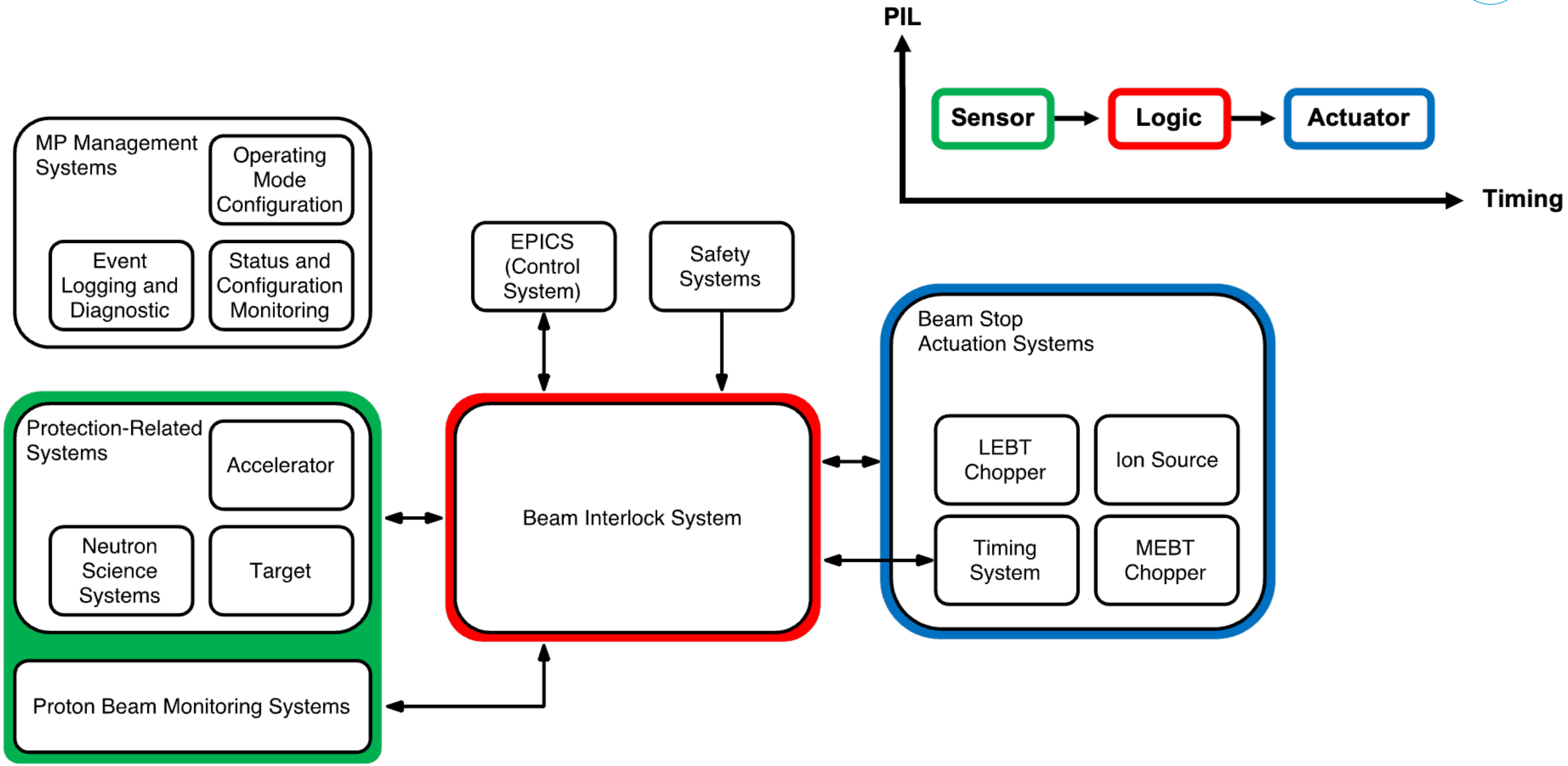
EUROPEAN
SPALLATION
SOURCE

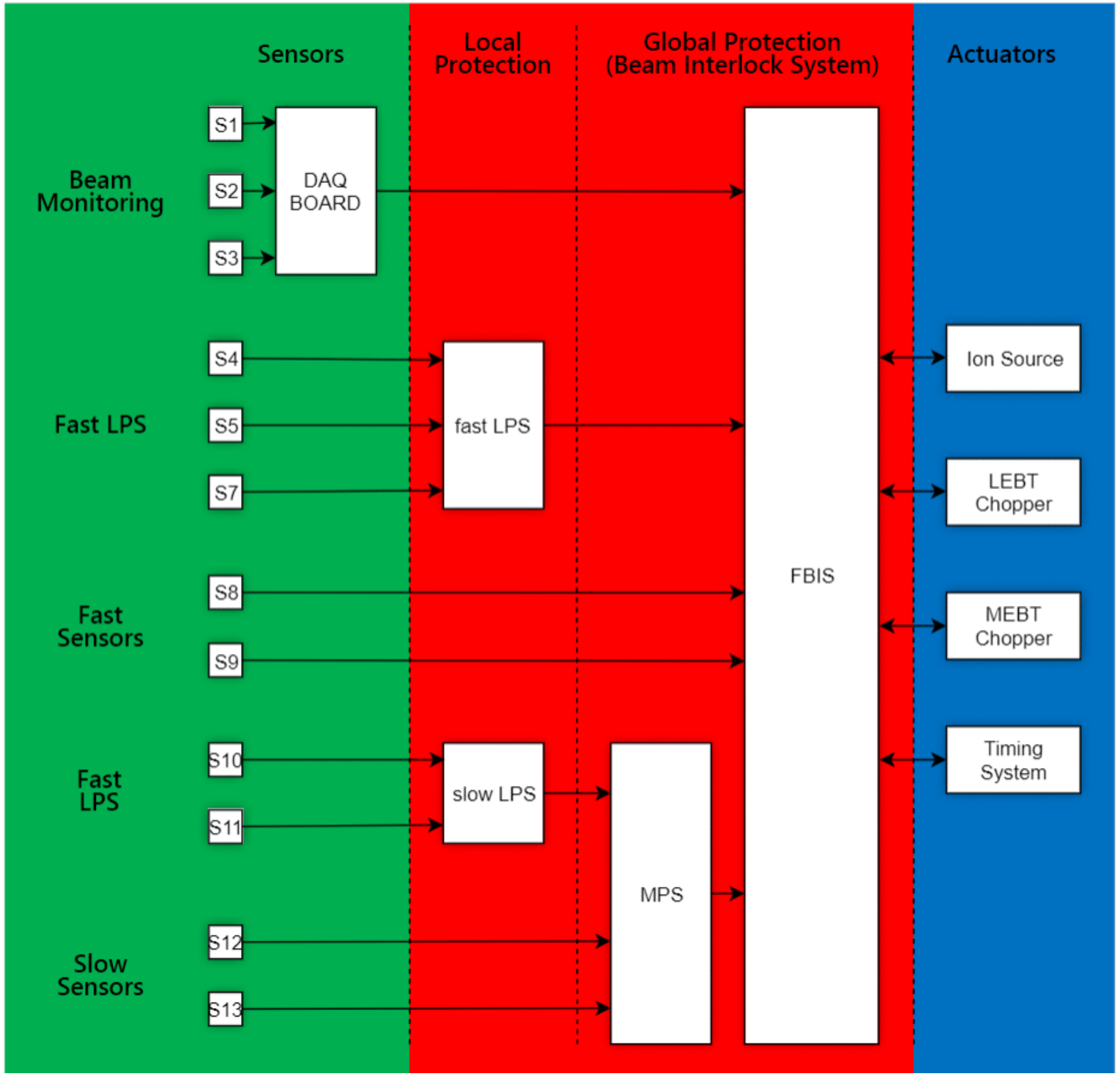
A.Nordt on behalf of
M. Carroll, D. Cosco, E. D’Costa, S. Gabourin, J. Gustafsson, J. Järhög, G. Ljungquist,
X. Mananga, S. Pavinato, R. Silveira, A. Petrushenko, C. Webber, M. Zmuda

