ZHAW – Institute of Applied Mathematics and Physics (IAMP)

Fast Beam Interlock System (FBIS)

Architectural Design Options

Version:	-
Alias:	-
Date:	31.07.2017
Author:	Christian Hilbes, Martin Rejzek
ID:	CB:283431

Distribution List:

Christian Hilbes	ZHAW – IAMP
Martin Rejzek	ZHAW – IAMP
Sven Stefan Krauss	ZHAW – IAMP
Monika Reif	ZHAW – IAMP
Edy Rehm	ZHAW – IAMP
Hans Doran	ZHAW – INES
David Ganz	ZHAW – INES
David Blatter	ZHAW – INES
Prosper Leibundgut	ZHAW – INES

Revision History:

Christian Hilbes	09.04.2017	Document created
Martin Rejzek	05.05.2017	Extended with discussion results from 04.05.2017. Replaced figures
Martin Rejzek	09.06.2017	Extended Sensor Side Interfaces. Reworked and improved drawings. Completed pro/con-tables.
Martin Rejzek	15.06.2017	Added chapter with FBIS architectural design proposal
Martin Rejzek	12.07.2017	Moved design proposal to separate document. Added design options conclusion.
Martin Rejzek	31.07.2017	Fixed typos.

Table Of Contents

1 Introduction

1.1 Purpose

This document systematically summarizes and analyzes the driving requirements for the architectural design of the ESS Fast Beam Interlock System (FBIS) and collects the main architectural design options that have been considered so far.

The purpose of this document is twofold:

- To trigger the generation of further architectural design options.
- To support the decision-making process of selecting a final FBIS architecture.

To allow for the necessary discussions, the document is written in a rather informal style.

The document is structured as following:

- Chapter 2 analyses the driving requirements and describes their rationales. For every driving requirements the architectural design constraints are summarized.
- Chapter 3 provides architectural design options and discusses their pros and cons
- Finally, chapter 4 contains a preliminary conclusion.

1.2 Scope

It is recognized that some hazards will require Protection Functions with very fast reaction times in order to avoid damage or activation of the machine. We call those functions *Fast Protection Functions*.

The *Fast Beam Interlock System* (FBIS) is that part of the *Beam Interlock System* (BIS) that deals with Fast Protection Functions. All Protection Functions involving the BIS are by definition Beam-related Protection Functions. We will omit the suffix “beam-related” in the rest of this document in obvious cases.

Figure 1 gives an overview of the FBIS environment and Figure 2 shows the internal scope of the FBIS.

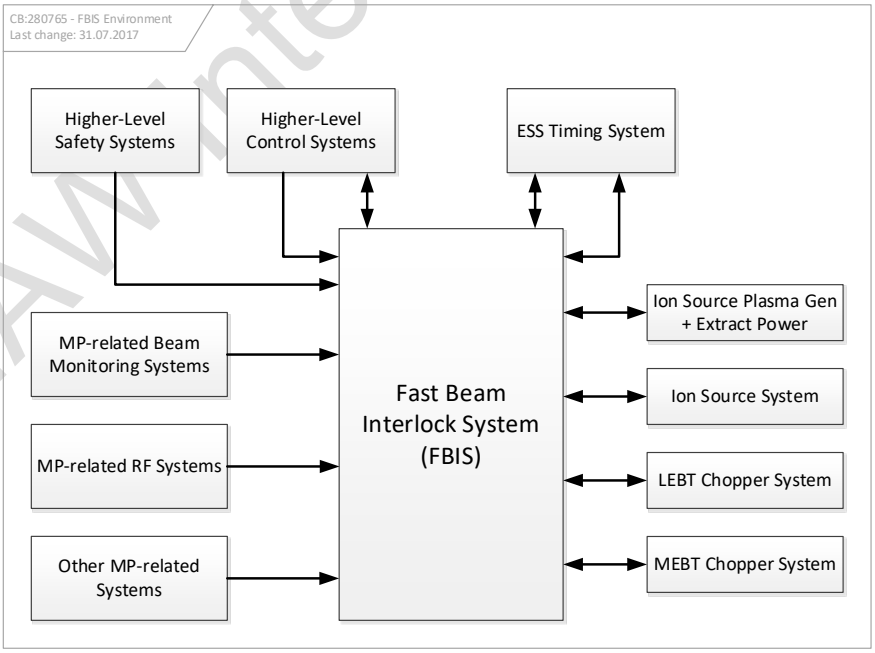

Figure 1: FBIS Environment.

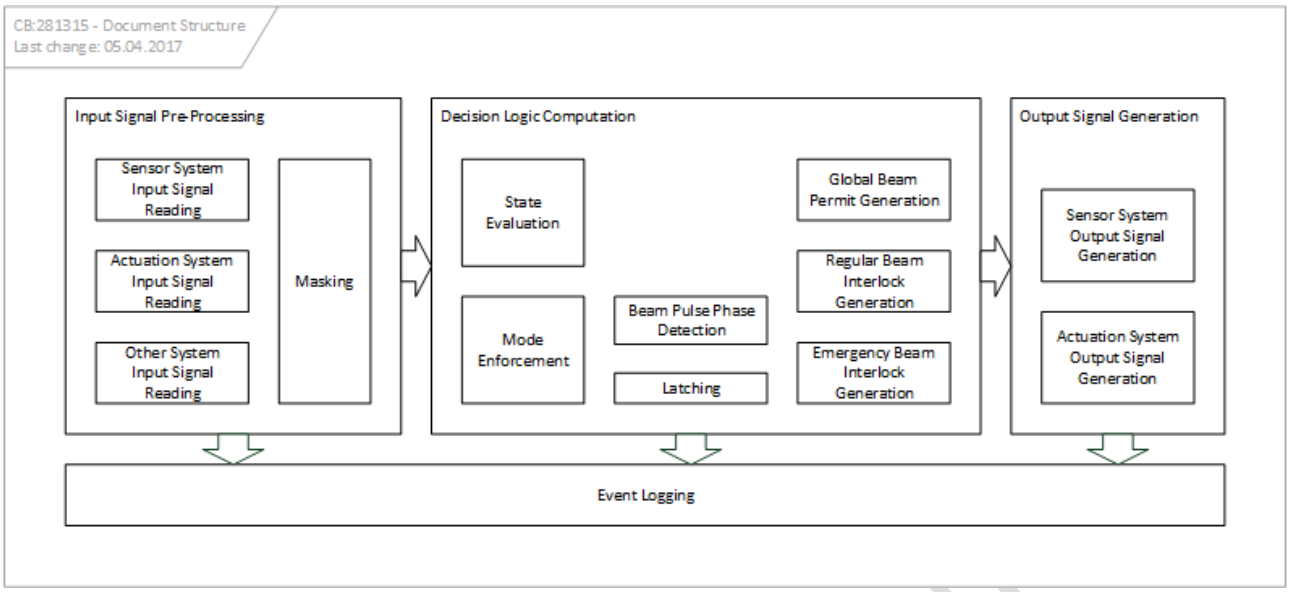

Figure 2: FBIS internal scope (draft).

1.3 References

None

2 FBIS Driving Requirements Analysis

The main requirements driving the architectural design of the FBIS can be summarized as:

1. Minimize latency
2. Maximize availability
3. Support PIL2 Protection Functions (IEC 61508 SIL2 Requirements)
4. Scalable with respect to number of inputs
5. Support staged commissioning of ESS
6. Support ESS Lifetime Requirements
7. Seamless integration into ESS Control System Landscape

The following sections contain an analysis of those requirements, deriving architectural design constraints.

2.1 Minimize Latency

2.1.1 Rationale

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

A clear specification of the reaction time requirements for the individual Fast Protection Functions and a maximal latency requirement for the FBIS would be ideal. However, we believe that it will not be possible for ESS to generate exact requirements specifications, at the level of single micro-seconds, for the reaction time of Fast Protection Functions in this phase of the project. There are simply too many unknowns with respect to the dynamic behavior of many of the accelerator elements at this time. Rather than making a best guess on the maximal tolerable FBIS latency, we adopt the conservative approach to minimize the latency as far as possible.

2.1.2 Architectural Design Constraints

2.1.2.1 Direct Interfacing to MP-related Beam Switch-Off Actuation Systems

The following analysis does in principle take place at the scope level of the BIS and not the FBIS. Hence, it results in an architectural design constraint for the BIS and not for the FBIS. Unfortunately, architectural design at the scope level of the BIS has not progressed to a sufficient level. But, because this question is of high importance to the FBIS design, we include it here.

The MP-related Beam Switch-Off Actuation Systems are used in all Beam-related Protection Functions, including of course the Fast Beam-related Protection Functions. If we want to minimize the reaction time of Fast Beam-related Protection Functions, we have to interface the FBIS with the MP-related Beam Switch-Off Actuation Systems as directly as possible. Especially, we would like to avoid additional systems between the FBIS and the MP-related Beam Switch-Off Actuation Systems that could introduce additional latency.

Now, the MP-related Beam Switch-Off Actuation Systems feature only a single interface for Machine Protection. So, we have to find a solution to grant both Normal and Fast Protection Functions access to the MP-related Beam Switch-Off Actuation Systems. There are two basic solutions to this problem:

1. We add an extra MP-related Beam Switch-Off Actuation System Control Box inside the BIS that duplicates the single MP-interface of the MP-related Beam Switch-Off Actuation Systems.
2. The FBIS takes direct control over the MP-related Beam Switch-Off Actuation Systems and is implemented such as to allow the other parts of the BIS dealing with Normal Protection Functions access to the MP-related Beam Switch-Off Actuation Systems.

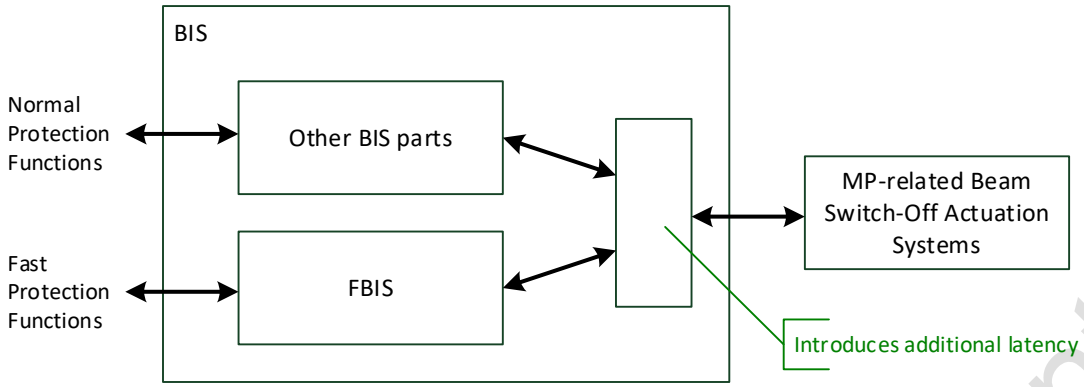

Figure 3: Introduction of additional latency due to an additional MP-related Beam Switch-Off Actuation System control box inside the BIS has to be avoided.

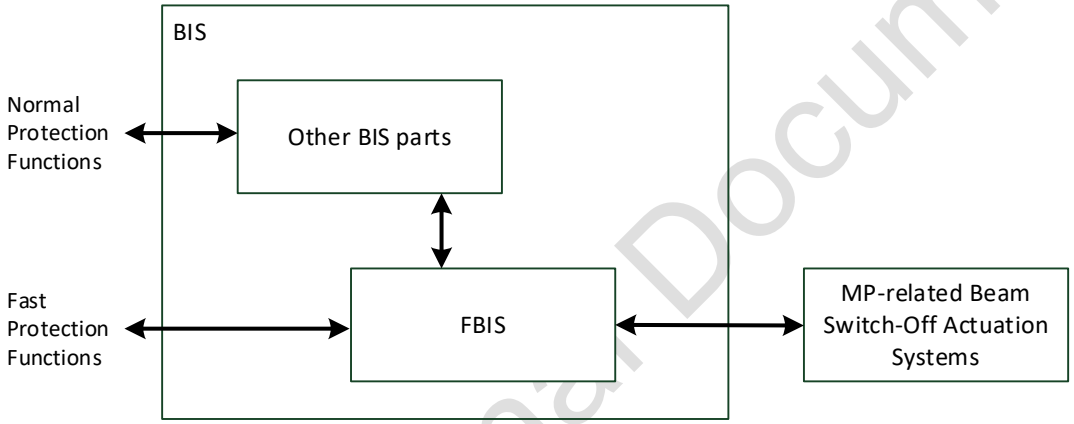

Figure 4: MP-related Beam Switch-Off Actuation Systems under direct control of the FBIS to minimize Fast Protection Function reaction time.

Option 1 clearly introduces additional latency, which has to be avoided.

Option 2 has more potential in minimizing Fast Protection Function reaction times. Hence, the FBIS has to provide control access to the MP-related Beam Switch-Off Actuation Systems to other parts of the BIS.

2.1.2.2 Avoid Cascading

Typical accelerator facility interlock systems are often built-up as a tree (Figure 5). The inputs that need to be processed by the complete interlock system are first connected to a larger number of logic boards with a limited amount of inputs. Those logic boards aggregate the inputs following some logic rules and generate an output. Those outputs are then fed to a next layer of logic boards and so on, until a final logic board, controlling the actuators, is reached.

