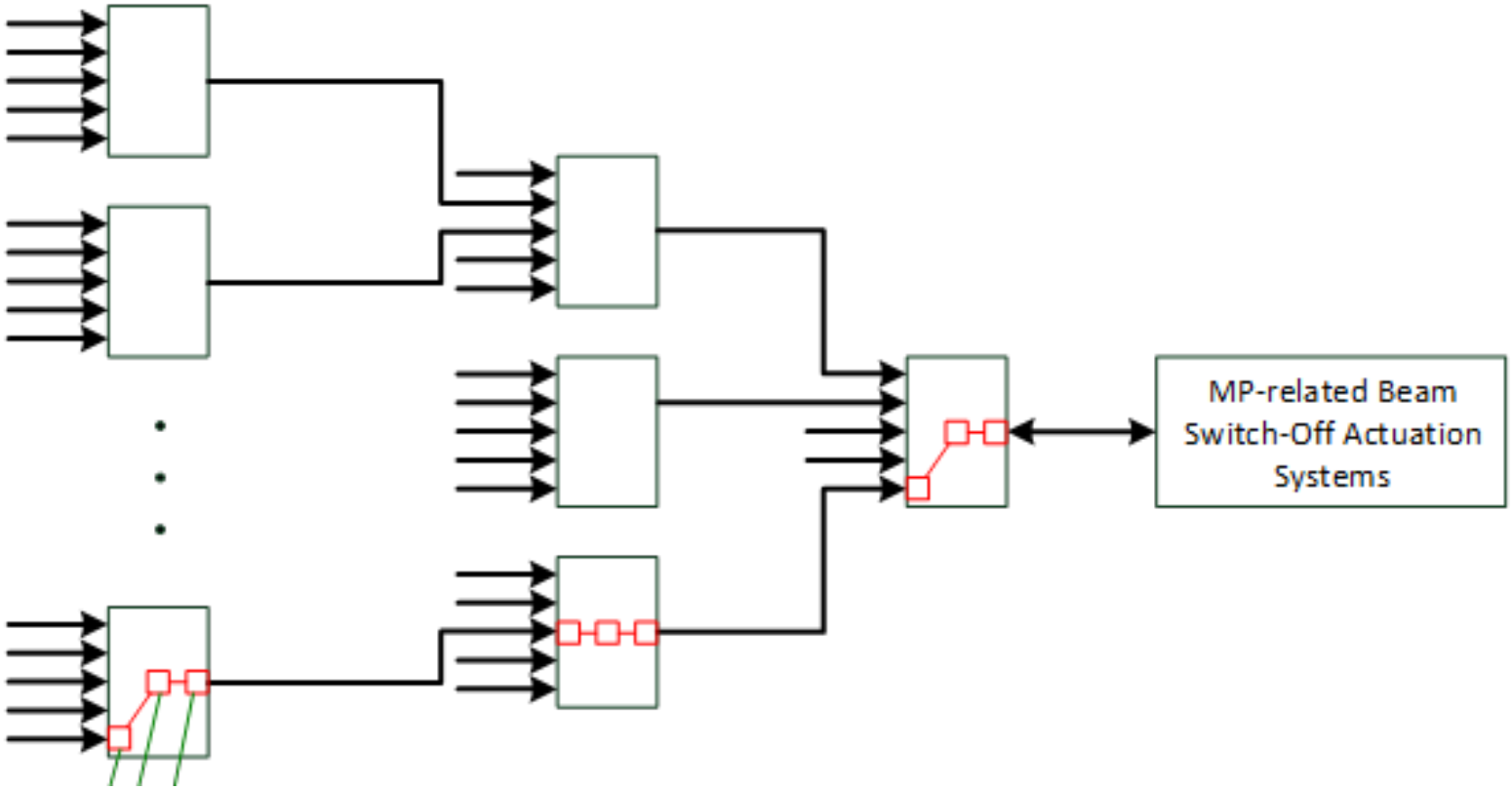
Favorable:



Architectural Design Constraint:

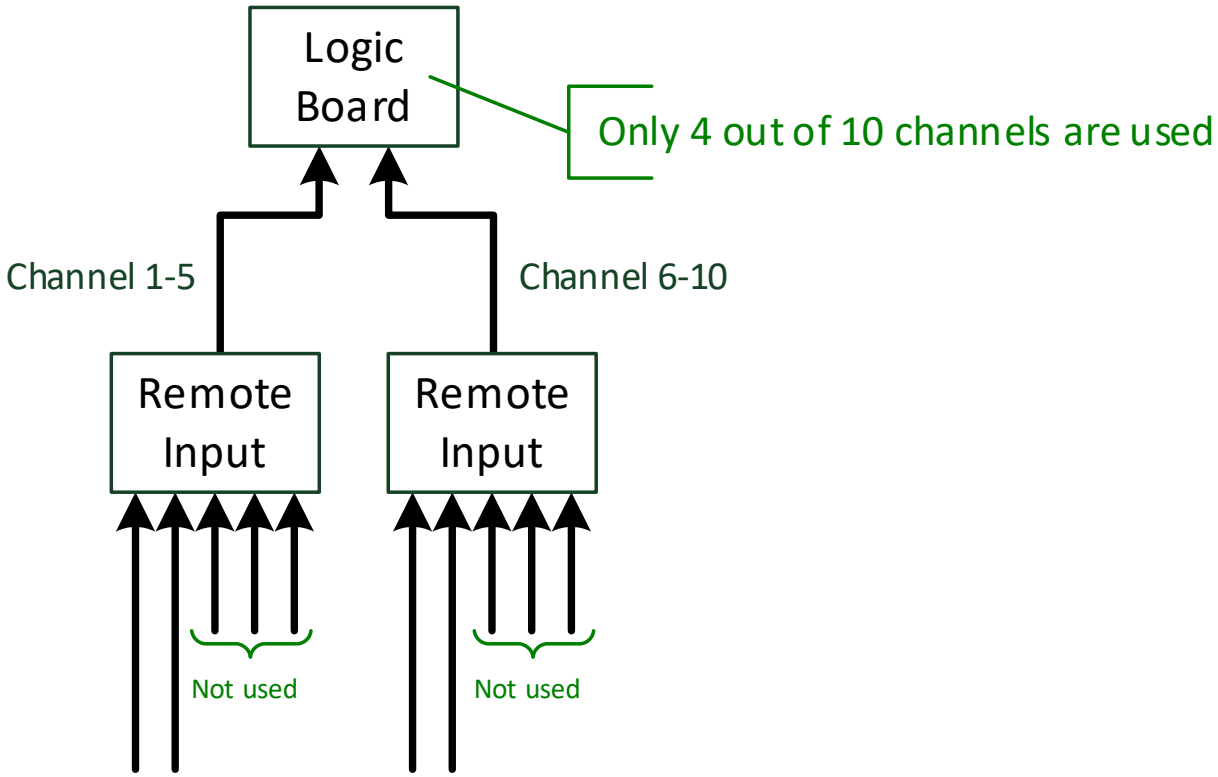
The FBIS has to be implemented such as to allow other parts of the BIS to access to the MP-related Beam Switch-Off Actuation Systems.

1. Minimize Latency



Implement the FBIS such as to maximize the number of inputs that can be processed in one single step in order to minimize tree depth.

1. Minimize Latency



Arrange connection of signals to the FBIS such as to avoid unused inputs.

2. Maximize Availability

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

- Prefer Modular Approach with High Diagnostic Coverage and Easy Replacement
  - Reduce MTTR through a modular system
  - Well-designed built-in tests for quick problem localization
  - Reduce dis- and reconnecting of cables whenever possible (can be time consuming, bears a high risk for errors)
  - Rules out pizza-box designs

The FBIS should be structured in well-defined LRU's that need to be easily replaceable. Special attention has to be put on external connections.