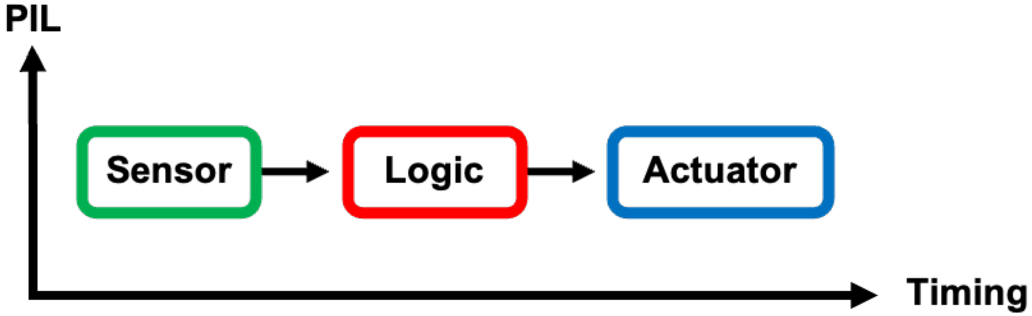
Short Introduction To ESS Machine Protection

Machine Protection System-of-Systems MP-SoS



MP-SoS Organisation and Responsibilities





MP Team is responsible to:

1. Coordinate MP across ESS
2. Define (global) protection functions
3. Develop, operate, and maintain Beam Interlock System (BIS)
4. Ensure working interfaces with BIS
5. Foster awareness that things can break
6. Foster awareness that thorough testing leads to success

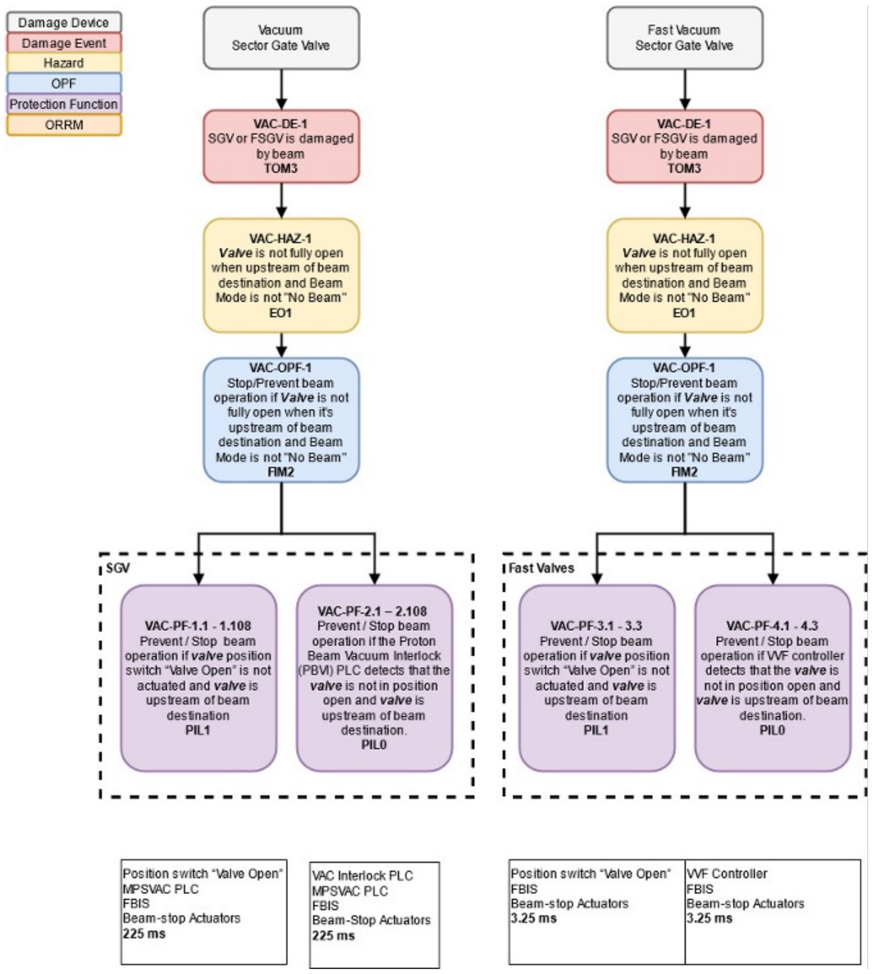
System Owners are responsible to:

1. Develop reliable systems
2. Implement local protection functions
3. Implement MP requirements in their system
4. Provide sensors needed for global protection functions