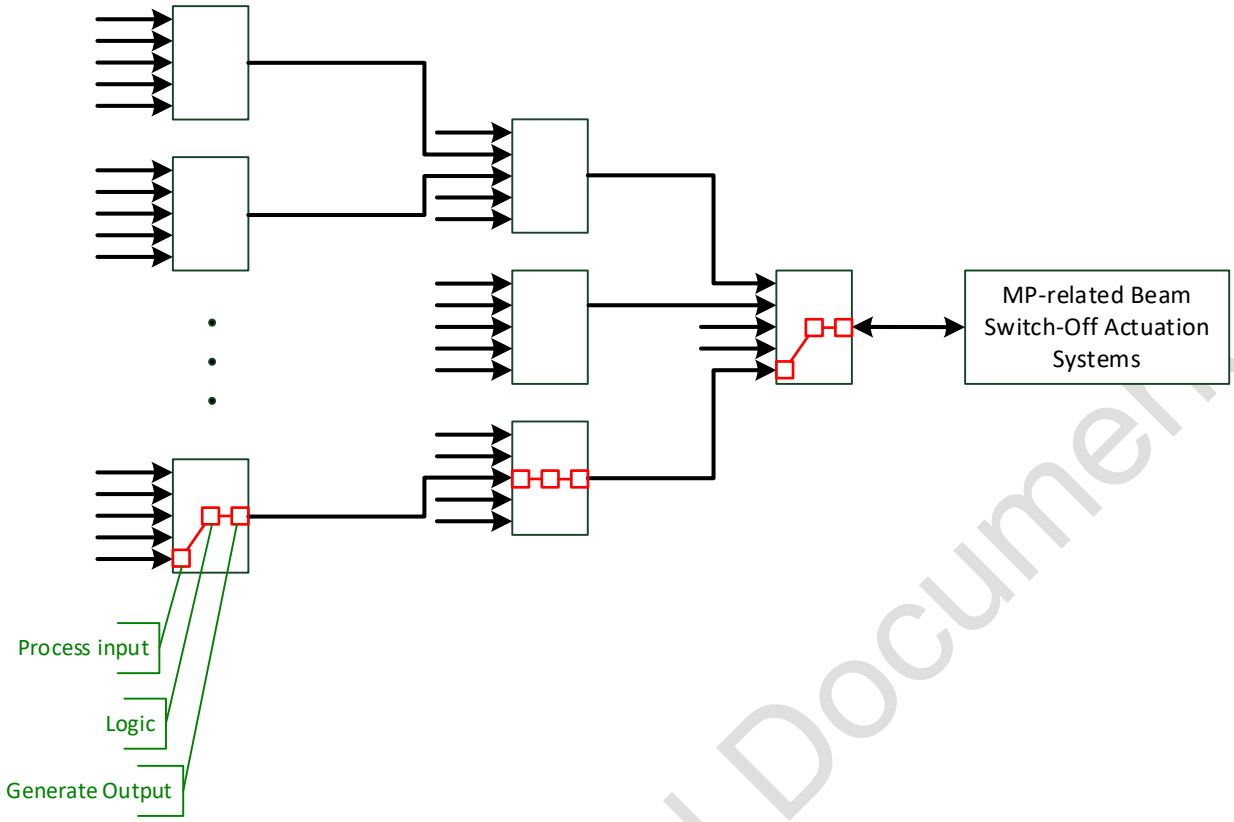

Figure 5: Typical accelerator facility Interlock System Tree Structure. Additional latency is introduced in each layer.

The caveat of this architecture is obvious: additional latency is added in each layer. Such an architecture can only be time efficient if the number of layers is minimized. This again means, that the number of inputs processed in a single logic board has to be maximized.

Maximizing the inputs processed on a logic board means two things:

1. Implement the boards with a high input count.
2. Make sure the inputs of each board are efficiently used.

While the first point is obvious, the second point is illustrated in Figure 6. If the FBIS design relies on remote input panels, featuring a specific number of inputs and that are directly connected to the logic boards, then, signals that are not used on the input panels will result in unused inputs. This should be avoided.

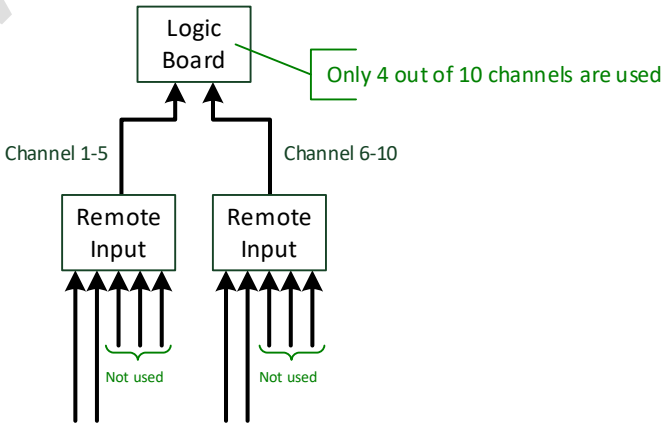

Figure 6: Inefficient use of inputs due to fixed point-to-point cabling.

2.1.2.3 Architectural Design Constraints Summary

DC-1 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.
DC-2 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.
DC-3 Arrange connection of signals to the FBIS such as to avoid unused inputs.

2.2 Maximize Availability

2.2.1 Rationale

The availability requirements for ESS are very high. Machine Protection supports this requirement by taking over the job to prevent and mitigate damage to the machine as well as unwanted activation of the machine. What we want is to avoid downtime because something has been damaged and needs to be fixed. And, if repair is necessary, then downtime should not be increased because of unanticipated activation.

The FBIS is involved in Fast Protection Functions: those are typically the ones that act on hazards that could cause severe damage in a very short amount of time. Producing beam without a fully operational FBIS, which would mean without all of the Fast Protection Functions in a working state, would mean taking a very high risk. This then puts very high availability requirements on the FBIS: the reliability of the FBIS parts has to be high and the Mean-Time-To-Restoration has to be minimized.

2.2.2 Architectural Design Constraints

2.2.2.1 Prefer Modular Approach with High Diagnostic Coverage and Easy Replacement

The Mean-Time-To-Restoration can be effectively reduced through a modular system design. If a system is composed of a set of well-defined Line-Replaceable-Units (LRU), each of them featuring well designed built-in-tests (providing diagnostic coverage), failures can be quickly located and the system can be restored to a working state, simply by replacing the faulty LRU.

For this to work, failure analysis and localization have to be easy, spare LRU's have to be available, the replacement procedure of the LRU's has to be simple, and personnel qualified to do the replacement needs to be there on time.

Simple replacement especially poses constraints on the external connections to interlock systems. Replacement must not involve disconnecting and reconnecting a large number of connectors, as this could turn out to be very time consuming and bear a high risk for ending up with faulty connections.

Those constraints also rule out so called "pizza-box" designs, i.e. custom made single-box systems. Indeed, once optimized for availability, "pizza-box" designs will in general exhibit more or less the same features as readily available modular systems as MTCA.

2.2.2.2 Operation in "Degraded Mode"

The goals of high protection integrity can obviously conflict with the requirement on high availability. The FBIS shall be flexible in the sense that it allows proton beam production although certain parts of the system (either of the FBIS itself or other systems) are not operational. It is clear that the decision to produce proton beam in such a situation needs to be explicitly taken and a proper risk analysis done as the protection integrity is going to be lowered.

2.2.2.3 Architectural Design Constraints Summary

DC-4 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.
DC-5 The FBIS should allow easy failure localization and feature sufficient built-in testing functions for this.

DC-6 The FBIS should be based as much as possible on standard ESS Controls equipment to simplify spare-parts management and maintenance procedures.

DC-7 The FBIS should allow disabling selected parts under controlled circumstances (degraded mode).

2.3 Support PIL2 Protection Functions

2.3.1 Rationale

Even though the ESS hazard and risk analysis has not yet been completed, and even though Overall Protection Functions requiring stronger risk reduction might be needed, we believe that Protection Integrity Level 2 will be the highest achievable in the context of the ESS project. Aiming at satisfying IEC61508 SIL3 requirements is not realistic in the context of the whole ESS project setup. Thus, the FBIS will have to suffice PIL 2 requirements. Any requirement for a PIL3 Protection Function will need to be redefined into a requirement for more than one PIL2 and/or PIL1 Protection Function.

2.3.2 Architectural Design Constraints

2.3.2.1 Safe Failure Fraction and Hardware Fault Tolerance

A thorough analysis of the IEC61508 requirements still needs to be made and results will enter the FBIS System Requirements Specification. However, for the purpose of this document, we can already state the architectural constraints for the FBIS components following Table 3 of IEC61508-2:2010. The FBIS needs to comply with the requirements applying to SIL 2.

It is expected that the FBIS will request a beam switch-off more often than once a year. Following the IEC61508 definitions the FBIS is therefore considered to implement protection functions with “high-demand mode”.

Note that besides the requirements in Hardware fault tolerance, Safe failure fraction and Reliability IEC61508 states additional requirements about the systematic capability of a safety/protection system.

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

Figure 7: Table 3 from IEC 61508-2:2010, specifying the minimal hardware fault tolerance and safe failure fraction of a single element for being useable in safety functions of different SIL’s.

2.3.2.2 Architectural Design Constraints Summary

DC-8 Design the FBIS components such as to keep the option to achieve a Hardware Fault Tolerance of 1 or higher.

DC-9 Built-in test functionality must be extended with a fail-safe failure reaction mechanism to increase the safe failure fraction.

2.4 Scalable with respect to Number of Inputs

2.4.1 Rationale

ESS is a research facility. We do not expect the list of Protection Functions that is being specified now neither to be complete nor to be static. Changes have to be expected.

While the FBIS logic will be flexible enough to accommodate for functional change requests, adding additional Protection Functions or input signals to the FBIS will only be possible if the physical design is scalable. It should be possible to add inputs to the FBIS without having to compromise too much on the overall FBIS performance and without having to add a substantial amount of hardware.

2.4.2 Architectural Design Constraints

We believe that no additional constraints are introduced by this requirement. If the FBIS is designed in a modular way and such as to avoid deep tree structures, i.e. according to 2.1.2.2, input scalability will result.

2.5 Support staged Commissioning of ESS

2.5.1 Rationale

We expect that the ESS accelerator will be built and commissioned step-by-step, e.g. by adding accelerator segment after segment. Commissioning a segment with beam will require the Fast Protection Functions that are necessary for that segment to be operational. Hence those sections of the FBIS needed for those functions also need to be commissioned beforehand and have to be operational. Once an FBIS section has been tested and verified, changes should only be applied if really necessary.

2.5.2 Architectural Design Constraints

2.5.2.1 FBIS Segmentation

The FBIS architecture should support segmentation. Figure 8 illustrates the concept. In a first step, the FBIS will implement the control of the MP-related Beam Switch-Off Actuation Systems and only the Interlock Logic specific to segment 1 of the accelerator. When segment 2 gets added the accelerator, the FBIS is extended to implement the Interlock Logic specific to segment 2, and so on. In our view, a segment is defined by all accelerator parts needed to produce beam up to a specific beam destination.

We do not know at this point, if such a segmentation is feasible in a strict way, i.e. such that all segments are completely independent. But even if there is some overlap, we expect a high gain from not having to rebuild the FBIS after each step of the accelerator build-up.

2.5.2.2 Architectural Design Constraints Summary

DC-10 The FBIS architecture should support the concept of segments and be scalable in terms of segments.

DC-11 Signals related to Protection Functions dedicated to one accelerator segment should be connected to the corresponding FBIS segment.

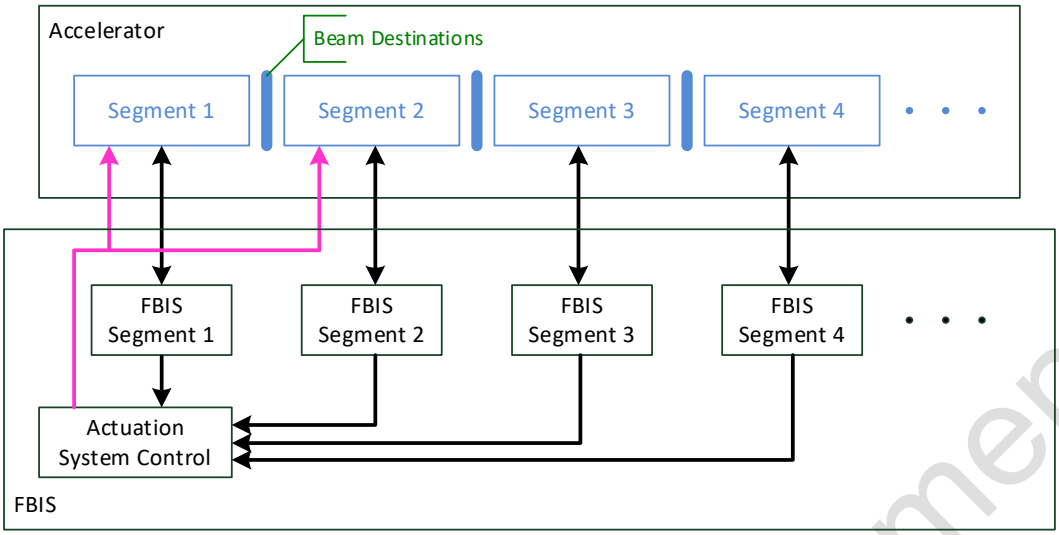

Figure 8: Segmentation and incremental build-up of the accelerator and the FBIS.

2.6 Support ESS Lifetime requirements

2.6.1 Rationale

ESS is supposed to have lifetime longer than 20 years. In such a time, electronics components tend to get obsolete, even if carefully selected. While hardware ageing and components obsolescence might force us to replace the FBIS hardware, the basic function of the FBIS is likely to stay the same over the lifetime of ESS. A change of hardware components should be feasible without having to completely redevelop the FBIS functionality.

2.6.2 Architectural Design Constraints

2.6.2.1 Abstraction from Hardware

The function of the FBIS will largely be defined in firmware. If we want to be able to replace the hardware, e.g. change the type of FPGA, the firmware defining the FBIS function has to be abstracted away from the hardware it runs on and must not contain any FPGA specific details. In case of a hardware change, only the abstraction layer will need to be re-implemented and possibly only the integration between the FBIS firmware and the abstraction layer will need to be tested. The FBIS function implementation will not need changes and can be reused as is.

On classical embedded and processor based systems, this is for example achieved by means of a board support package that contains the hardware-dependent part of the software needed to run the system and that “hides” hardware details away from the user.

2.6.2.2 Architectural Design Constraints Summary

DC-12 The firmware defining the FBIS function should not have direct dependencies to the hardware it runs on.

2.7 Seamless Integration into ESS Control System Landscape

2.7.1 Rationale

This requirement can be interpreted as a consequence from the requirement to maximize availability (see 2.2). If the FBIS integrates seamlessly into the ESS Control System Landscape, i.e. is based on standard ESS Controls equipment, spare-parts management and maintenance will be hugely simplified.

2.7.2 Architectural Design Constraints

We believe that no additional constraints are introduced by this requirement. Integration with e.g. EPICS or the ESS Timing System are already required and a constraint to use standard ESS Controls equipment has been deduced in section 2.2).

3 FBIS Architectural Design Options

The following sections collects the architectural design options that have been considered so far for the FBIS.

The section is structured according to the set of architectural elements defined in Figure 9 and in Table 1.