The FBIS should allow easy failure localization and feature sufficient built-in testing functions for this.

The FBIS should be based as much as possible on standard ESS Controls equipment to simplify spare-parts management / maintenance procedures

2. Maximize Availability

- Operation in “Degraded Mode”
  - Allow operation although certain elements (FBIS or external to FBIS) are not operational

The FBIS should allow disabling selected parts under controlled circumstances (degraded mode).

3. Support PIL2 Protection Functions

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

- Even though:
  - ESS hazard and risk analysis has not yet been completed,
  - Overall Protection Functions requiring stronger risk reduction might be needed
- … we believe PIL 2 will be the highest achievable in the context of the ESS project
- Aiming at satisfying IEC61508 SIL3 requirements is not realistic
- Any requirement for a PIL3 Protection Function will need to be “broken down”

3. Support PIL2 Protection Functions

- Expectation: FBIS requests beam-switch off more often than once a year → high-demand mode → IEC 61508-2

Table 3 – Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	Not Allowed	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Design the FBIS components such as to keep the option to achieve a Hardware Fault Tolerance of 1 or higher.

Built-in test functionality must be extended with a fail-safe failure reaction mechanism to increase the safe failure fraction.

4. Scalable with respect to Number of Inputs

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

- List of Protection Functions defined now is neither
  - Complete
  - Static

→ No additional Architecture Constraints

5. Support staged Commissioning of ESS

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

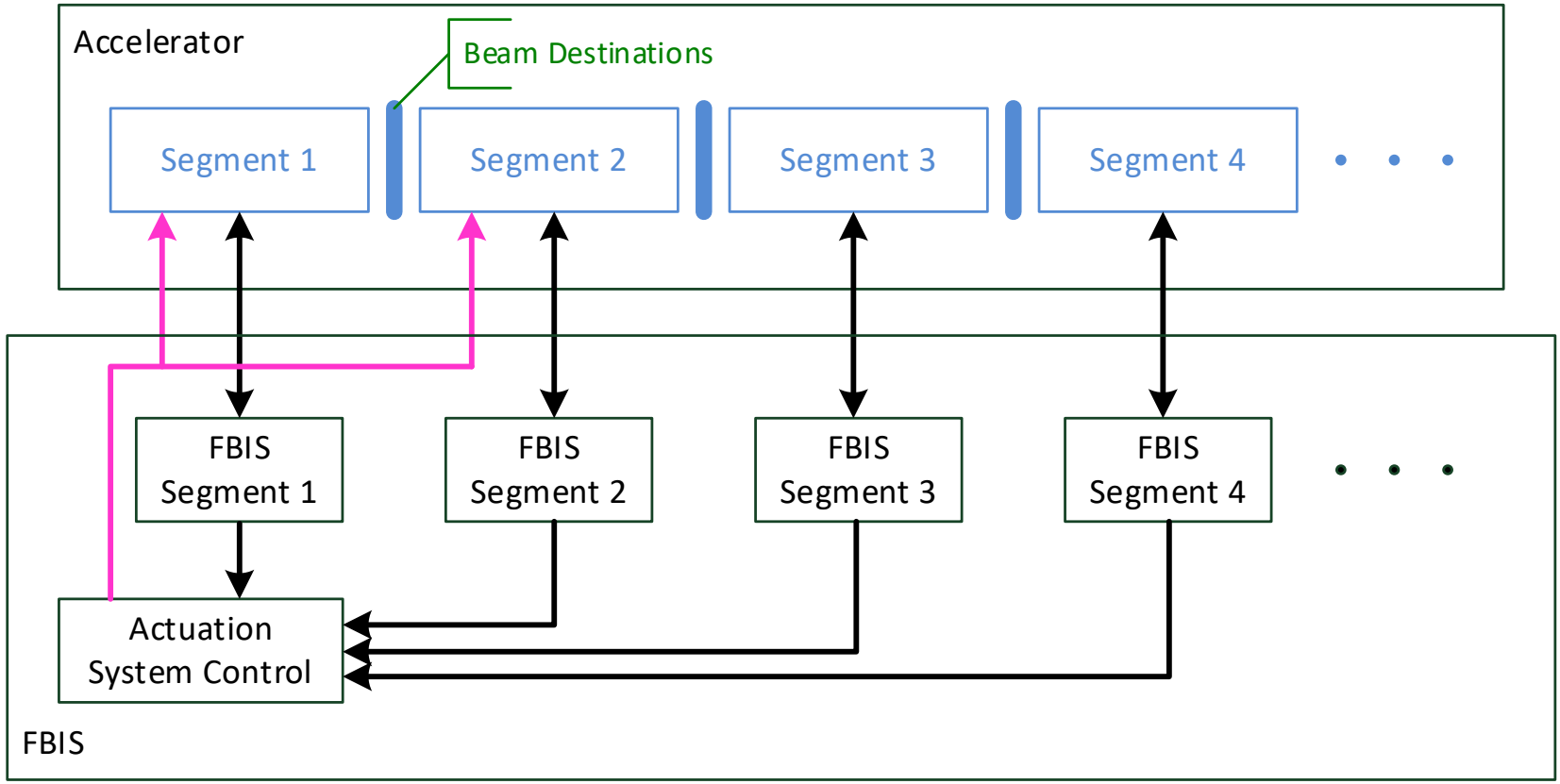
- ESS accelerator will be built and commissioned step-by-step
- Commissioning a segment with beam will require the Fast Protection Functions to be operational.
- FBIS sections needed for those functions needs to be
  - commissioned beforehand
  - Operational
- Tested and verified FBIS sections should only be changed when really necessary.

