EUROPEAN SPALLATION SOURCE

Beam Interlock System

System Requirements Specifications

Christian Hilbes, ZHAW

Lund
Date: 2015-12-09

Overview

- Purpose of the BIS SRS document
- BIS Requirements (selection)
  - Main function: interlocking
  - Interlock Logic Configurations
  - MP Beam-Off functions
  - Diagnostic features, Error Detection
  - Operational State dependent behaviour
  - Operating Modes and BIS Configuration
  - Logging / Access Control
  - Performance Requirements

Purpose of the Beam Interlock System Requirements Specification Document

- Collect a list of all features the BIS shall have, while staying solution-neutral as far as possible (and reasonable).
  - This includes functional requirements as well as quality or other properties the BIS shall fulfil.
- Serve as base for the design of a BIS architecture and the further specification of BIS components.
- Serve as base for BIS verification planning.

Main Function: Interlocking

- Main function of the BIS: Evaluate all BEAM-PERMIT input signals and control actuation systems to reach and maintain a safe state in case of hazards.
- Safe-state: defined as proton beam off, i.e. no more proton injection into the accelerator and safely deflecting all protons that are in the accelerator.
- This function is specified in two steps:
  - Step 1: Compute a GLOBAL-BEAM-PERMIT state (value OK is good, value NOK should lead to a safe state).
  - Step 2: Trigger actuation devices based on GLOBAL-BEAM-PERMIT.

Step 1: GLOBAL-BEAM-PERMIT Generation

- Should be NOK by default (safe state by default, unless actively set to OK).
- Compute new GLOBAL-BEAM-PERMIT “continuously”, based on Interlock Logic Configuration
  - “Continuously” is implementation dependent. Proof of “continuous enough” part of protection function verification.

Interlock Logic Configuration

- Slight solution-oriented requirement…
- Interlock Logic Configuration composed of
  - Boolean equation (in whatever format) relating the GLOBAL-BEAM-PERMIT to the BEAM-PERMIT inputs.
  - Specification of “operating modes” it is compatible with.
  - Per BEAM-INPUT
    - Allowed PROTECTION MODE setting
    - LATCH-MODE (Latch only inputs, not GLOBAL-BEAM-PERMIT)
    - ERROR-VALUE to use in case errors are detected at the input level.
- Define boolean equation as to lead to safe-state in case of potential hazard (as indicated by inputs) in actual operating mode.

Step 2: MP Beam-Off Functions

- The BIS can trigger the beam-off function of multiple actuation systems.
  - Which sequence or combination is best is not clear yet → should be configurable and is called MP beam-off function.
- Independently of the concrete actuation systems, we discern several MP beam-off functions.

MP Beam-Off Functions

Function	Usage/Properties
Regular MP Beam-Off	“Normal” Interlock; should be fast enough and with negligible damage risk.
Emergency MP Beam-Off	In case the regular function fails (because of actuator error status or detected beam); should be effective and if possible redundant to the regular function (common cause).
Actuator-Error MP Beam-Off	In case an actuator error gets detected; whenever possible with negligible damage risk.
BIS-Error MP Beam-Off	In case the BIS self-diagnostics detect an error; should be effective.

Diagnostic Features, Error Detection

- At the BEAM-PERMIT input level
  - Detect link problems.
  - Detect functional-readiness of BEAM-PERMIT signal providers (configurable per input).
  - Set BEAM-PERMIT input state to ERROR-VALUE in case of problems.
- At the actuator level
  - Detect link problems.
  - Detect functional-readiness of actuation systems (for all of them).
  - Actuator-Error MP Beam-Off function in case of problems.

Diagnostic Features, Error Detection

- BIS self-diagnostics
  - Requirements for diagnostic coverage and reaction on error detection integrated in IEC 61508 – part of the protection integrity level requirement.
  - BIS-Error MP Beam-Off function in case of problems.

Operational State dependent Behaviour

- Beam only when BIS in full operational state.
  - GLOBAL-BEAM-PERMIT can only become OK in full operational state.
  - All connected actuation systems have to have their beam-off function activated (independently of the GLOBAL-BEAM-PERMIT).
  - If the BIS is not operational, nothing will work.
- Solution-oriented requirement: we specifically ask for a power-on self test.

Interlock Logic Configuration to Operating Mode Mapping

- Require one-to-one assignment of Interlock Logic Configurations to Operating Modes.
  - The BIS will need more than one Interlock Logic Configuration to support operation.
  - Should be clear which one to use in what operating mode.
- The BIS should check this assignment for validity at the moment it is configured.

Interlock Logic Configuration Switching

- BIS should support both automated and manual Interlock Logic Configuration switching.
  - Interlock Logic Configuration Switching: the BIS changes the *active* configuration used to compute the GLOBAL-BEAM-PERMIT.
- Automated switching relies on operating mode detection
  - The function to detect the actual operating mode shall be implemented as a protection function (complying with IEC 61508 requirements) with highest protection integrity of the functions processed by the BIS.

Logging / Access Control

- BIS should log all information necessary for causal interlock event analysis.
  - Log all state transitions; all configuration changes, … with time stamps.

- Prevent unauthorized and unintended access to the BIS
  - Unintended: e.g. a command coming from a normally authorized system when it is not expected.

Protection Integrity Requirements

- The BIS is part of all beam-related protection functions.
- It has to be capable of supporting the beam-related protection function with the highest protection integrity requirement.
  - This includes systematic protection integrity and hardware protection integrity.
  - Note that the hardware protection integrity requirements apply to whole protection functions.

Spurious Trip Performance

- The BIS shall not only focus on protection integrity requirements.
- It shall be designed as to minimize spurious trips (interfering with the beam for no reason).

- Remember that the goal of Machine Protection is availability in the first place.

BIS Timing Performance

- Processing protection functions related to imminent hazards with an impact on the LEBT, RFQ, MEBT and DTL sections: 3 µs.
  - Measurement of that time starts when the corresponding signal at the BIS input changes state and stops when the BIS outputs to the actuation system change state.
- Processing protection functions related to imminent hazards and other sections: 9 µs.
- Processing protection functions not related to imminent hazards and other sections: 15 ms.
- Reaction time after error detection: 3 µs.