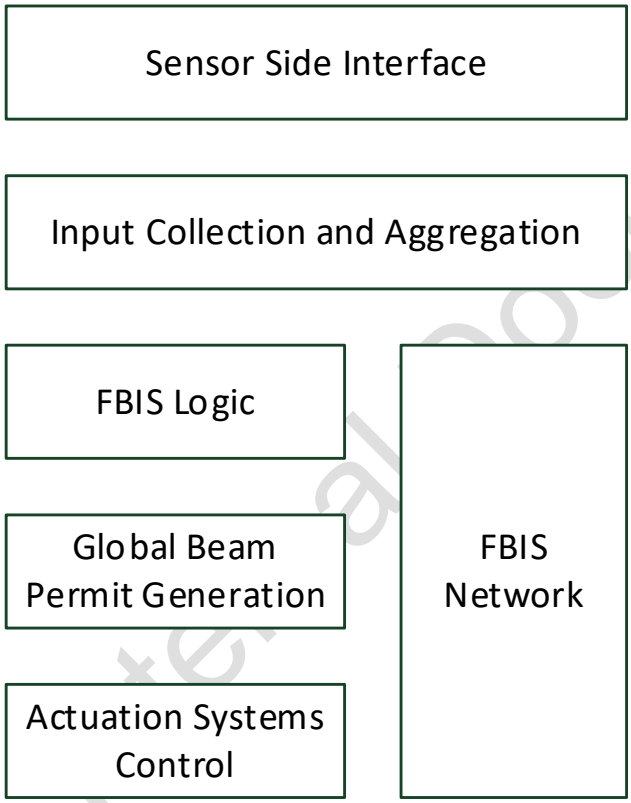

Figure 9: Architectural elements of the FBIS.

Architectural Element	Role
Sensor Side Interface	Provide an interface for sensor-side data. We consider two types of data: • Discrete interlock signals of OK/NOK type. • Continuous data-stream for the redundant transmission of OK/NOK information as well as configuration, status and health information.
Input Collection and Aggregation	Collect the discrete signals and data links from sensor system, route them to the FBIS logic, and aggregate for an optimal use of Logic input channels.
FBIS Logic	Process all connected input data and take a decision with respect to

	Beam Permit, based on that data.
Global Beam Permit Generation	Combine the results of all FBIS Logic Elements into a Global Beam Permit and route this information to the Actuation Control Systems.
Actuation Systems Control	Control the MP-related Beam Switch-Off Actuations Systems according to the Global Beam Permit.
FBIS Network	Interconnect all FBIS elements for redundancy and for diagnostic purposes.

Table 1: Architectural elements of the FBIS.

3.1 Sensor Side Interface

We have to transfer two types of data from the MP-related Sensor Systems to the FBIS: discrete OK/NOK information and a data-stream for redundancy, mode checking and diagnostic purposes. This can be solved either by (a) implementing two distinct interfaces, one for the OK/NOK type and one for the data stream (Figure 10), or by (b) using one single high-speed serial link the transfer of both data types over the same link Figure 11).

The driving requirement for this part is speed: OK/NOK information has to be transferred with as little latency as possible from the MP-related Sensor System to the FBIS. This means that option (b) to transfer the OK/NOK information over the data-link is only viable if this does not introduce too much latency, i.e. if the link is “fast” enough.

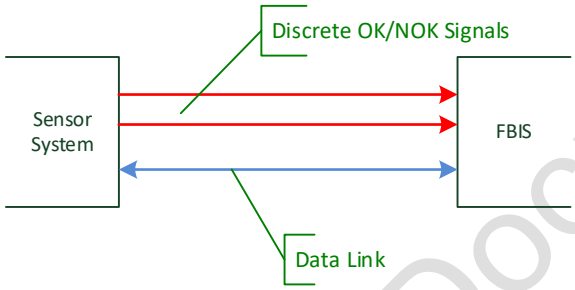

Figure 10: Interface with two distinct physical connection types: a discrete link for OK/NOK transmission and a communication link for data transmission.

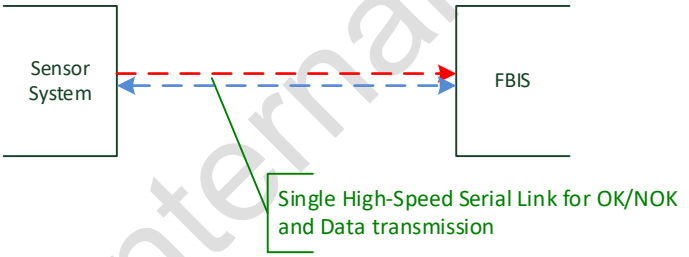

Figure 11: Interface featuring a single high-speed serial link for the transfer of both OK/NOK and data.

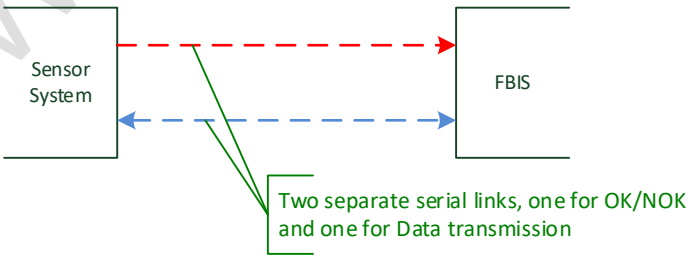

Figure 12: Interface featuring two separate serial links, one for OK/NOK transmission, one for data transmission.

The following sections contain options for implementing both discrete OK/NOK and data-links in the context of option (a) (Figure 10).

3.1.1 Discrete Interlock Interface

The discrete interlock interface is used to transmit the BEAM-PERMIT OK or NOK state from the MP-related Sensor System to the FBIS with minimal latency. In addition, the interface has to be done such as to allow explicit detection of link faults, like connection loss, short circuit, etc. and should fail safe to the NOK state.

We are considering two types of interface implementations right now: 3-wire current loops and 2-wire differential RS-422 with error detection.

3.1.1.1 3-Wire Current Loop Interface

Principle of operation: this interface signals both the OK and the NOK state with a dedicated current loop. To be in a valid state, one and only one of the current loops must be active (carry current) at a time. Both or none of them being active is interpreted as an error state. The FBIS firmware must correctly interpret the error state and translate it to a NOK.

Concrete implementation proposals: this is in principle the interface used at PSI. We currently have a preliminary schematic for a newer version of this interface developed at PSI.

Pro		Con	
P1	Proven in use at PSI	C1	No off-the-shelf components that directly implement this in an integrated circuit → need to design this with discrete components
P2	Short-circuits can be detected continuously on input side only	C2	Fault detection on input side only
P3	Disconnected/interrupted links can be detected continuously on input side only	C3	Only point-to-point signal transmission
P4	Compatible with electromechanical switches (if needed in “fast” protection functions), more generally, output side can be “passive”	C4	Custom probe needed for measurement
P5	State of current loops can be read continuously (it’s analog)	C5	Needs 3 wires for signal transmission
P6	Current-loop state can easily be measured without disconnecting the signal with a custom probe	C6	Custom equipment needed to generate tests
P7	Robust against EMI (proven in use at PSI)	C7	Cable type has influence on latency
P8	Does not need common ground	C8	Need to consider ESD issues at inputs and outputs
P9	Fast: to be confirmed	C9	If opto-couplers are used: degeneration of opto-couplers “Arbeitspunktverschiebung” may lead to faulty signal detection
P10	Resistance in transmission line has no influence		

3.1.1.2 2-Wire Differential RS-422 with Error Detection

Principle of operation: this solution uses RS422 or RS485 driver/receiver chips with built-in fault detection used to output a constant High or constant Low signal. High is interpreted as OK, Low as NOK. The chips feature an extra pin indicating link failures. That extra pin needs to be evaluated by the FBIS firmware.

Concrete implementation proposals: this is the way the CERN LHC BIS transports BEAM-PERMIT information internally.

Pro		Con	
P11	Proven in use at CERN	C10	Electromechanical switches not supported on output side, more
P12	Short-circuits can be detected		

continuously on input and output side (to be confirmed) P13 Disconnected/interrupted links can be detected continuously on input and output side (to be confirmed) P14 State of signal can be read continuously (no serial protocol but used in a continuous way) P15 Off-the-shelf integrated circuits for RS-422 available → obsolescence management P16 Standardized protocol and signal levels (if used in a standard way) P17 One “sender”, multiple “reader” support P18 Robust against EMI (proven in use technology) P19 Does not need common ground P20 Fast: TTL to RS-422 through short cable to RS-422 to TTL needs about 20 ns P21 2 wires are enough for signal transmission → off-the-shelf standard twisted pair cables can be used	generally, both sides must be “active” C11 Error detection needs additional circuitry (for the fastest available chips without integrated error detection) C12 Custom error detection is based on non-standard voltage levels (to be confirmed) C13 To be clarified: Reliability of fault-detection? C14 Can only handle a small common-mode range (-7 .. +12 V) C15 Resistance of cables/connectors might cause voltage drop C16 Cable type and length have an influence on latency C17 Connection to off-the-shelf test equipment might be simpler (to be confirmed)

3.1.1.3 Optical Transmission with Correlator

Principle of operation: On sender side two orthogonal bit-patterns are generated. One pattern to code the OK-state, the other to code the NOK-state. This could for example be done with 31 bits per pattern. The bit pattern is transmitted via an optical fiber (preferably glass) to the receiver which checks for a correlation with the bit-patterns and thus detects OK, NOK and error states. If the transmission uses a 100 Mbit link, the time needed to transmit an NOK is 310ns

Pro	**Con**
P22 Robust against EMI P23 Does not need common ground P24 Fast sender/receiver are available P25 Large cable bandwidth P26 Probability of false signal transmission P27 Light via fiber is slightly faster than electrons via a “cooper cable”	C18 Needs intelligence at outputs and inputs C19 Fiber is more expensive than cooper cable, might be more difficult to handle C20 Electromechanical switches not supported on output side, more generally, both sides must be “active” C21 Error detection needs only possible after reception of a complete “sequence” C22 Length of “sequence” has influence on latency C23 Fiber might degenerate with time or “blur” due to radiation.

3.1.2 Data Link Interface

The data link is used to transfer mode information for mode consistency checks, status and diagnostic data for plausibility and health checks as well as BEAM-PERMIT information for redundancy. The data is transferred from the MP-related Sensor System to the FBIS.

A communication from the FBIS to the MP-related sensor systems might be of interest for handshaking or enforced mode information transmission, but we have not seen such a feature being required by any of the use-cases we analyzed up to now.

We are considering two types of interfaces right now: Ethernet and RS-422.

3.1.2.1 Ethernet

Data is transferred by means of standard 100 Mbit Ethernet.

Pro	Con
P28 Standard off-the-shelf equipment for testing, diagnostics P29 Compatible with standard off-the-shelf networking equipment and cabling P30 Can be “switched” with off-the-shelf components P31 Standardized protocols are supported (UDP, TCP, …), EtherCAT (to be confirmed) P32 Compatible with PLC Systems P33 Robust versus EMI (proven in use technology) P34 Longer cable length support (to be confirmed)	C24 Needs high pin-count, not only Rx/Tx pairs; 8 pins RMII C25 Ethernet stack needed on FPGA side

1.3.1.1 RS-422

We use a transmit-only RS-422 serial connection to transfer the data.

Pro	Con
P35 RS-485 supports multiple sender over same line P36 Simple to generate data from FPGA (does not need “stack”) P37 Compatible with PLC Systems P38 Minimal pin count for Rx/Tx P39 Robust versus EMI (proven in use technology)	C26 RS-422 supports only one sender C27 Not clear whether “switching” off-the-shelf components are available C28 Transmission speed limitations (to be confirmed), dependent on cable length

Note: via this link, different serial protocols could be used:

- The standard RS-422 protocol
- SPI Protocol with ECC protection (as implemented by IOxOS)

3.1.3 High-Speed Serial Link for Data and Interlocks

If the data-link is fast enough, the OK/NOK information could be transferred over that link (Figure 11) without suffering too much latency.

Pro		Con	
P40	Only one link needed for all	C29	Short-circuits cannot be detected continuously
P41	Off-the-shelf solutions for high-speed serial links are available, including SFP based stuff.	C30	Disconnected/interrupted links cannot be detected continuously
P42	Transfer medium can be selected to be copper or optical fibers	C31	State of signal cannot be read continuously
P43	Long cable support	C32	OK/NOK transmission suffers from latency due to packetized transfer → might be slower than discrete solutions
P44	OK/NOK link faults detectable at data packet level	C33	Only point-to-point support
P45	Support for high-speed serial (SERDES) built-in on FPGA	C34	Rocket-IO pins from FPGA needed for using built-in FPGA high-speed serial link capabilities (Aurora)
P46	Networking and Telecom standard interfaces	C35	Higher complexity compared to RS-422 or current loops
P47	Robust versus RMI (proven in use technology)	C36	Packet transfer rate depends on packet size
P48	No ground related problems in case of optical transfer (electrical to be confirmed)	C37	Solution not “established”
P49	Number of OK/NOK signals scalable	C38	Data packet transmission might block OK/NOK transmission
		C39	Lost redundant transmission of OK/NOK (everything goes over one single link)

3.1.4 Separate serial links for OK/NOK and for data transmission

Similar to 3.1.3 but:

Pro		Con	
P50	OK/NOK data packets not delayed by data transmission	C40	Needs two fibers
P51	Packet transfer rate for OK/NOK transmission is not dependent on data transfer		
P52	Redundant transmission of OK/NOK over two links		

3.1.5 Interface Integration into Sensor Systems

3.1.5.1 Interface Integration into IOxOS IFC14x0 based Sensor Systems

Multiple options exist to integrate the FBIS interface into IOxOS IFC14x0 based Sensor Systems.

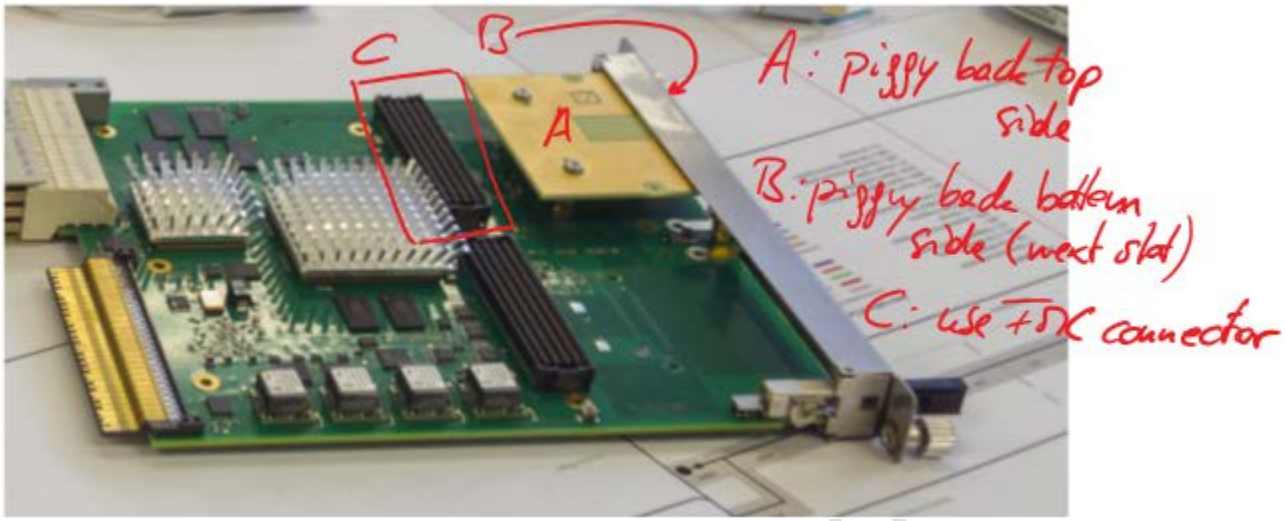

Figure 13: FBIS Interface integration options for IFC14x0.