The FBIS architecture should support the concept of segments and be scalable in terms of segments.

Signals related to Protection Functions dedicated to one accelerator segment should be connected to the corresponding FBIS segment.

5. Support staged Commissioning of ESS

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics



6. Support ESS Lifetime requirements

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

- ESS is supposed to have lifetime longer than 20 years.
  - Hardware ageing, obsolescence issued
  - Basic function of the FBIS is likely to stay the same
  - Basic function of FBIS mainly defined by firmware

The firmware defining the FBIS function should not have direct dependencies to the hardware it runs on.

7. Seamless Integration into ESS Control System Landscape

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

- consequence from → maximize availability
- Simplifies
  - spare-parts management
  - Maintenance

→ No additional Architecture Constraints

For more information see document:

FBIS_Architectural_Design_Options

Contact:

Martin Rejzek
martin.rejzek@zhaw.ch

http://www.iamp.zhaw.ch/sks

List of Architectural Design Constaints 1/3

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

- The FBIS has to be implemented such as to allow other parts of the BIS to access to the MP-related Beam Switch-Off Actuation Systems.
- Implement the FBIS such as to maximize the number of inputs that can be processed in one single step in order to minimize tree depth.
- Arrange connection of signals to the FBIS such as to avoid unused inputs.
- The FBIS should be structured in well-defined LRU's that need to be easily replaceable. Special attention has to be put on external connections.
- The FBIS should allow easy failure localization and feature sufficient built-in testing functions for this.

List of Architectural Design Constaints 2/3

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

- The FBIS should be based as much as possible on standard ESS Controls equipment to simplify spare-parts management and maintenance procedures.
- The FBIS should allow disabling selected parts under controlled circumstances (degraded mode).
- Design the FBIS components such as to keep the option to achieve a Hardware Fault Tolerance of 1 or higher.
- Built-in test functionality must be extended with a fail-safe failure reaction mechanism to increase the safe failure fraction.

List of Architectural Design Constaints 3/3

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

- The FBIS architecture should support the concept of segments and be scalable in terms of segments.
- Signals related to Protection Functions dedicated to one accelerator segment should be connected to the corresponding FBIS segment.
- The firmware defining the FBIS function should not have direct dependencies to the hardware it runs on.