Global Protection Functions - Example

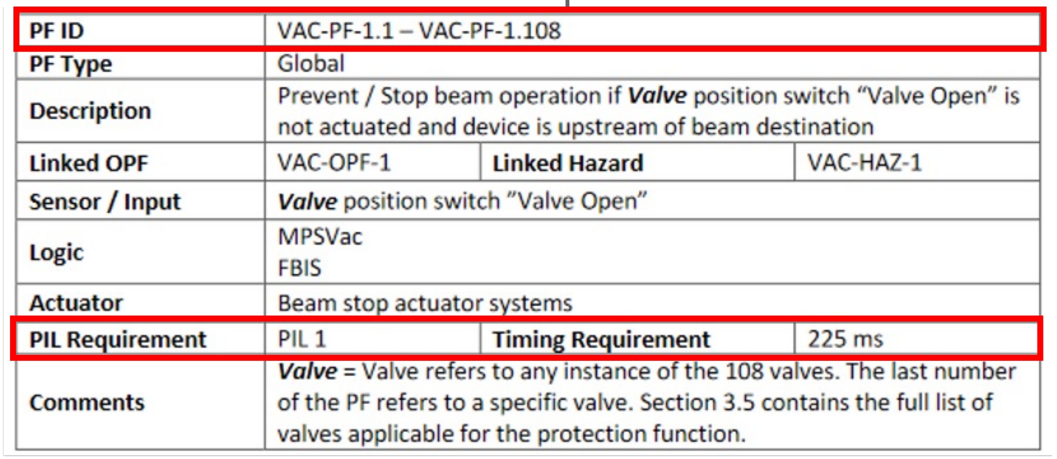
MP Analysis and Protection Functions to avoid Beam Induced Damage

Machine Protection Analysis Example



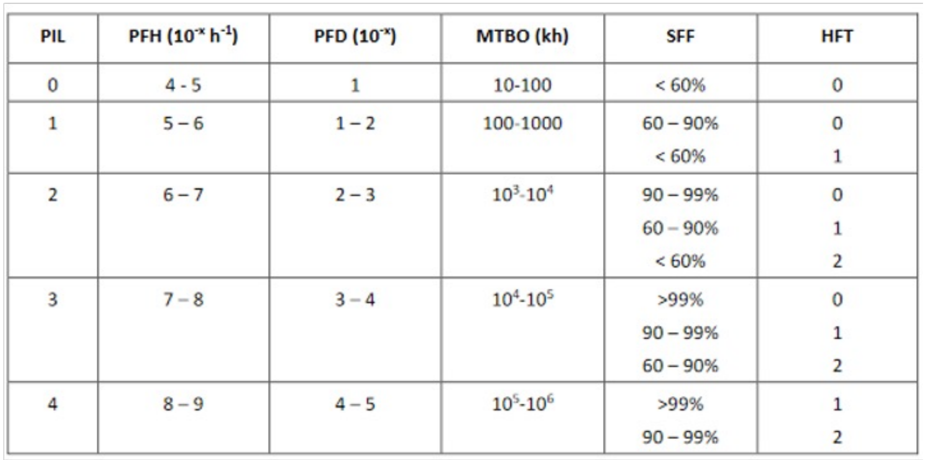
Damage Device
Damage Event
Hazard
OPF
Protection Function
ORRM
Vacuum Sector Gate Valve
VAC-DE-1 SGV or FSGV is damaged by beam TOM3
VAC-HAZ-1 *Valve* is not fully open when upstream of beam destination and Beam Mode is not "No Beam" EO1
VAC-OPF-1 Stop/Prevent beam operation if *Valve* is not fully open when it's upstream of beam destination and Beam Mode is not "No Beam" FIM2
Fast Vacuum Sector Gate Valve
VAC-DE-1 SGV or FSGV is damaged by beam TOM3
VAC-HAZ-1 *Valve* is not fully open when upstream of beam destination and Beam Mode is not "No Beam" EO1
VAC-OPF-1 Stop/Prevent beam operation if *Valve* is not fully open when it's upstream of beam destination and Beam Mode is not "No Beam" FIM2
SGV
VAC-PF-1.1 - 1.108 Prevent / Stop beam operation if *valve* position switch "Valve Open" is not actuated and *valve* is upstream of beam destination PIL1
VAC-PF-2.1 – 2.108 Prevent / Stop beam operation if the Proton Beam Vacuum Interlock (PBVI) PLC detects that the *valve* is not in position open and *valve* is upstream of beam destination. PIL0
Fast Valves
VAC-PF-3.1 - 3.3 Prevent / Stop beam operation if *valve* position switch "Valve Open" is not actuated and *valve* is upstream of beam destination PIL1
VAC-PF-4.1 - 4.3 Prevent / Stop beam operation if VVF controller detects that the *valve* is not in position open and *valve* is upstream of beam destination. PIL0
Position switch "Valve Open" MPSVAC PLC FBIS Beam-stop Actuators 225 ms
VAC Interlock PLC MPSVAC PLC FBIS Beam-Stop Actuators 225 ms
Position switch "Valve Open" FBIS Beam-stop Actuators 3.25 ms
VVF Controller FBIS Beam-stop Actuators 3.25 ms

Protection Function example



PF ID	VAC-PF-1.1 – VAC-PF-1.108		
PF Type	Global		
Description	Prevent / Stop beam operation if ***Valve*** position switch "Valve Open" is not actuated and device is upstream of beam destination		
Linked OPF	VAC-OPF-1	**Linked Hazard**	VAC-HAZ-1
Sensor / Input	***Valve*** position switch "Valve Open"		
Logic	MPSVac FBIS		
Actuator	Beam stop actuator systems		
PIL Requirement	PIL 1	**Timing Requirement**	225 ms
Comments	***Valve*** = Valve refers to any instance of the 108 valves. The last number of the PF refers to a specific valve. Section 3.5 contains the full list of valves applicable for the protection function.		