3.1.5.1.1 FBIS Connection Piggy-Back Component Side

Ioxos has prepared a 24-pin connector on both sides of the AMC PCB for the connection of an FBIS Interface piggy-back module (Figure 13, A). With this solution, the data-link speed is limited and OK/NOK information has to be transferred through dedicated signals.

Pro	Con
P53 Same piggy-back can be used on both sides (top and bottom) P54 No additional mTCA slot is blocked	C41 FMC slot is blocked

3.1.5.1.2 FBIS Connection Piggy-Back Back Side

Figure 13, option B would be to attach the piggy-back to the rear side of the AMC. This would require a free neighboring slot.

Pro	Con
P55 Same piggy-back can be used on both sides (top and bottom) P56 FMC slot is not blocked	C42 mTCA slot is blocked

3.1.5.1.3 FBIS Interface FMC

Figure 13, option C highlights the FMC connector that could be used to mount an FBIS Interface FMC module. The FMC connector features high-speed links to the FPGA, which would allow transferring both data types (OK/NOK and DATA) over one single high-speed link (Figure 11) to the FBIS.

Pro	Con
P57 More pins available than with piggy-back P58 Could be used to implement more “sophisticated” interfaces	C43 Requires a free FMC slot

3.1.5.1.4 FBIS Interface on customized µRTM

A last option would be to develop a custom made µRTM featuring the interface to the FBIS. As we have high-speed links optionally going from the AMC to the µRTM, we could transfer both data types (OK/NOK and DATA) over one single high-speed link (Figure 11) to the FBIS.

Pro	Con
P59 No free FMC slot is required P60 No free mTCA slot is required	C44 Interface circuit needs to be added to RTM C45 Existing RTMs would need to be modified

3.1.5.2 Interface Integration into Struck SIS8300/SIS8900 based Sensor Systems

Beam Instrumentation will use the Struck SIS8300/SIS8900 for ACCT data readout and processing. MP-related checks that are part of Fast Protection Functions will be performed on the Struck board, hence we have to interface the Struck boards with the FBIS.

3.1.5.2.1 Front-Panel Connection

Figure 14 shows the front panel of the SIS8300. There are 2 LVDS outputs free on the marked connector. We could use one as OK/NOK and one to drive a serial data communication line. This option requires an additional external interface box to convert LVDS to the FBIS interface format.

Figure 14: Use 2 free LVDS pairs on front-panel connector for «alarm» and «serial data».

Pro	Con
P61 Signals are easily accessible	C46 Might need to split signal from one and the same connector (some are used for FBIS, others are used for other purposes) C47 Low number of signals C48 Pre-defined direction

3.1.5.2.2 µRTM Flat-Cable Connection

Figure 15 shows the SIS8900 and we can see a 6 LVDS output and a 6 LVDS input connector on the PCB. We could attach a flat cable to the output (and potentially the input) connector and install a module in the neighboring µTCA slot with connectors to the FBIS. Electronics to convert LVDS to the FBIS interface format could be integrated into that module.

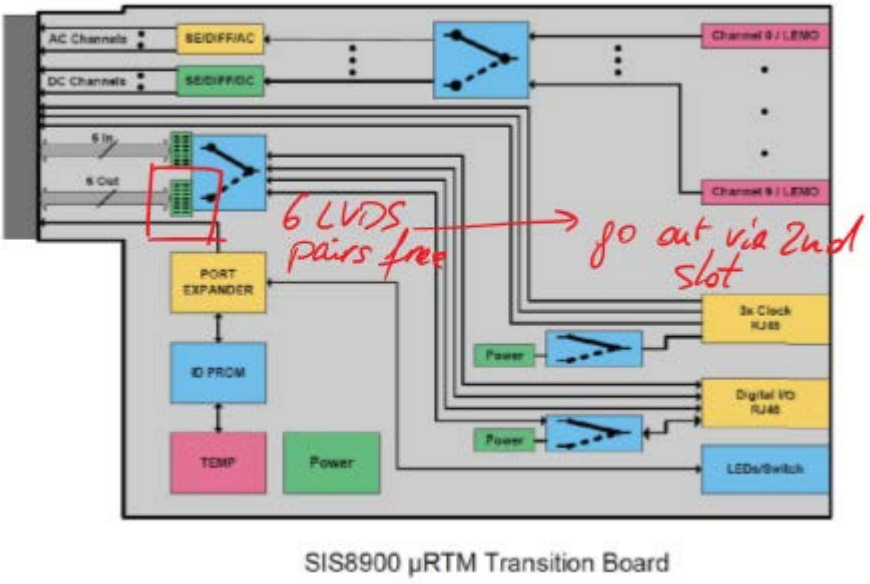

Figure 15: Connect via µRTM extension connector: plug a flat-cable to the marked connector and use the neighboring µTCA slot for an FBIS interface µRTM.

Pro	Con
P62 More signals than on front-panel P63 Direction can be selected	C49 Flat band-cable might be difficult to handle or might even block a full mTCA slot

3.1.5.2.3 µRTM RJ-45 Connection

Figure 16 again shows the SIS8900. We can see that a total of 4 LVDS in/out can be routed to an RJ45 connector of the SIS8900 panel. We could route 2 LVDS out for two OK/NOK type signals and 1 LVDS out and 1 LVDS in pair for bi-directional communication. Alternatively, 4 LVDS outputs could be routed to the RJ45 if the data-link is not being use bi-directionally.

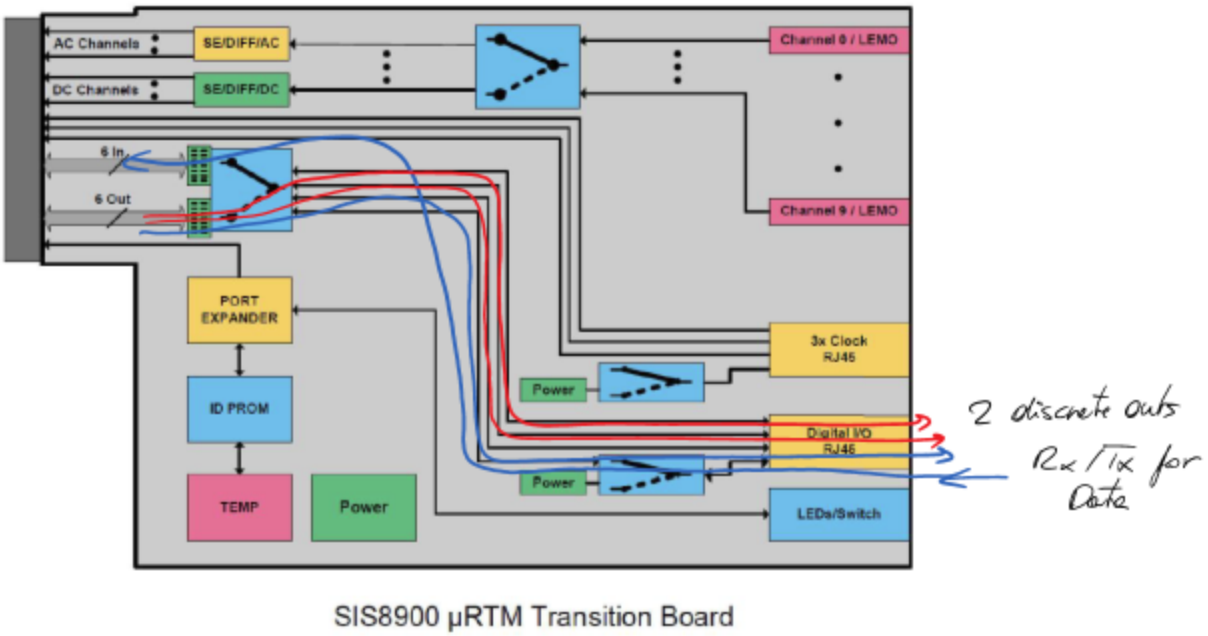

Figure 16: Route 3 LVDS outputs and 1 LVDS input to the Digital I/O RJ45 connector on the µRTM panel and use 2 LVDS out for OK/NOK type outputs and 1 LVDS out and 1 LVDS in for a bi-directional data-link.

Pro	Con
P64 More signals than on front-panel but maximal 4 P65 Direction can be selected P66 Standardized connector	C50 Maximally 4 signals

3.2 Input Collection and Aggregation

MP-related Sensor Systems are distributed along rack enclosures. We want to process as many inputs in one single FBIS Logic Board as possible. Hence the information from both discrete link and data links have to be collected, aggregated and brought to the location of the FBIS Logic Board.

This can be achieved in many different ways, each of them being a more or less aggressive or a more or less conservative variation of serialized or point-to-point connections.

For simplicity, we use the term BEAM-PERMIT to designate the discrete signals type and we use the term DATA to designate the information transferred through the data-link.

3.2.1 Fully Serialized – Single High-Speed Link

In this option (Figure 17), both BEAM-PERMIT and DATA from k Systems are serialized into a high-speed data stream to an FBIS Logic Board. The FBIS Logic Board features j high-speed serial inputs. A total of k x j inputs can be processed by one FBIS Logic Board.

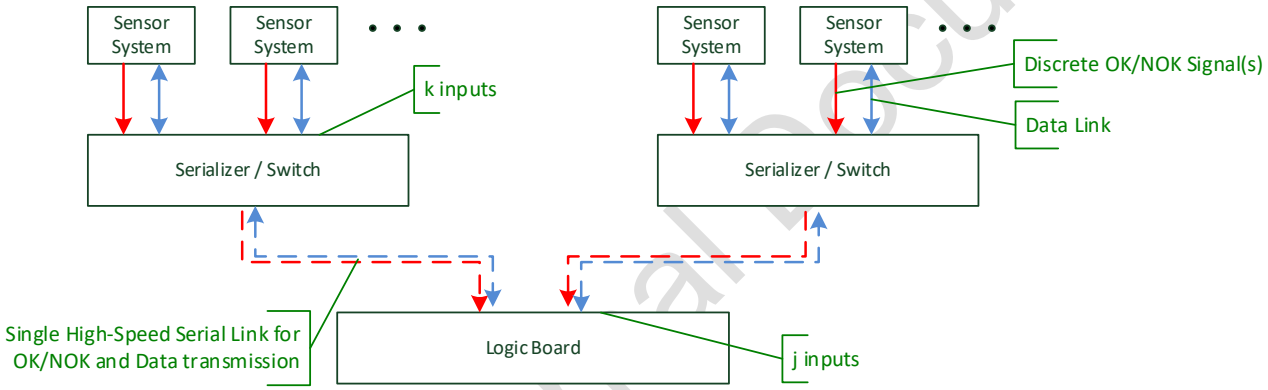

Figure 17: Fully serialized/switched, single high-speed serial link input collection.

Pro	Con
P67 Input density on FBIS Logic Board side can be high → Only one link needed for all P68 Off-the-shelf solutions for high-speed serial links are available, including SFP based stuff. P69 Transfer medium can be selected to be copper or optical fibers P70 Long cable support P71 Link faults detectable at data packet level P72 Support for high-speed serial (SERDES) built-in on FPGA if Serializer/Switch is realized with FPGA P73 Networking and Telecom standard interfaces P74 Robust versus RMI (proven in use technology) P75 No ground related problems in case of optical transfer (electrical to be	C51 Lost redundant transmission of OK/NOK (everything goes over one single link) C52 Data packet transmission introduces latency C53 Only point-to-point support (One Serializer/Switch is connected with one FBIS Logic Board, unless the HW features multiple high-speed serial links) C54 Packet transfer rate depends on packet size C55 Technology is generally not used at Research Facilities (CERN, …) C56 Number of High-Speed serial links per FBIS Logic Board depends on physical type of link and on FPGA size and type (to be confirmed)

confirmed) P76 Number of input signals scalable P77 Technology is widely used in industry + PSI Center for Proton Therapy P78 Principally multiple Serializer/Switch could be cascaded (tree structure) P79 Interface can be easily multiplied (one Serializer/Switch could provide multiple identical High-Speed links) P80 Allocation of Sensor Systems to Serializer/Switch is flexible (1 big switch, multiple small switches, …)	

3.2.2 Fully Serialized – Dual High-Speed Link

A second variation, based on the same principle, is shown in Figure 18: DATA and BEAM-PERMIT would be transferred via two different high-speed serial links to the logic board.

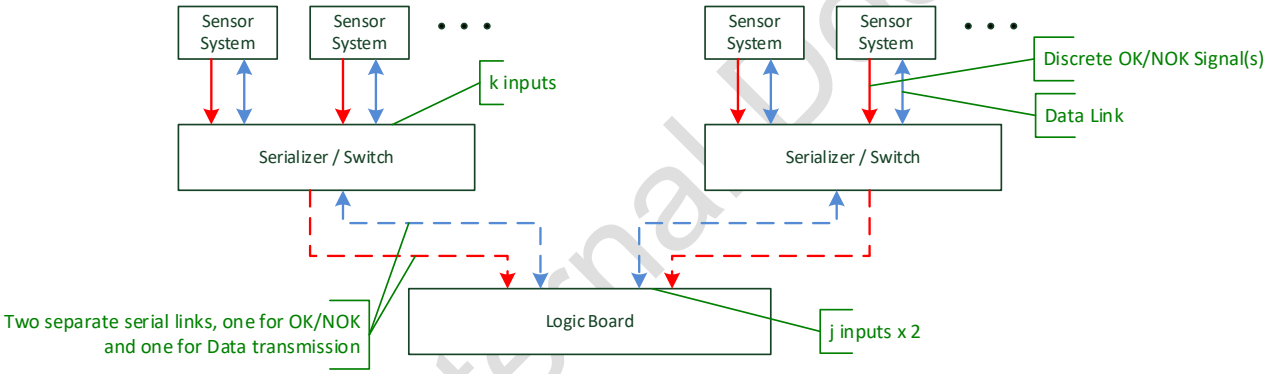

Figure 18: Fully serialized/switched, separate high-speed serial link input collection.