Protection Integrity Level (PIL) Definitions

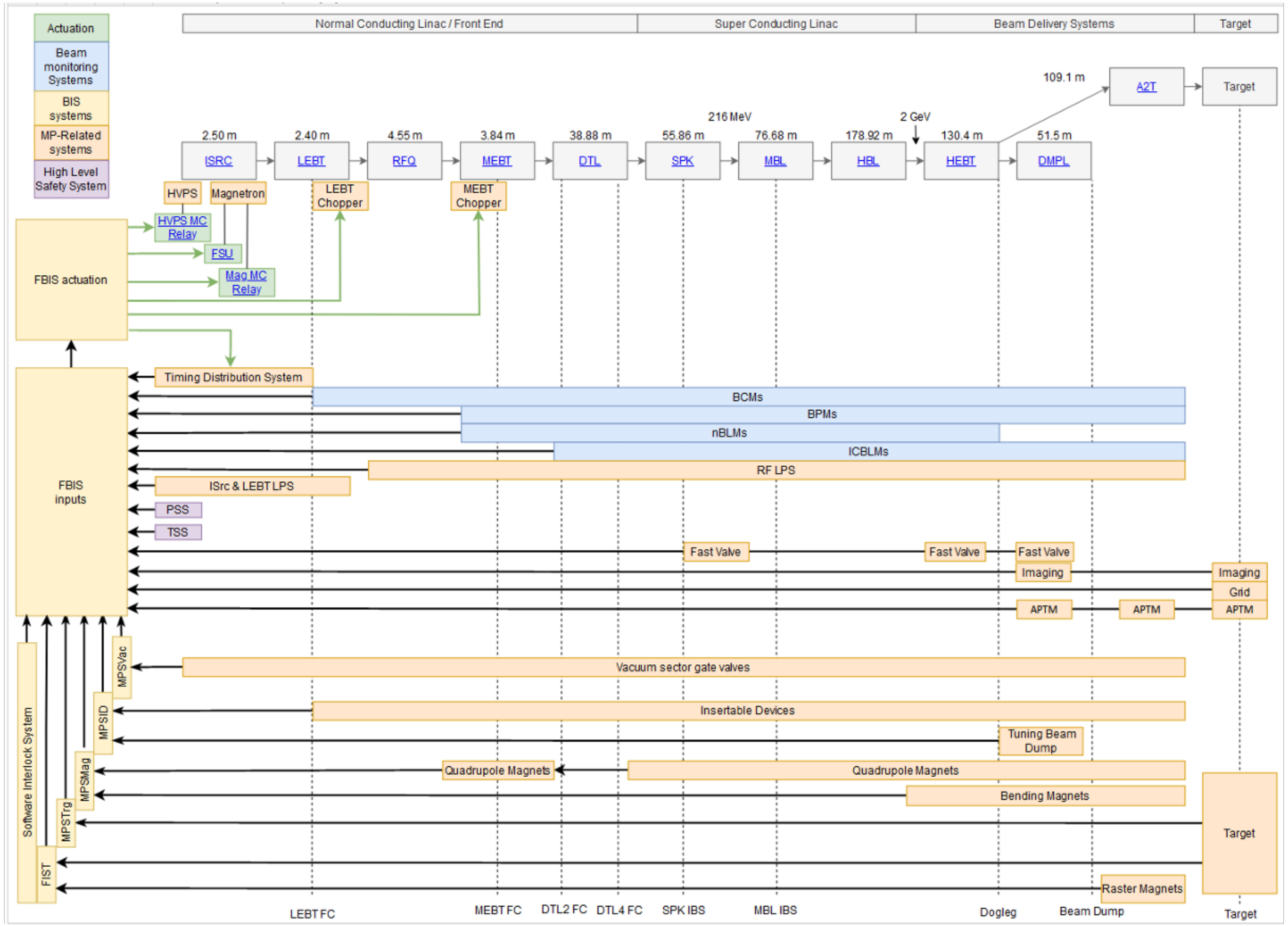


PIL	PFH (10^{-x} h^{-1})	PFD (10^{-x})	MTBO (kh)	SFF	HFT
0	4 - 5	1	10-100	< 60%	0
1	5 – 6	1 – 2	100-1000	60 – 90%	0
				< 60%	1
2	6 – 7	2 – 3	10^3-10^4	90 – 99%	0
				60 – 90%	1
				< 60%	2
3	7 – 8	3 – 4	10^4-10^5	>99%	0
				90 – 99%	1
				60 – 90%	2
4	8 – 9	4 – 5	10^5-10^6	>99%	1
				90 – 99%	2

ESS MP-SoS Distributed View

Layout and scope of Machine Protection Systems of Systems (MP-SoS)

Thousands of inputs



Actuation
Beam monitoring Systems
BIS systems
MP-Related systems
High Level Safety System

Normal Conducting Linac / Front End
Super Conducting Linac
Beam Delivery Systems
Target

109.1 m
A2T
Target
216 MeV
2 GeV
2.50 m ISRC
2.40 m LEBT
4.55 m RFQ
3.84 m MEBT
38.88 m DTL
55.86 m SPK
76.68 m MBL
178.92 m HBL
130.4 m HEBT
51.5 m DMPL

HVPS
Magnetron
LEBT Chopper
MEBT Chopper
HVPS MC Relay
FSU
Mag MC Relay
FBIS actuation

FBIS inputs
Timing Distribution System
BCMs
BPMs
nBLMs
ICBLMs
RF LPS
ISrc & LEBT LPS
PSS
TSS
Fast Valve
Fast Valve
Fast Valve
Imaging
Imaging
Grid
APTM
APTM
APTM

Software Interlock System
FIST
MPSTrg
MPSMag
MPSID
MPSVac
Vacuum sector gate valves
Insertable Devices
Tuning Beam Dump
Quadrupole Magnets
Quadrupole Magnets
Bending Magnets
Target
Raster Magnets

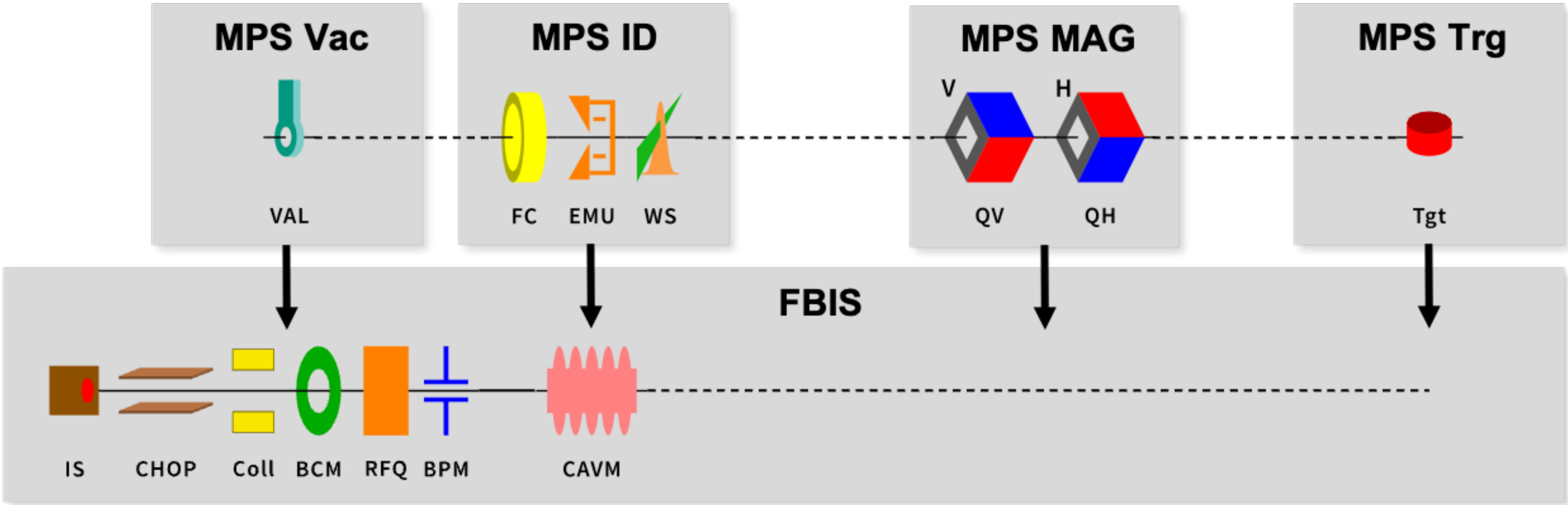
LEBT FC
MEBT FC
DTL2 FC
DTL4 FC
SPK IBS
MBL IBS
Dogleg
Beam Dump
Target

Beam Interlock System: PLC based Systems

MPS**Vac**: Machine Protection System for Vacuum
MPS**ID**: Machine Protection System for Insertable Devices
MPS**Mag**: Machine Protection System for Magnets
MPS**Trg**: Machine Protection System for Target

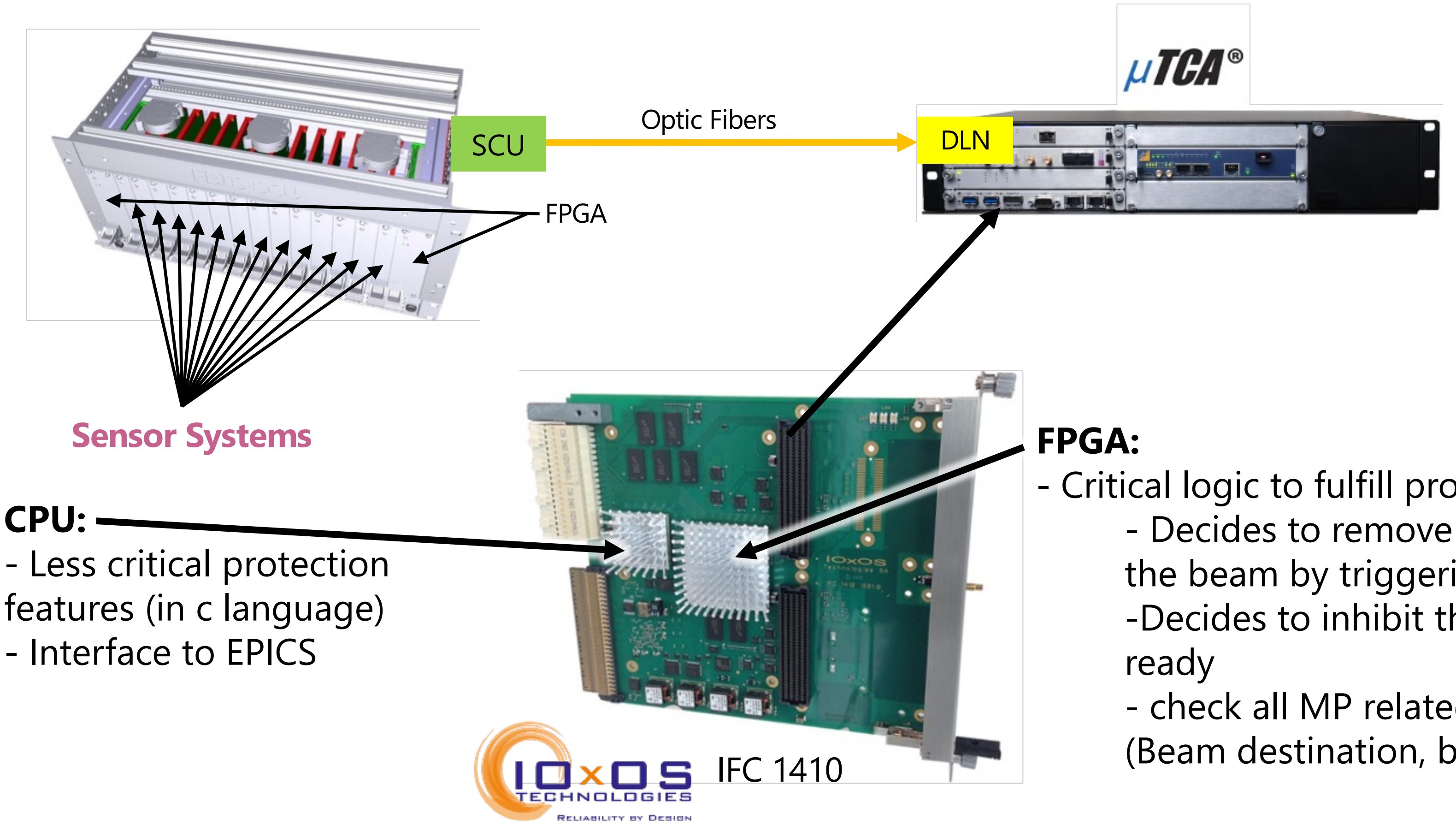
PLC based interlock systems:
- 1 fail safe CPU and multiple, distributed I/Os
- I/Os connect to sensor systems (VSG, FC, EMU, WS, Quads,…)