Same as 3.2.1 with the following exceptions:

Pro	Con
P81 Data and Discrete signals are communicated via different channels (redundancy)	C57 Increased cabling C58 Requires more High-Speed Serial Link inputs and outputs

3.2.3 Serialized Data-Link – Passive Point-to-Point Discrete

In this option (Figure 19), DATA from k systems is serialized and sent over high-speed serial links to the FBIS Logic Board. The BEAM-PERMIT signals are routed through Passive Input Panels and a Patch-Panel (Output to Input patching) in a point-to-point connection to the FBIS Logic Board.

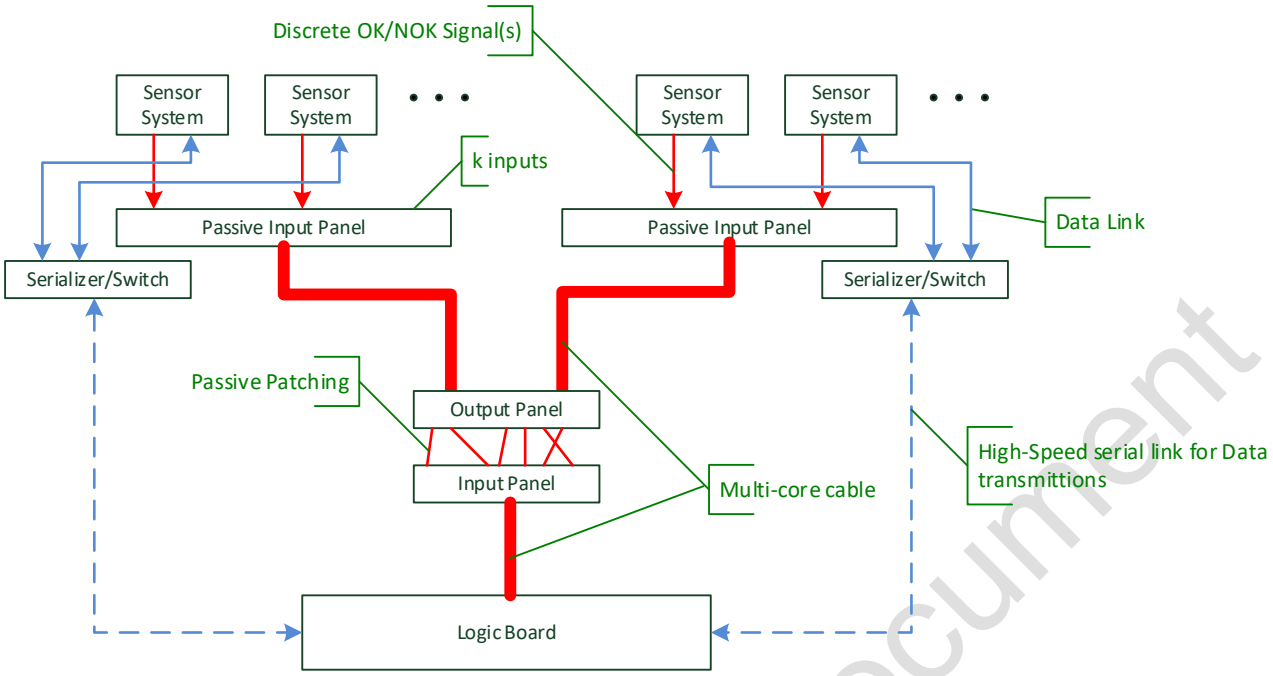

Figure 19: Serialized/switched Data-Link and point-to-point discrete link collection with passive patching.

Pro	Con
P82 Redundant transmission of OK/NOK signals P83 OK/NOK signals do not need to be serialized → fast transmission P84 OK/NOK signals does not base on “advanced technologies” such as SERDES, etc. → obsolescence management, reliability P85 This is the “traditional” technology used at Research Facilities (CERN, PSI, …) P86 Link faults of OK/NOK signals continuously detectable if interface features this	C59 Need to consider EMI protection C60 Requires many “passive” components such as multi-core cables, connectors, patch-panels, etc. C61 Not scalable with respect to the OK/NOK signals one FBIS logic board can process → as FPGA pins are limited C62 OK/NOK signals cannot easily be duplicated (depends also on type of interface) C63 FBIS logic board needs to detect faults of OK/NOK signals → might increase the number of pins needed to read one single OK/NOK signal C64 Physical space available for connectors on FBIS Logic Board is limited → may impose constraints on number of connectors and multi-core cable C65 Re-assigning OK/NOK signals involves “manual” work → e.g. re-patching of connections

3.2.4 Serialized Data-Link – Active Point-to-Point Discrete

Figure 20 shows a variation of the point-to-point discrete links, this time with active patching, i.e. with a programmable input to output "router".

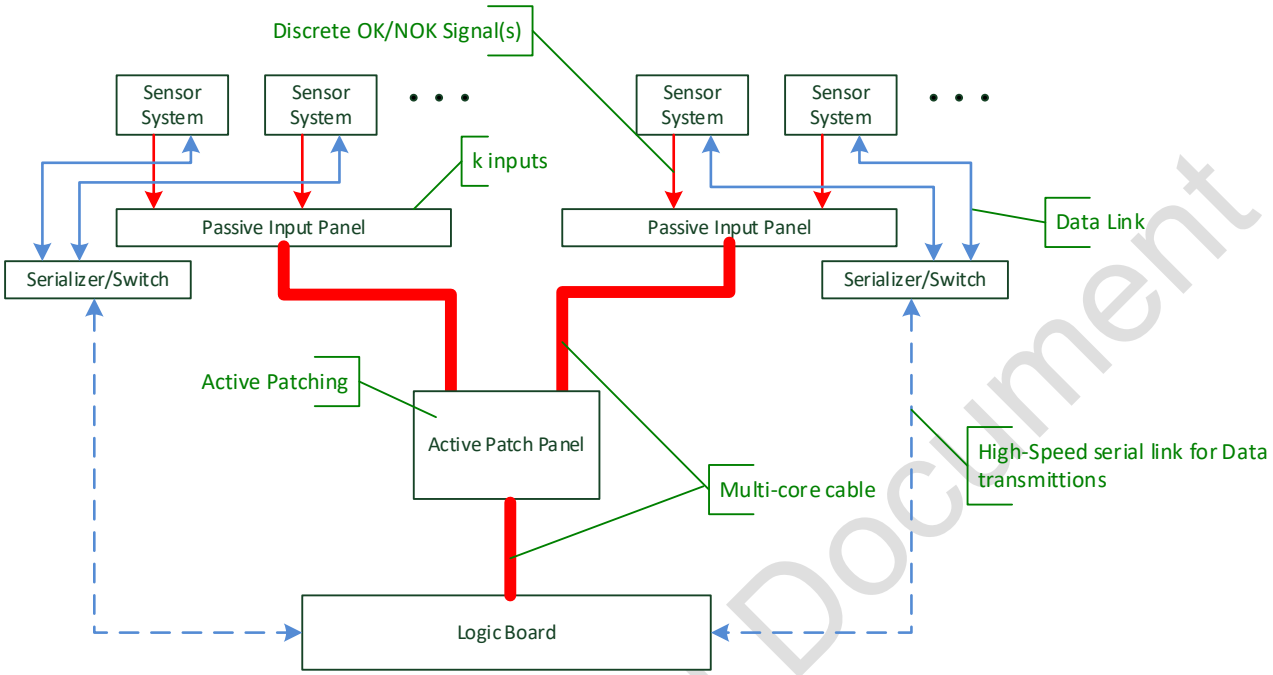

Figure 20: Serialized/switched Data-Link and point-to-point discrete link collection with active patching.

Same as 3.2.3 with the following exceptions:

Pro	Con
P87 Less "manual" work required to re-assign signals	C66 Additional complexity due to "active patching" C67 Additional overhead for configuration management, diagnostics, obsolescence management, V&V C68 Might introduce additional latency

3.2.5 Fully Serialized Hybrid with Point-to-Point Discrete Option

As shown in Figure 21, one can think of hybrid solutions, featuring for example a dual high-speed serial link for DATA and BEAM-PERMIT and an output connector for routing the BEAM PERMIT directly to a logic board or a patch-panel.

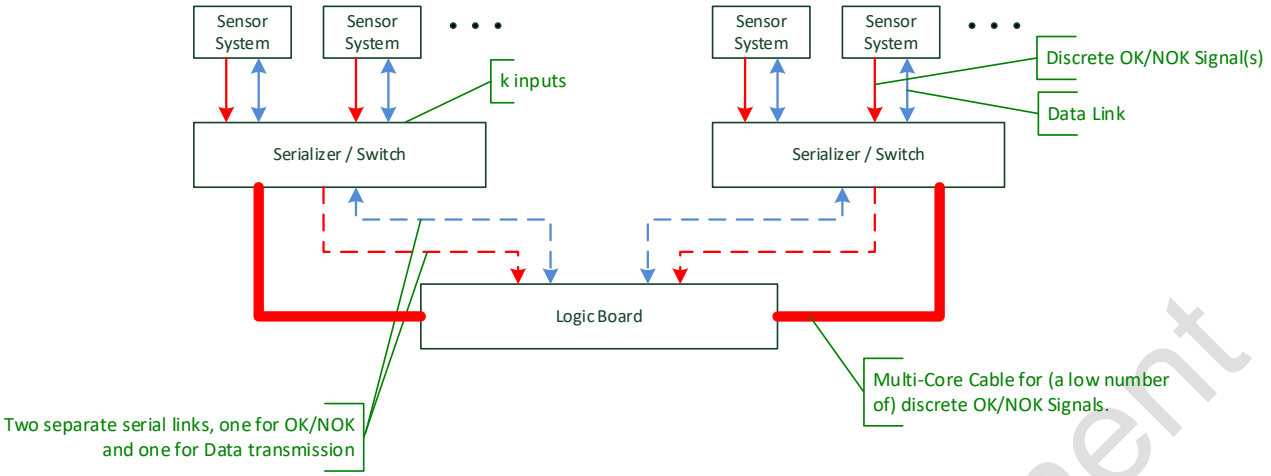

Figure 21: Hybrid serialized/switched and point-to-point input collection.

Pro	Con
P88 Very flexible. Feature can be used if necessary but is not “mandatory” P89 Certain signals (required to be very fast) could be routed discrete and not via the high-speed serial data-link → these signals would not suffer from the latency introduced by serialization/deserialization	C69 Different latencies depending on how the signal is routed → could increase FPGA firmware complexity C70 Increased cabling overhead. Overhead, depends heavily on concrete usage C71 Increase complexity as both, discrete signals and high-speed serial link is required. (Note: Unless the technology is used anyways, e.g. for the interface between Sensor Systems and Serializer/Switch) C72 Additional overhead for configuration management → need to support “different” Serializer/Switches e.g. with different FPGA Firmware

3.3 FBIS Logic

Once all the input data, both BEAM-PERMIT and DATA have been collected and properly aggregated, it needs to be processed according to the FBIS logic rules and an aggregated BEAM-PERMIT, based on the available data, has to be computed. The implementation options of the FBIS Logic Boards depend on how the input data is collected and aggregated. The following sections describe some options, without claiming to list all possible solutions.

3.3.1 Point-to-Point Discrete – On-Board 1oo2 Redundancy

Figure 22 illustrates an option where a total of 4 x 12 BEAM-PERMIT signals could be processed on a single board with 1oo2 redundancy and diagnostic testing with fail-safe failure response. Signals would be routed over a very simple µRTM over LVDS to FPGA’s on the AMC. The data links from all connected sensor systems would be serialized in an external box and fed into the logic board through a high-speed serial link. Both FPGA’s A and B would process the input data, generate an aggregated BEAM-PERMIT and communicate their respective results to a diagnostic unit. The diagnostic unit would compare the results from A and B and generate a BEAM-PERMIT NOK in case of discrepancies.

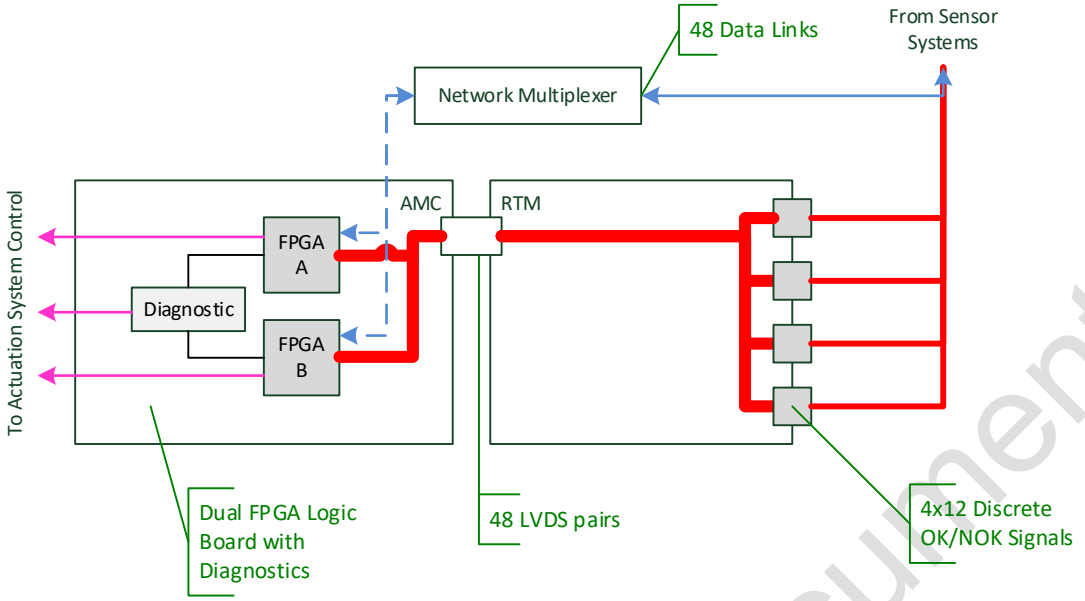

Figure 22: Processing point-to-point BEAM-PERMIT and serialized DATA on a single logic board with on-board 1oo2 redundancy and diagnostic testing with fail-safe failure response.

Pro	Con
P90 If one FPGA fails to correctly compute the decision logic or stops working, the diagnostic unit would detect that and enter the protected state P91 If one FPGA fails and the ESS expert could “isolate” this FPGA under controlled conditions, beam operation could continue in a “degraded mode” P92 One could besides of the redundant FPGA on the board also use two boards resulting in 2x2 FPGA’s	C73 Diagnostic unit might need to handle jitter-problematic C74 If both FPGA’s would share the same clock (for easier synchronization) this would be a common cause issue (Could be avoided by using independent clocks and external synchronization) C75 Generally: common cause issues C76 Redundancy is only introduced at “FGPA level” no redundancy between Sensor Systems and FPGA

3.3.2 Fully Serialized – Single-Slot 1oo2 Redundancy

Figure 23 shows an option to process serialized data in a redundant way on a single-slot system. The FPGA A on the µRTM would serialize all input channels and pass them to the FPGA B on the AMC. Both A and B would process the input data, generate an aggregated BEAM-PERMIT and communicate their respective results to a diagnostic unit. The diagnostic unit would compare the results from A and B and generate a BEAM-PERMIT NOK in case of discrepancies.

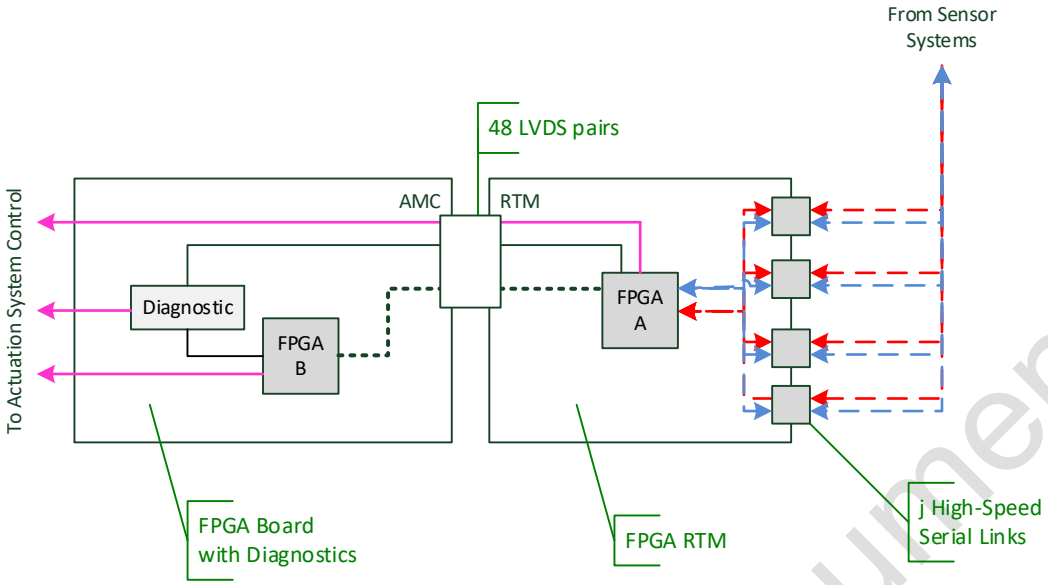

Figure 23: Processing serialized data in a single slot 1oo2 µRTM and AMC system with integrated diagnostic testing with fail-safe failure response.

Same as 3.3.1 with the following exceptions:

Pro	Con
	C77 If FPGA A fails, the correct functioning of FPGA B could be compromised as well as sensor data goes “via” FPGA A C78 uRTM receives power from AMC-card, uRTM does not have its own power supply

3.3.3 Fully Serialized – Dual Board 1oo2 Redundancy

Figure 24 illustrates a solution where the 1oo2 redundancy is implemented by two independent boards connected to the same serial data stream. Both systems would independently process the input data and generate an aggregated BEAM-PERMIT, and addition exchange their conclusion and generate a BEAM-PERMIT NOK in case of discrepancies.

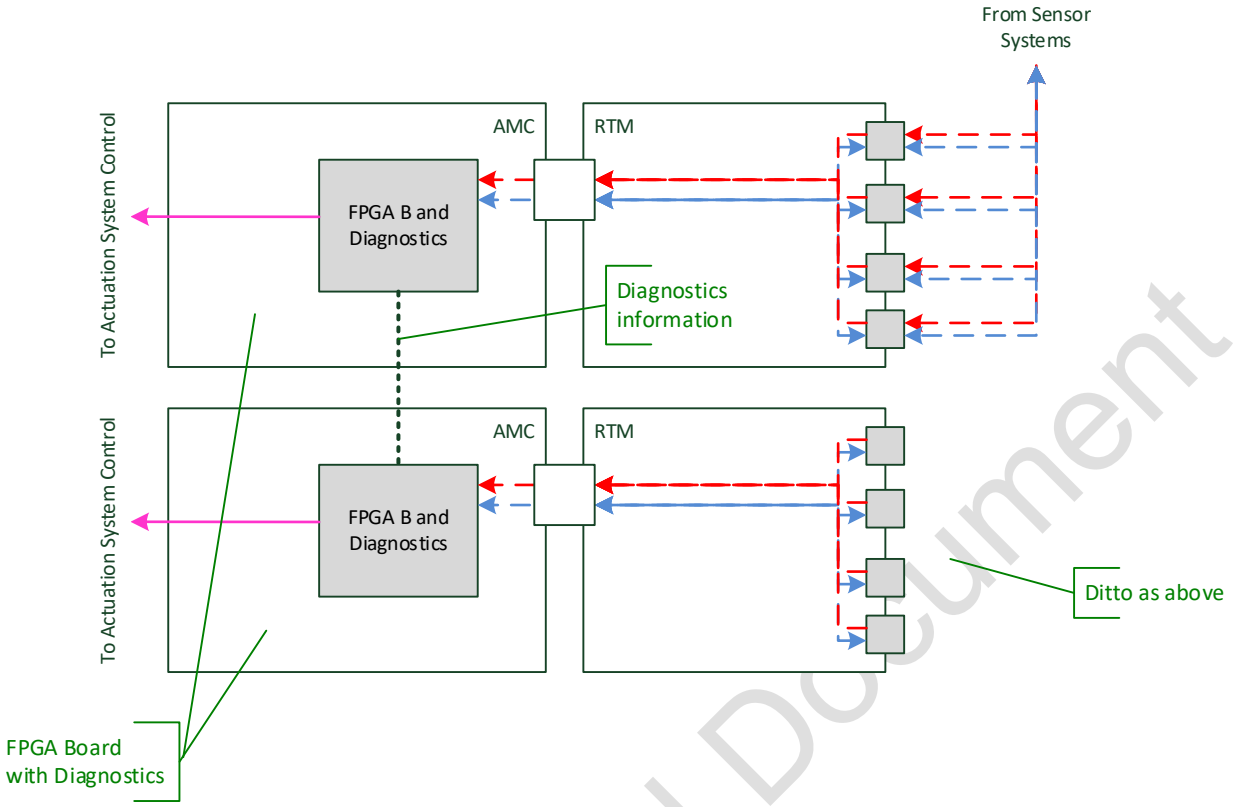

Figure 24: Input Collection Panel with redundant high-speed serial link outputs connected to two independent, single FPGA systems with result cross-checking and integrated diagnostic testing with fail-safe failure response.

Pro	Con
P93 Fully redundant pattern between "Redundant Output" and the system which receives the Beam Permits of the FBIS Logic Boards → not only HFT of FPGA is 1 but also the high-speed link, etc. P94 If one FBIS Logic Board fails to correctly compute the decision logic or stops working, the diagnostic unit would detect that and enter the protected state P95 If one FBIS Logic Board fails and the ESS expert could "isolate" this FBIS Logic Board under controlled conditions, beam operation could continue in a "degraded mode"	C79 Double number of uRTM and AMC Cards (the FBIS Logic Board) unless the existing uRTM and AMC Card of another "segment" is used or a "neighbor" Card is used

3.4 Global Beam Permit Generation

In a final step, the FBIS has to compute a Global Beam Permit that will finally be used to control the actuation systems. The following sections show a set of options to allow achieving this, again, without claiming to have found all potential solutions.

3.4.1 Optical Protection Line

In the setup shown on Figure 25, the FBIS logic boards can use an Optical Switch to interrupt an optical signal carried by one or multiple Optical Protection Lines that are connected to the Actuation Systems Control part. Presence of the optical signal will be interpreted as Global Beam Permit OK, otherwise a NOK is assumed.

Note that his option can be realized with different levels of redundancy at the level of the Optical Switch:

- n inputs to an Optical Switch, fitted with m independent optical fibers can be arranged in any redundancy pattern.
- Multiple Optical Switch elements can be introduced into the Optical Protection Line. The combined action of all Optical Switches is equivalent to a logic OR operation.

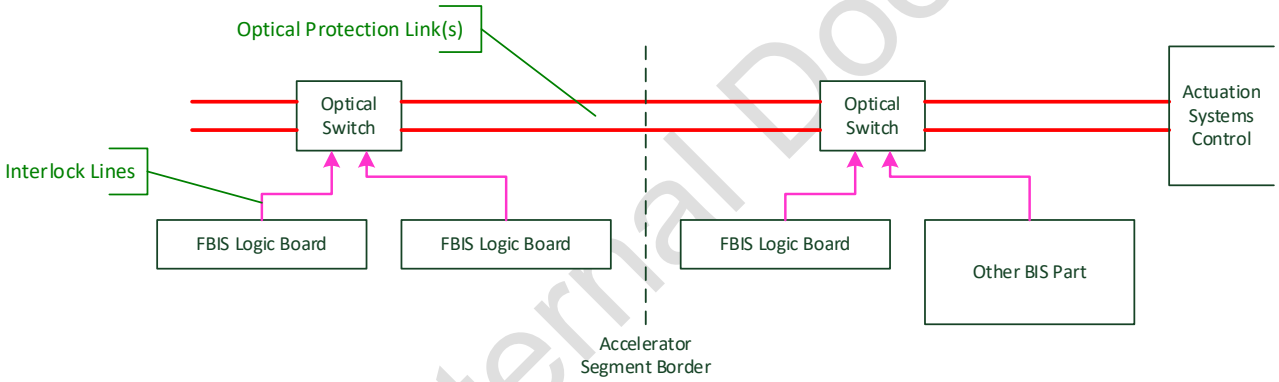

Figure 25: Data from each segment is processed by one or more segment specific FBIS Logic Boards. The generation of a Global Beam Permit is achieved through an “Optical Protection Line” that can be “interrupted” by each segment specific FBIS Logic Board or any other BIS part, causing the Actuation Systems Control to dump and inhibit beam.

Pro	Con
P96 Scalable with respect to number of nodes (node = optical switch) P97 ESD/EMV not expected to be a problem P98 No ground loops P99 Multiple optical lines could be used without a lot of overhead	C80 Every node introduces latency C81 If one node interrupts line due to a failure beam operation is stopped. Node needs to be “isolated” in order to continue beam operation C82 Opt. Switch needs to provide a feedback about its status to some kind of “intelligence” C83 Realization of opt. Switch might not be as easy as it seems (need to take care about multiple inputs, needs to logically OR the inputs, might need to provide masking feature, needs to provide diagnostic info, etc.)

3.4.2 Global Beam Permit Tree

Figure 26 illustrates the classical tree architecture. The aggregated beam-permits are connected to a centralized logic that combines them to produce a Global Beam Permit.

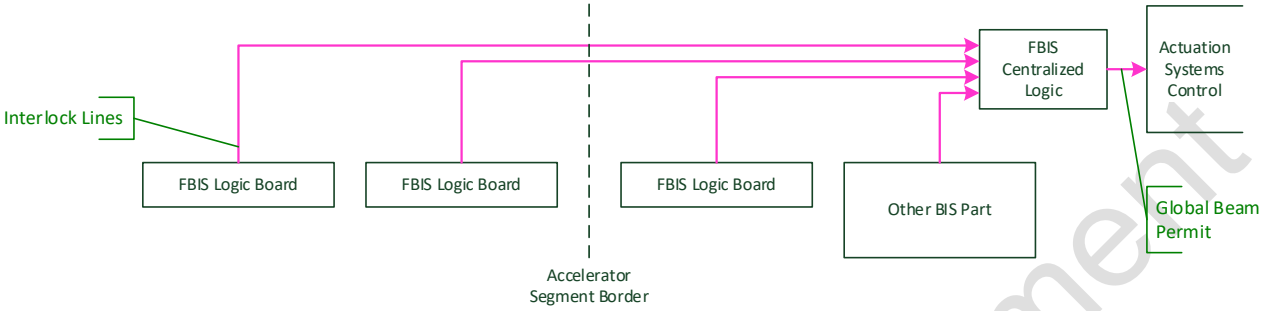

Figure 26: The Global Beam Permit is generated in a centralized logic by combining the values of all aggregated beam permits.

Pro	Con
P100 No latency introduced per additional FBIS logic board. Only latency of FBIS centralized logic	C84 There is one “FBIS centralized logic” module which has to centralize all the aggregated Beam Permits → if that one fails, big problem! C85 Multiplication of optical protection lines requires multiplication of fibers and FBIS centralized logic module

3.4.3 Fully Centralized FBIS Logic

Figure 27 proposes a fully centralized FBIS logic. Input data is not processed segment-wise, but all data is serialized and fed into one central logic where a Global Beam Permit is directly computed.

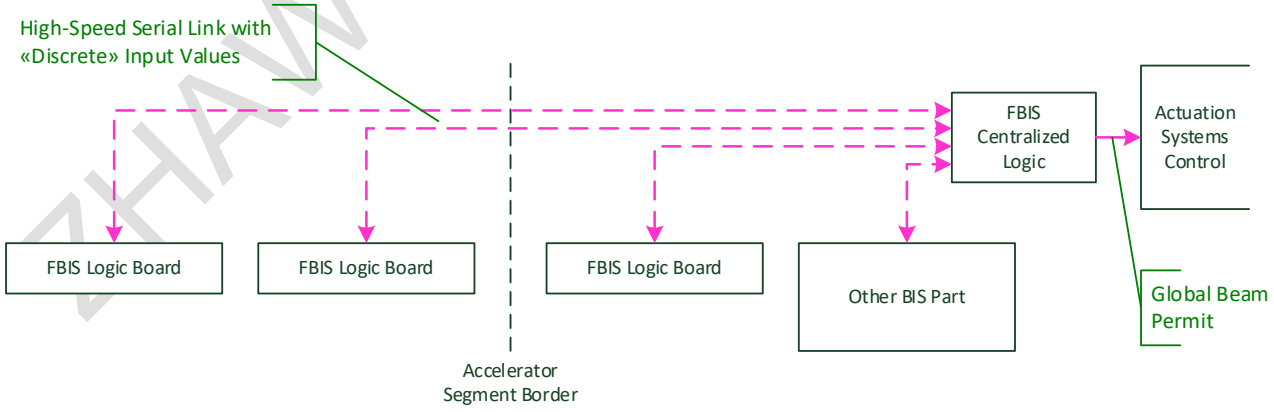

Figure 27: Data is not processed on a per-segment basis, there is no segment specific beam-permit aggregation. All information is serialized and brought to a centralized FBIS Logic Board where the decision on the Global Beam Permit is taken.