Slow reaction time > 10ms
Target PIL: PIL 2



Fast Beam Interlock System

- **SCU** (Signal Conversion Unit) concentrating signals from **Sensor Systems** and **MPS PLC based systems**
- **DLN** (Decision Logic Node) concentrating signals from several SCUs, deriving global beam permit and triggering **Actuators** to stop Beam



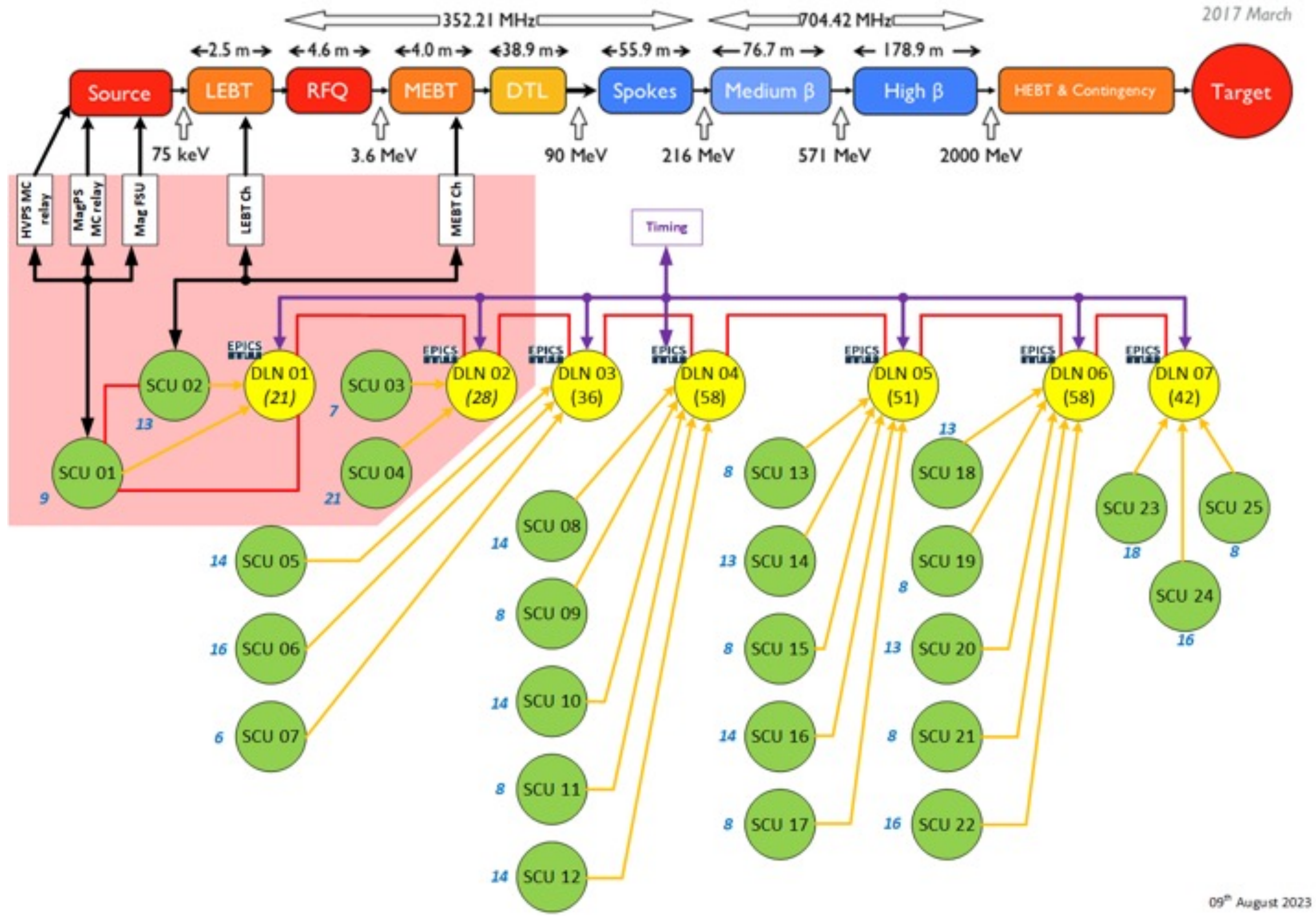
Fast reaction time < 1us
Target PIL: PIL 2

CPU:
- Less critical protection features (in c language)
- Interface to EPICS

FPGA:
- Critical logic to fulfill protection functions (VHDL)
  - Decides to remove the global beam permit and stop the beam by triggering the Actuators
  -Decides to inhibit the beam if sensor systems are not ready
  - check all MP related systems are properly configured (Beam destination, beam mode)

Fast Beam Interlock System - Layout

Layout and scope of the Fast Beam Interlock System (FBIS)

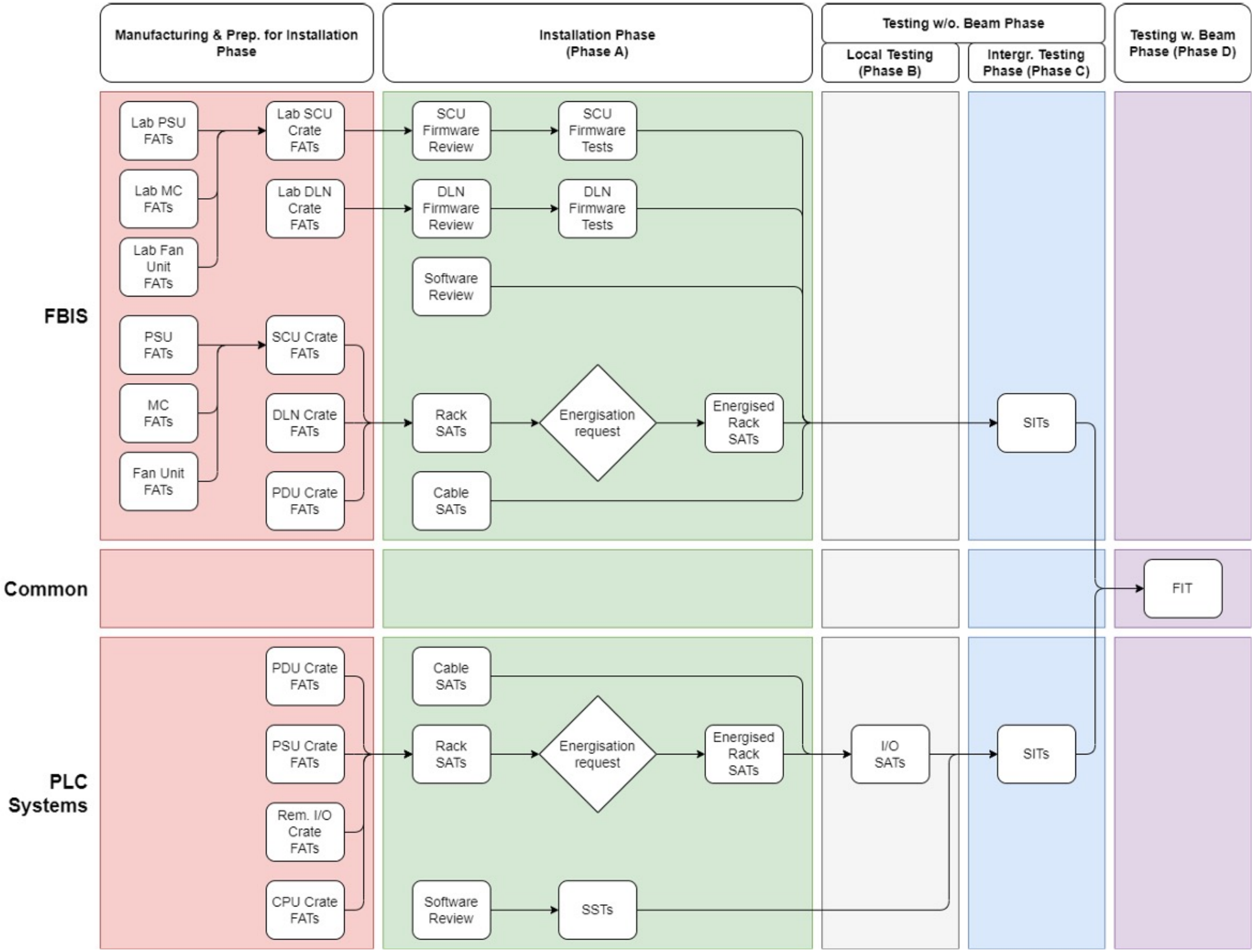


09th August 2023

Verification Strategy of ESS Machine Protection

BIS System Verification Overview

Flow Followed for Systems Developed by MP Team



Manufacturing & Prep. for Installation Phase

Installation Phase (Phase A)

Testing w/o. Beam Phase

Local Testing (Phase B)

Intergr. Testing Phase (Phase C)

Testing w. Beam Phase (Phase D)