Pro	Con
P101 Depending on technical realization might result in less latency.	C86 If FBIS Centralized Logic fails → big problem C87 Multiplication of optical protection lines requires multiplication of fibers and FBIS centralized logic module

3.5 Actuation System Control

Based on the state of the Global Beam Permit, several actuation systems have to be controlled in order to achieve the safe state. This task will be assumed by Actuation System Controllers.

3.5.1 All-in-One Actuation Systems Controller

Figure 28 shows an option where all the actuation systems are controlled by one single, integrated controller.

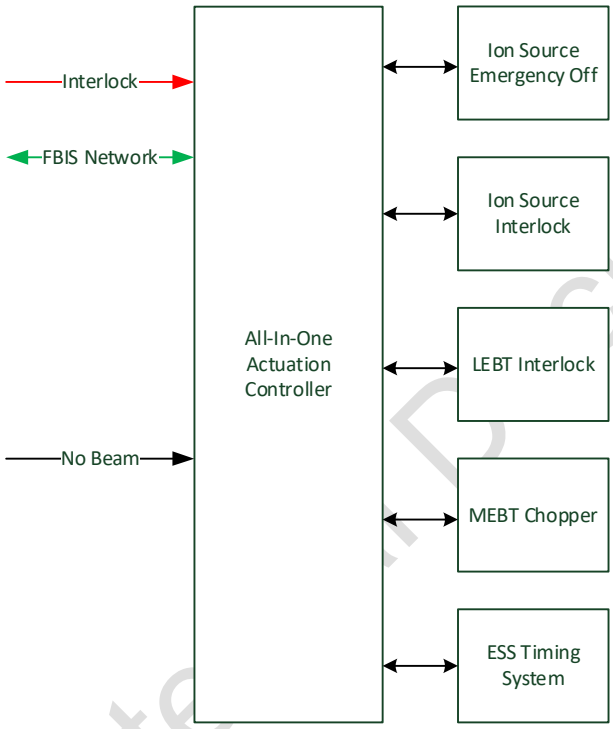

Figure 28: One single element controls all of the actuation systems based on the Global Beam Permit.

Pro	Con
	C88 If Actuation Systems are distributed across facility the “All-In-One Actuation Controller” has to interface with all of them which might result in long cables C89 If “All-In-One Actuation Controller” fails → Big Problem

3.5.2 Dedicated Actuation Systems Controller – Individual Interlock

Figure 29 shows an alternative, where each actuation system is controlled by an independent controller, each getting the Global Beam Permit information individually.

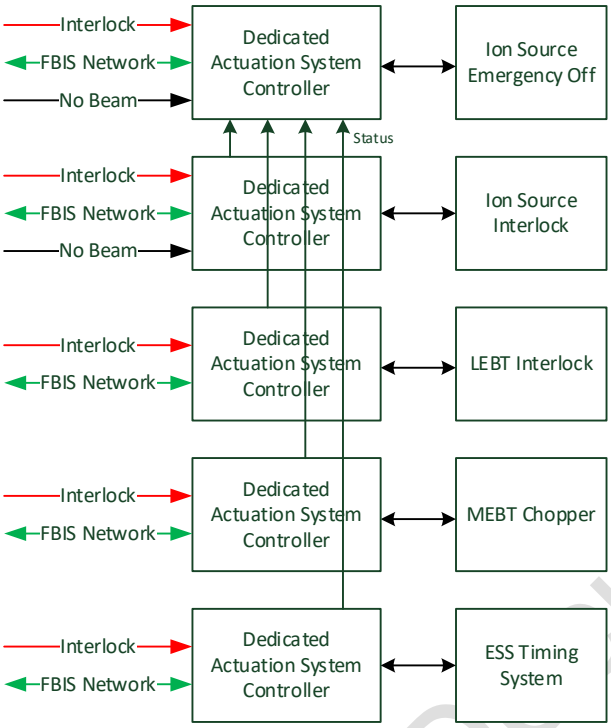

Figure 29: The actuation systems are controlled by individual controllers, all receiving an independent Global Beam Permit signal.

Pro	Con
P102 If one “Dedicated Act. Ctrl.” Fails, the others could detect that and enter the protected state	C90 Every “Dedicated Act. Ctrl.” needs an ILK Input (the red lines) and FBIS-Network (the green line)

3.5.3 Dedicated Actuation Systems Controller – Grouped Interlock

Figure 30 proposes a solution where the actuation systems are still controlled by individual controllers, but where the number of Global Beam Permit signals is reduced to three, one for the Timing System, one for the Ion-source Emergency Off and one to be shared among the normal Ion-source Interlock and the LEBT and MEBT-chopper interlocks.

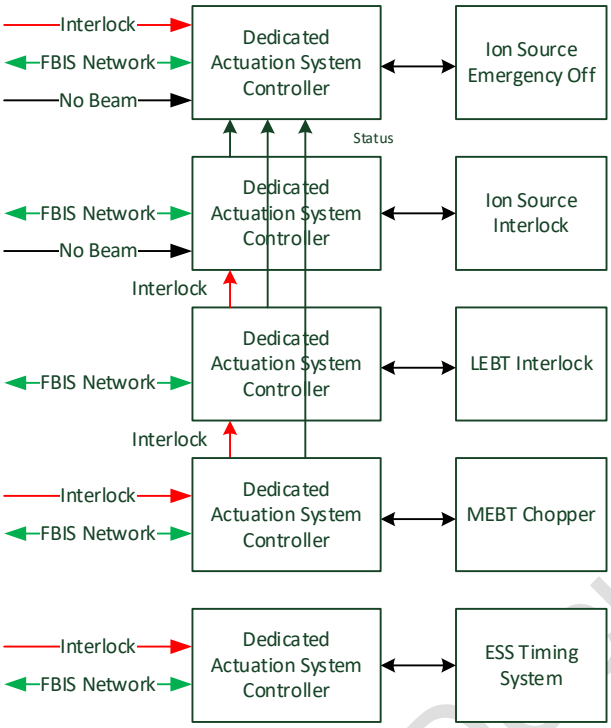

Figure 30: The actuation systems are controlled by independent controllers. The ion-source, LEBT and MEBT chopper interlock controllers use the same Global Beam Permit signal.

Pro	Con
P103 One could “group” the boards according to the physical location of the Actuation Systems and according to Inhibit/Regular/Emergency Interlock	C91 Propagating “ILK” from one “Dedicated Act. Ctrl.” to the next might introduce additional latency

3.6 FBIS Network

In order to achieve a high-level of diagnostic coverage and give additional redundancy possibilities, we propose to link the elements of the FBIS through a network.

3.6.1 Dedicated FBIS Ethernet Network

In the proposal shown in Figure 31 we connect all the FBIS elements over a standard Ethernet network.

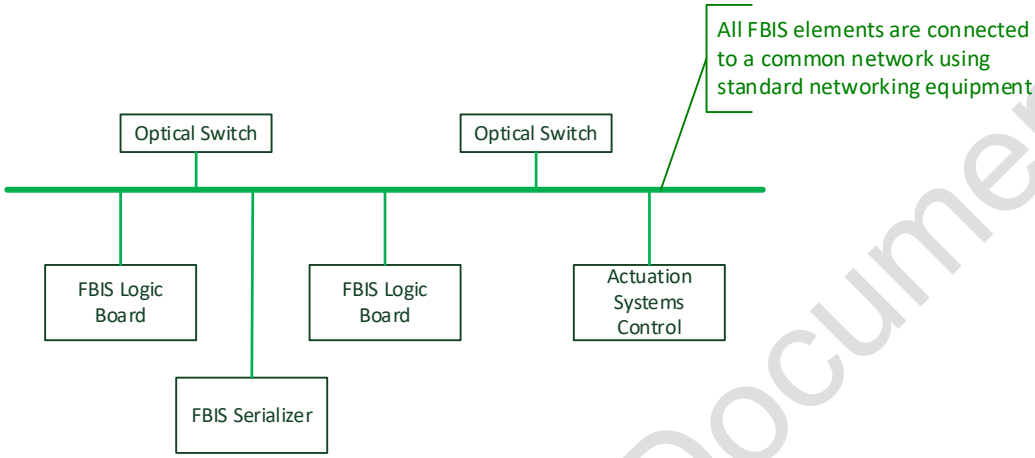

Figure 31: Dedicated FBIS Ethernet Network

Pro	Con
P104 Very scalable approach	C92 Latency might be difficult/impossible to "forecast"

3.6.2 Daisy-Chained FBIS Elements Communication

Figure 32 shows an option where the FBIS logic boards are daisy-chained up to the Actuation Control Systems.

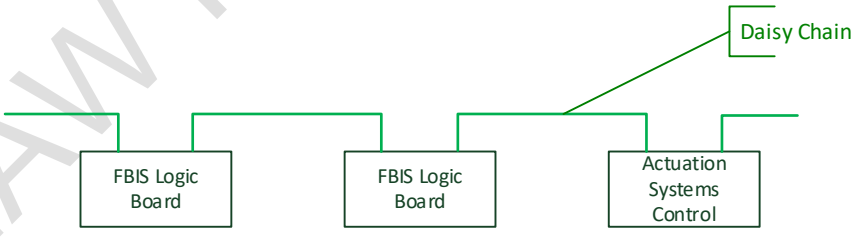

Figure 32: Daisy-chained data-link connection between FBIS Logic Boards

Pro	Con
	C93 If one fails the communication is interrupted → more clever topology needed C94 Every node might introduce latency

4 Preliminary Conclusion

This chapter describes contains a preliminary conclusion from above discussed design options. The conclusions take reference on the design constraints, pros and cons from above using the following format:

- Design constraints are directly referenced by their identifier: DC-2
- An upwards pointing arrow is used to express that an advantage is supported ↑P4
- A downwards pointing arrow is use to express that a disadvantage is repressed ↓C3

4.1 Sensor Side Input

The preliminary conclusion about the sensor side input is the following:

- The interface to sensors shall be realized by easily replaceable mezzanine cards in order to accommodate the different needs and requirements of the interfaces
- Discrete signals shall be based on the electrical characteristics of RS422 unless a system explicitly requires something different:
    - RS422 is state of the art and a fast, proven in use technology at CERN (↑P1, ↑P7, ↑P9, ↑P27, ↑P25, ↑P24)
    - Commercial transceivers which include failure and diagnostic features are available (↑P2, ↑P3, ↑P5, ↑P26)
    - It is very unlikely that the FBIS needs to interface with passive systems in the ESS context. If necessary a custom mezzanine card could be developed. (↑P4)
    - RS422 features multi-drop which means that the signal can be probed easily (↑P6)
    - Galvanic isolation shall be foreseen (↑P8, ↑P23)
    - RS422 is a robust and reliable interface (↑P10, ↑P22)
- Ethernet with a low-level protocol shall be used as data link interface unless a system explicitly requires something different:

4.2 Input Collection and Aggregation

The preliminary conclusion about the signal collection and aggregation is the following:

- The input signals shall be collected and aggregated to a single serial high-speed link as described in chapter “3.2.1 Fully Serialized – Single High-Speed Link”
- The serializer shall be fully redundant:
    - Instead of one single high-speed link, the unit shall feature redundant links. In order to be still operational when one single link fails (↓C51, DC-8, ↑P81, ↑P82) and to increase HFT and diagnostic coverage (DC-8, DC-7)
    - The serializer unit shall be equipped with redundant FPGAs (DC-8)
- The number of input signals processed by a serializer unit shall be high enough such that:
    - One serializer unit can handle all signals from at least one Rack Island (DC-2)
- It is expected that the latency of today’s available high-speed serial links is low enough to not significantly increase the overall system latency (↓C52, ↓C54, ↑P83). However, this is to be confirmed.
- A single serializer unit shall feature multiple high-speed link interfaces. Choosing the FPGA shall take this into account (↓C56). Having multiple high-speed link interfaces principally allows to build up tree structures (see Figure 5) although this is not of primary interest. More important, this allows to connect one serializer unit to multiple FBIS Logic Boards for reasons of Hardware Fault Tolerance (DC-8) and operation in degraded mode (DC-7).
- As the technology is used widely in telecommunication and at PSI and can be considered “state of the art” (↓C55, ↑P84, ↑P85).
- The serializer unit shall be designed such, that it can also generate discrete signals. Again, this principally allows to build up tree structures (see Figure 5). At the same time this allows to process signals without having to serialize them (↑P88, ↑P89)
- The serializer unit firmware shall be generic for all units (DC-12).

4.3 FBIS Logic

The preliminary conclusion about the FBIS Logic is the following:

- The basic pattern for the FBIS Logic shall follow chapter “3.3.3 Fully Serialized – Dual Board 1oo2 Redundancy”
- One pair of boards shall be used for every beam line section. The overall number of boards is therefore still low (approx. 15 to 20 boards in total) (↓C79)
- The both redundant boards shall compute the decision logic (DC-8).
- A board shall diagnose its redundant board and enter a fail-safe state if a discrepancy is detected (↑P90).
- Although a 1oo2 pattern is proposed, the pattern could principally be extended to a more complex one, e.g. a 2oo3 pattern (↑P92) or reduced to a 1oo1 pattern (↑P91, DC-7).
- An IFC-1410 shall be used a board (DC-6).
- The firmware implementation shall be based on the TOSCA 3 framework (DC-12).

4.4 Global Beam Permit Generation

The preliminary conclusion about the Global Beam Permit Generation is the following:

- An optical protection line as discussed in chapter “3.4.1 Optical Protection Line” shall be realized.
- The optical protection line shall be redundant and bi-directional, meaning that nodes upstream and downstream detect an interruption.
- In case one line is unavailable it shall be possible to run the system with a single line in a degraded mode (↓C81).
- The latency introduced by a repeater is considered to be low enough to not significantly increase the overall latency of the system (↓C80, ↑P100, ↑P101).
- The Optical Protection Line Repeater shall be realized as mezzanine card which can be installed either on a serializer unit or on a FBIS Logic board. This allows to read back status and diagnostic information without additional overhead (↓C82). At the same time the switch can be easily controlled (↓C83).
- The mezzanine card shall be designed such that other parts of the BIS can interrupt the link as well without having to pass a serializer unit and FBIS logic board (DC-1).

4.5 Actuation System Control

The preliminary conclusion about the Actuation System Control is the following:

- Principally, the pattern introduced in chapter “3.5.2 Dedicated Actuation Systems Controller – Individual Interlock” shall be followed.
- The same hardware as used for input signal aggregation and serialization shall be used (DC-4).
- Escalation from Beam Inhibit to Regular Beam Interlock to Emergency Beam Interlock shall be realized through interfaces between the controllers directly (↑P103).
- The firmware shall detect failures (e.g. when an chopper does not deflect beam within a certain timeout), escalate the beam switch-off function (DC-9).

4.6 FBIS Network

The preliminary conclusion about the FBIS Network is the following:

- The structure introduced in chapter “3.6.1 Dedicated FBIS Ethernet Network” shall be followed.
- It is expected that today’s state of the art technology has low enough latencies. However, this has to be confirmed (↓C92).

Appendix

5 List of Figures

6 List of Tables

7 List of Architectural Design Constraints

DC-1 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.

DC-2 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.

DC-3 Arrange connection of signals to the FBIS such as to avoid unused inputs.

DC-4 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.

DC-5 The FBIS should allow easy failure localization and feature sufficient built-in testing functions for this.

DC-6 The FBIS should be based as much as possible on standard ESS Controls equipment to simplify spare-parts management and maintenance procedures.

DC-7 The FBIS should allow disabling selected parts under controlled circumstances (degraded mode).

DC-8 Design the FBIS components such as to keep the option to achieve a Hardware Fault Tolerance of 1 or higher.

DC-9 Built-in test functionality must be extended with a fail-safe failure reaction mechanism to increase the safe failure fraction.

DC-10 The FBIS architecture should support the concept of segments and be scalable in terms of segments.

DC-11 Signals related to Protection Functions dedicated to one accelerator segment should be connected to the corresponding FBIS segment.

DC-12 The firmware defining the FBIS function should not have direct dependencies to the hardware it runs on.

8 List of Pros

P1 Proven in use at PSI

P2 Short-circuits can be detected continuously on input side only

P3 Disconnected/interrupted links can be detected continuously on input side only

P4 Compatible with electromechanical switches (if needed in “fast” protection functions), more generally, output side can be “passive”

P5 State of current loops can be read continuously (it’s analog)

P6 Current-loop state can easily be measured without disconnecting the signal with a custom probe

P7 Robust against EMI (proven in use at PSI)

P8 Does not need common ground

P9 Fast: to be confirmed

P10 Resistance in transmission line has no influence

P11 Proven in use at CERN

P12 Short-circuits can be detected continuously on input and output side (to be confirmed)

P13 Disconnected/interrupted links can be detected continuously on input and output side (to be confirmed)

P14 State of signal can be read continuously (no serial protocol but used in a continuous way)

P15 Off-the-shelf integrated circuits for RS-422 available → obsolescence management

P16 Standardized protocol and signal levels (if used in a standard way)

P17 One “sender”, multiple “reader” support

P18 Robust against EMI (proven in use technology)

P19 Does not need common ground

P20 Fast: TTL to RS-422 through short cable to RS-422 to TTL needs about 20 ns

P21 2 wires are enough for signal transmission → off-the-shelf standard twisted pair cables can be used

P22 Robust against EMI

P23 Does not need common ground

P24 Fast sender/receiver are available

P25 Large cable bandwidth

P26 Probability of false signal transmission

P27 Light via fiber is slightly faster than electrons via a “cooper cable”

P28 Standard off-the-shelf equipment for testing, diagnostics

P29 Compatible with standard off-the-shelf networking equipment and cabling

P30 Can be “switched” with off-the-shelf components

P31 Standardized protocols are supported (UDP, TCP, …), EtherCAT (to be confirmed)

P32 Compatible with PLC Systems

P33 Robust versus EMI (proven in use technology)

P34 Longer cable length support (to be confirmed)

P35 RS-485 supports multiple sender over same line

P36 Simple to generate data from FPGA (does not need “stack”)

P37 Compatible with PLC Systems

P38 Minimal pin count for Rx/Tx

P39 Robust versus EMI (proven in use technology)

P40 Only one link needed for all

P41 Off-the-shelf solutions for high-speed serial links are available, including SFP based stuff.

P42 Transfer medium can be selected to be copper or optical fibers

P43 Long cable support

P44 OK/NOK link faults detectable at data packet level

P45 Support for high-speed serial (SERDES) built-in on FPGA

P46 Networking and Telecom standard interfaces

P47 Robust versus RMI (proven in use technology)

P48 No ground related problems in case of optical transfer (electrical to be confirmed)

P49 Number of OK/NOK signals scalable

P50 OK/NOK data packets not delayed by data transmission

P51 Packet transfer rate for OK/NOK transmission is not dependent on data transfer

P52 Redundant transmission of OK/NOK over two links

P53 Same piggy-back can be used on both sides (top and bottom)

P54 No additional mTCA slot is blocked

P55 Same piggy-back can be used on both sides (top and bottom)

P56 FMC slot is not blocked

P57 More pins available than with piggy-back

P58 Could be used to implement more “sophisticated” interfaces

P59 No free FMC slot is required

P60 No free mTCA slot is required

P61 Signals are easily accessible

P62 More signals than on front-panel

P63 Direction can be selected

P64 More signals than on front-panel but maximal 4

P65 Direction can be selected

P66 Standardized connector

P67 Input density on FBIS Logic Board side can be high → Only one link needed for all

P68 Off-the-shelf solutions for high-speed serial links are available, including SFP based stuff.

P69 Transfer medium can be selected to be copper or optical fibers

P70 Long cable support

P71 Link faults detectable at data packet level

P72 Support for high-speed serial (SERDES) built-in on FPGA if Serializer/Switch is realized with FPGA

P73 Networking and Telecom standard interfaces

P74 Robust versus RMI (proven in use technology)

P75 No ground related problems in case of optical transfer (electrical to be confirmed)

P76 Number of input signals scalable

P77 Technology is widely used in industry + PSI Center for Proton Therapy

P78 Principally multiple Serializer/Switch could be cascaded (tree structure)

P79 Interface can be easily multiplied (one Serializer/Switch could provide multiple identical High-Speed links)

P80 Allocation of Sensor Systems to Serializer/Switch is flexible (1 big switch, multiple small switches, …)

P81 Data and Discrete signals are communicated via different channels (redundancy)

P82 Redundant transmission of OK/NOK signals

P83 OK/NOK signals do not need to be serialized → fast transmission

P84 OK/NOK signals does not base on “advanced technologies” such as SERDES, etc. → obsolescence management, reliability

P85 This is the “traditional” technology used at Research Facilities (CERN, PSI, …)

P86 Link faults of OK/NOK signals continuously detectable if interface features this

P87 Less “manual” work required to re-assign signals

P88 Very flexible. Feature can be used if necessary but is not “mandatory”

P89 Certain signals (required to be very fast) could be routed discrete and not via the high-speed serial data-link → these signals would not suffer from the latency introduced by serialization/deserialization

P90 If one FPGA fails to correctly compute the decision logic or stops working, the diagnostic unit would detect that and enter the protected state

P91 If one FPGA fails and the ESS expert could “isolate” this FPGA under controlled conditions, beam operation could continue in a “degraded mode”

P92 One could besides of the redundant FPGA on the board also use two boards resulting in 2x2 FPGA’s

P93 Fully redundant pattern between “Redundant Output” and the system which receives the Beam Permits of the FBIS Logic Boards → not only HFT of FPGA is 1 but also the high-speed link, etc.

P94 If one FBIS Logic Board fails to correctly compute the decision logic or stops working, the diagnostic unit would detect that and enter the protected state

P95 If one FBIS Logic Board fails and the ESS expert could “isolate” this FBIS Logic Board under controlled conditions, beam operation could continue in a “degraded mode”

P96 Scalable with respect to number of nodes (node = optical switch)

P97 ESD/EMV not expected to be a problem

P98 No ground loops

P99 Multiple optical lines could be used without a lot of overhead

P100 No latency introduced per additional FBIS logic board. Only latency of FBIS centralized logic

P101 Depending on technical realization might result in less latency.

P102 If one “Dedicated Act. Ctrl.” Fails, the others could detect that and enter the protected state

P103 One could “group” the boards according to the physical location of the Actuation Systems and according to Inhibit/Regular/Emergency Interlock

P104 Very scalable approach

9 List of Cons

C1 No off-the-shelf components that directly implement this in an integrated circuit → need to design this with discrete components

C2 Fault detection on input side only

C3 Only point-to-point signal transmission

C4 Custom probe needed for measurement

C5 Needs 3 wires for signal transmission

C6 Custom equipment needed to generate tests

C7 Cable type has influence on latency

C8 Need to consider ESD issues at inputs and outputs

C9 If opto-couplers are used: degeneration of opto-couplers “Arbeitspunktverschiebung” may lead to faulty signal detection

C10 Electromechanical switches not supported on output side, more generally, both sides must be “active”

C11 Error detection needs additional circuitry (for the fastest available chips without integrated error detection)

C12 Custom error detection is based on non-standard voltage levels (to be confirmed)

C13 To be clarified: Reliability of fault-detection?

C14 Can only handle a small common-mode range (-7 .. +12 V)

C15 Resistance of cables/connectors might cause voltage drop

C16 Cable type and length have an influence on latency

C17 Connection to off-the-shelf test equipment might be simpler (to be confirmed)

C18 Needs intelligence at outputs and inputs

C19 Fiber is more expensive than cooper cable, might be more difficult to handle

C20 Electromechanical switches not supported on output side, more generally, both sides must be “active”

C21 Error detection needs only possible after reception of a complete “sequence”

C22 Length of “sequence” has influence on latency

C23 Fiber might degenerate with time or “blur” due to radiation.

C24 Needs high pin-count, not only Rx/Tx pairs; 8 pins RMII

C25 Ethernet stack needed on FPGA side

C26 RS-422 supports only one sender

C27 Not clear whether “switching” off-the-shelf components are available

C28 Transmission speed limitations (to be confirmed), dependent on cable length

C29 Short-circuits cannot be detected continuously

C30 Disconnected/interrupted links cannot be detected continuously

C31 State of signal cannot be read continuously

C32 OK/NOK transmission suffers from latency due to packetized transfer → might be slower than discrete solutions

C33 Only point-to-point support

C34 Rocket-IO pins from FPGA needed for using built-in FPGA high-speed serial link capabilities (Aurora)

C35 Higher complexity compared to RS-422 or current loops

C36 Packet transfer rate depends on packet size

C37 Solution not “established”

C38 Data packet transmission might block OK/NOK transmission

C39 Lost redundant transmission of OK/NOK (everything goes over one single link)

C40 Needs two fibers

C41 FMC slot is blocked

C42 mTCA slot is blocked

C43 Requires a free FMC slot

C44 Interface circuit needs to be added to RTM

C45 Existing RTMs would need to be modified

C46 Might need to split signal from one and the same connector (some are used for FBIS, others are used for other purposes)

C47 Low number of signals

C48 Pre-defined direction

C49 Flat band-cable might be difficult to handle or might even block a full mTCA slot

C50 Maximally 4 signals

C51 Lost redundant transmission of OK/NOK (everything goes over one single link)

C52 Data packet transmission introduces latency

C53 Only point-to-point support (One Serializer/Switch is connected with one FBIS Logic Board, unless the HW features multiple high-speed serial links)

C54 Packet transfer rate depends on packet size

C55 Technology is generally not used at Research Facilities (CERN, …)

C56 Number of High-Speed serial links per FBIS Logic Board depends on physical type of link and on FPGA size and type (to be confirmed)

C57 Increased cabling

C58 Requires more High-Speed Serial Link inputs and outputs

C59 Need to consider EMI protection

C60 Requires many “passive” components such as multi-core cables, connectors, patch-panels, etc.

C61 Not scalable with respect to the OK/NOK signals one FBIS logic board can process → as FPGA pins are limited

C62 OK/NOK signals cannot easily be duplicated (depends also on type of interface)

C63 FBIS logic board needs to detect faults of OK/NOK signals → might increase the number of pins needed to read one single OK/NOK signal

C64 Physical space available for connectors on FBIS Logic Board is limited → may impose constraints on number of connectors and multi-core cable

C65 Re-assigning OK/NOK signals involves “manual” work → e.g. re-patching of connections

C66 Additional complexity due to “active patching”

C67 Additional overhead for configuration management, diagnostics, obsolescence management, V&V

C68 Might introduce additional latency

C69 Different latencies depending on how the signal is routed → could increase FPGA firmware complexity

C70 Increased cabling overhead. Overhead, depends heavily on concrete usage

C71 Increase complexity as both, discrete signals and high-speed serial link is required. (Note: Unless the technology is used anyways, e.g. for the interface between Sensor Systems and Serializer/Switch)

C72 Additional overhead for configuration management → need to support “different” Serializer/Switches e.g. with different FPGA Firmware

C73 Diagnostic unit might need to handle jitter-problematic

C74 If both FPGA's would share the same clock (for easier synchronization) this would be a common cause issue (Could be avoided by using independent clocks and external synchronization)

C75 Generally: common cause issues

C76 Redundancy is only introduced at "FGPA level" no redundancy between Sensor Systems and FPGA

C77 If FPGA A fails, the correct functioning of FPGA B could be compromised as well as sensor data goes "via" FPGA A

C78 uRTM receives power from AMC-card, uRTM does not have its own power supply

C79 Double number of uRTM and AMC Cards (the FBIS Logic Board) unless the existing uRTM and AMC Card of another "segment" is used or a "neighbor" Card is used

C80 Every node introduces latency

C81 If one node interrupts line due to a failure beam operation is stopped. Node needs to be "isolated" in order to continue beam operation

C82 Opt. Switch needs to provide a feedback about its status to some kind of "intelligence"

C83 Realization of opt. Switch might not be as easy as it seems (need to take care about multiple inputs, needs to logically OR the inputs, might need to provide masking feature, needs to provide diagnostic info, etc.)

C84 There is one "FBIS centralized logic" module which has to centralize all the aggregated Beam Permits → if that one fails, big problem!

C85 Multiplication of optical protection lines requires multiplication of fibers and FBIS centralized logic module

C86 If FBIS Centralized Logic fails → big problem

C87 Multiplication of optical protection lines requires multiplication of fibers and FBIS centralized logic module

C88 If Actuation Systems are distributed across facility the "All-In-One Actuation Controller" has to interface with all of them which might result in long cables

C89 If "All-In-One Actuation Controller" fails → Big Problem

C90 Every "Dedicated Act. Ctrl." needs an ILK Input (the red lines) and FBIS-Network (the green line)

C91 Propagating "ILK" from one "Dedicated Act. Ctrl." to the next might introduce additional latency

C92 Latency might be difficult/impossible to "forecast"

C93 If one fails the communication is interrupted → more clever topology needed

C94 Every node might introduce latency