FBIS

Lab PSU FATs

Lab MC FATs

Lab Fan Unit FATs

Lab SCU Crate FATs

Lab DLN Crate FATs

SCU Firmware Review

SCU Firmware Tests

DLN Firmware Review

DLN Firmware Tests

Software Review

PSU FATs

MC FATs

Fan Unit FATs

SCU Crate FATs

DLN Crate FATs

PDU Crate FATs

Rack SATs

Energisation request

Energised Rack SATs

Cable SATs

SITs

Common

FIT

PLC Systems

PDU Crate FATs

PSU Crate FATs

Rem. I/O Crate FATs

CPU Crate FATs

Cable SATs

Rack SATs

Energisation request

Energised Rack SATs

I/O SATs

SITs

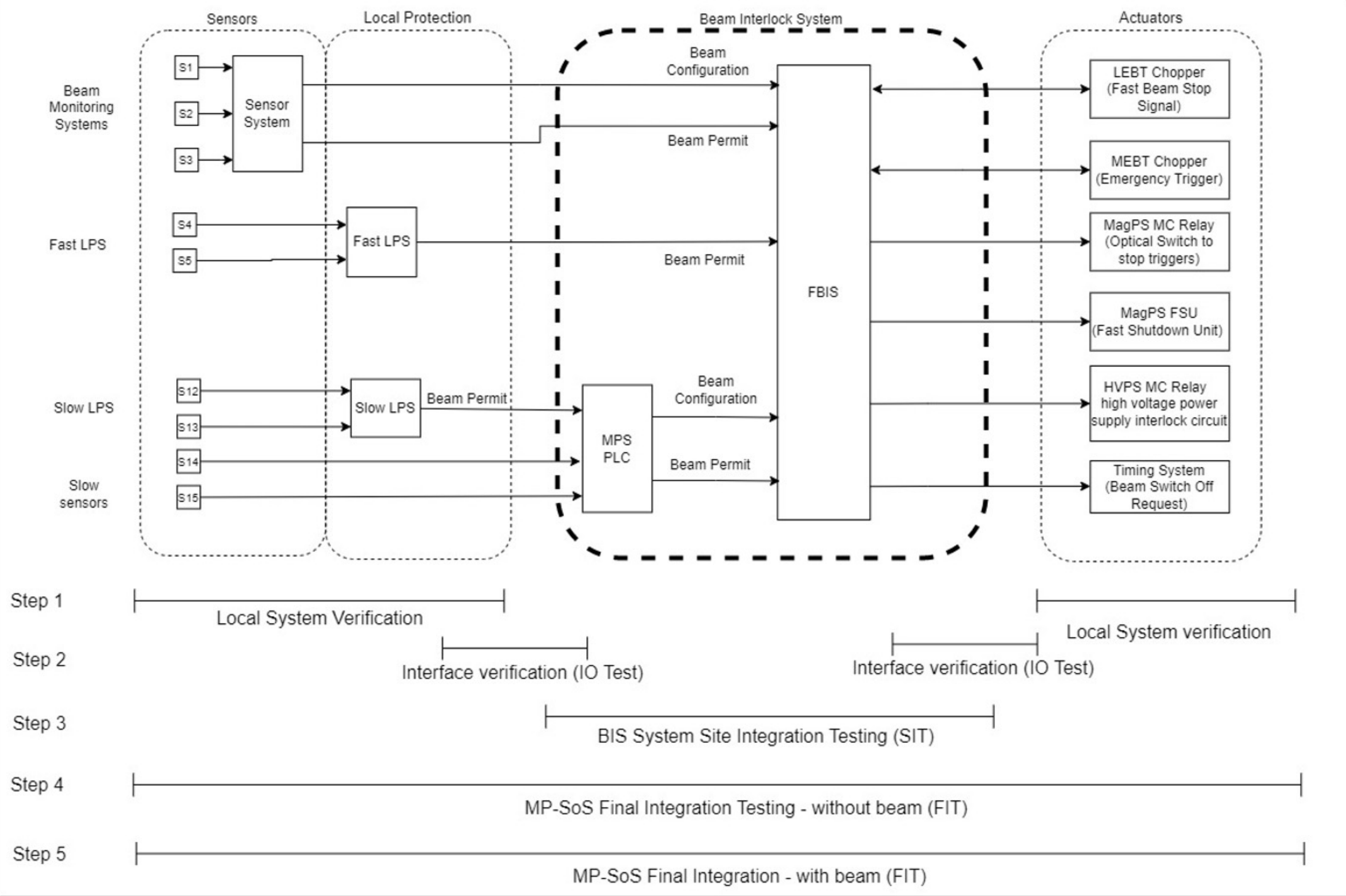
Software Review

SSTs

MP-SoS Verification Overview

Flow Followed for MP-SoS Interfacing Systems Verification

1. Interfacing System verification by system owners. Specifications and reports are reviewed by MP team against MP requirements.
2. Interfaces are verified between systems.
3. BIS systems are verified (SIT).
4. Subset of Protection Functions are tested in Final Integration Test for full chain verification.


Sensors
Local Protection
Beam Interlock System
Actuators
Beam Monitoring Systems
S1
S2
S3
Sensor System
Beam Configuration
Beam Permit
Fast LPS
S4
S5
Fast LPS
Beam Permit
FBIS
Slow LPS
S12
S13
S14
S15
Slow LPS
Beam Permit
Slow sensors
MPS PLC
Beam Configuration
Beam Permit
LEBT Chopper (Fast Beam Stop Signal)
MEBT Chopper (Emergency Trigger)
MagPS MC Relay (Optical Switch to stop triggers)
MagPS FSU (Fast Shutdown Unit)
HVPS MC Relay high voltage power supply interlock circuit
Timing System (Beam Switch Off Request)
Step 1
Local System Verification
Local System verification
Step 2
Interface verification (IO Test)
Interface verification (IO Test)
Step 3
BIS System Site Integration Testing (SIT)
Step 4
MP-SoS Final Integration Testing - without beam (FIT)
Step 5
MP-SoS Final Integration - with beam (FIT)

Lessons Learned

What Has Happened So Far?

Before executing the MP-SoS SIT, a Test Readiness Review is performed.

By the time of the MP-SoS Test Readiness Review all local MP testing shall be done, test reports shall be released and all systems should be ready for integrated testing (SIT).

3 beam commissioning phases have been conducted – beam to MEBT FC, DTL1 FC, DTL4 FC.

Readiness of sensor, actuator systems and BIS at the time of MP-SoS Test Readiness review:

Phase 1: 97%

Phase 2: 80%

Phase 3: 20%

Phase 4: 🫣

What Did We Learn?

Dealing with many stakeholders: behavioral and psychological factors

Don’t aim too high / ensure scope is clearly understood

– People can tend to become defensive and underestimate the remaining scope.
– If you ask if a system can be / or is “ready”, then inevitably the answer will be “yes”.

→ Assess and manage the achievable scope – focus on critical functionality. Defer or update ‘nice-to-haves’.

Example from TRR:

Q: “are you ready”?
A: “yes!”
Q: “nice, can we see the test report?”
A: “aja, … we are still working on the documentation – but we will be ready on time, trust us”

🤔

What Did We Learn?

Dealing with many stakeholders: behavioral and psychological factors

Be transparent about issues and challenges

- Don’t assume that declaring readiness is just a formality / ticking off an artificial milestone.
- Don’t let others push you to declaring readiness just to make your managers look good.

→ Admitting to issues is not a weakness, it is a strength and it will lead to real success.

Example: at ESS for the MP-SoS TRR #3, only 20% were ready, but we still passed the review.

Consequently, beam commissioning was bumpy with many trials to get things fixed during beam time – things that should have been fixed and tested long before.

What Did We Learn?

Dealing with many stakeholders: behavioral and psychological factors

Don’t underestimate the importance of thorough verification

- Separating functions that go across many systems into bits and pieces and testing these one by one first in the lab / in development environment, before testing full functions on site, saves a lot of time when it comes to integrated testing and related fault finding.

→ Following basic systems engineering approach from the beginning is very beneficial and saves time in the long run (have requirements, design documents, test specifications, etc in place).

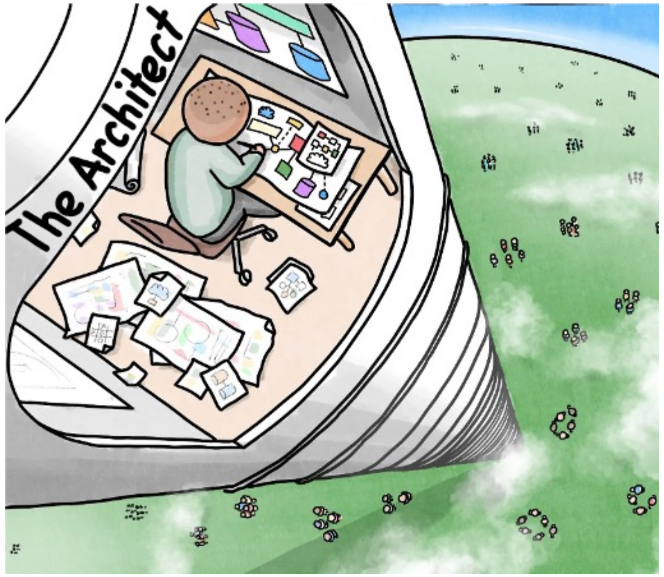
→ Well written and unambigious test documentation will save a lot of time, though it takes time to develop it.

What Did We Learn?

Dealing with many stakeholders: behavioral and psychological factors

Know your stakeholders

– Try to understand how they see the world.
– What are the issues in their teams?
– What is the mind set of their management?



→ Don't sit in an ivory tower.

→ Go for regular inspections on site, in the lab – meet and talk to the people in the field, rely less on written status reports or meetings.

→ Break down the silos.

The End