12th IAEA Technical Meeting on Control, Data Acquisition and Remote Participation for Fusion Research

Progress in the Design of the Interlock System for MITICA

A. Luchetta[a], N. Pomaro[a], C. Taliercio[a], M. Moressa[a], L. Svensson[b], F. Paolucci[c], C. Labate[c]

a) Consorzio RFX, Corso Stati Uniti 4, 35127 Padova, Italy

b) ITER Organization, Route de Vinon sur Verdon, CS 90 046, 13067 St Paul Lez Durance Cedex, France

c) Fusion for Energy, c/ Josep Pla, nº 2, Torres Diagonal Litoral, Edificio B3, 08019 Barcelona, Spain

adriano.luchetta@igi.cnr.it

ACKNOWLEDGMENT

The work leading to this presentation has been funded partially by Fusion for Energy under work programs WP2017/18/19. This publication reflects the views only of the authors, and Fusion for Energy and ITER Organization cannot be held responsible for any use, which may be made of the information contained therein. The views and opinions expressed herein do not necessarily reflect those of the ITER Organization.

Fig. 1. MITICA high voltage deck and insulating transformer

Outline

- ITER Neutral Beam Test Facility
- Overview of MITICA requirements
- Overview of MITICA plant systems
  - Beam source and line
  - Power supply
- MITICA I&C – Architectural Constraints
- MITICA Interlock
  - Functional Constraints
  - Methodology Constraints
  - Technological Constraints
- Fast track to MITICA Power Supply Integration
- Conclusions

ITER Neutral Beam Test Facility (NBTF)

- **R&D to develop the ITER Heating Neutral Beam Injector (HNB)**
- **Established in Padova - Italy at the Consorzio RFX site**
- **Two experiments**
  - **SPIDER – ITER full-size ion source**
    - **In operation since June 2018**
  - **MITICA – ITER HNB full-size prototype**
    - **Operation expected by 2023**

Fig. 2. NBTF buildings.

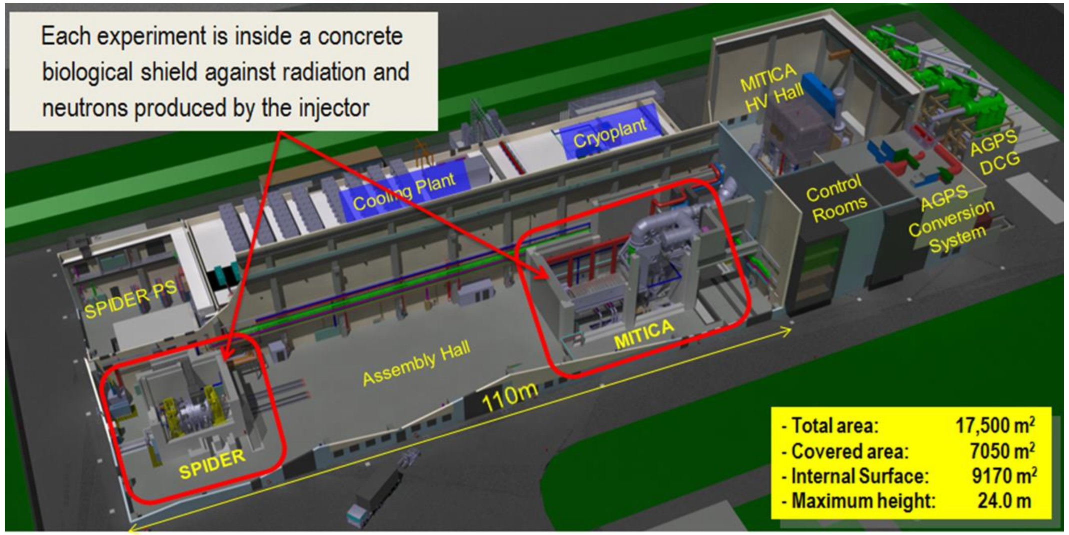


Fig. 3. NBTF building CAD overview.

Overview of MITICA Requirements

Table 1. MITICA requirements

Requirement	***Value***	***Unit***
Ion species (negative)	H- | D-	---
Acceleration voltage	1000	kV
Ion beam current (H-|D-)	45 | 50	A
Beam power	16.5	MW
Beam-on time	3600	s
Beamlet divergence	≤ 7	mrad
Co-extracted electron fraction e-/H- | e-/D-	< 0.5 | 1	---

- **MITICA requirements were never met together in existing neutral beam injectors.**

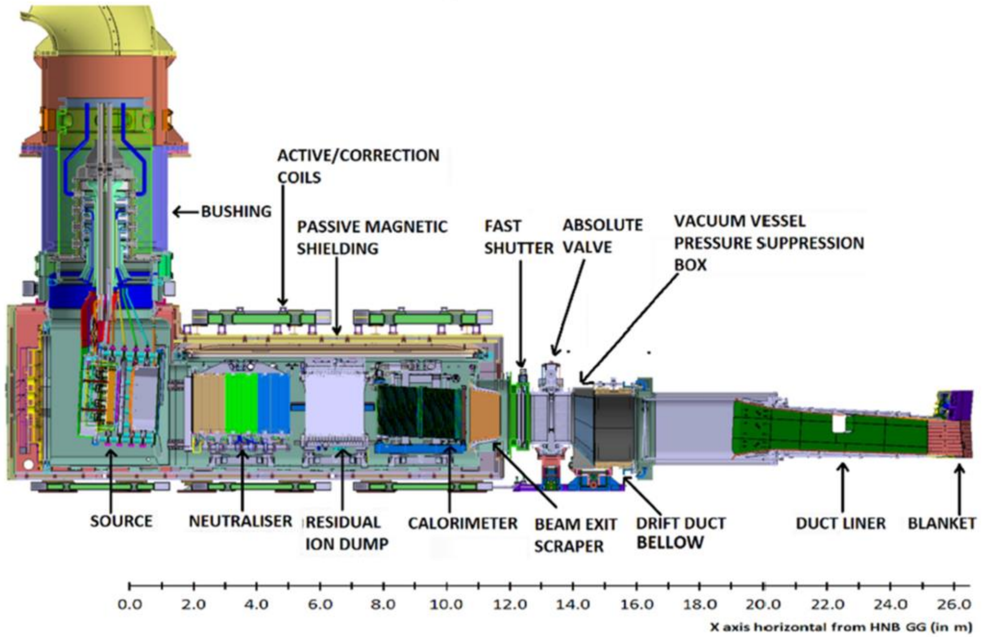


Fig. 4. CAD view of the ITER HNB.

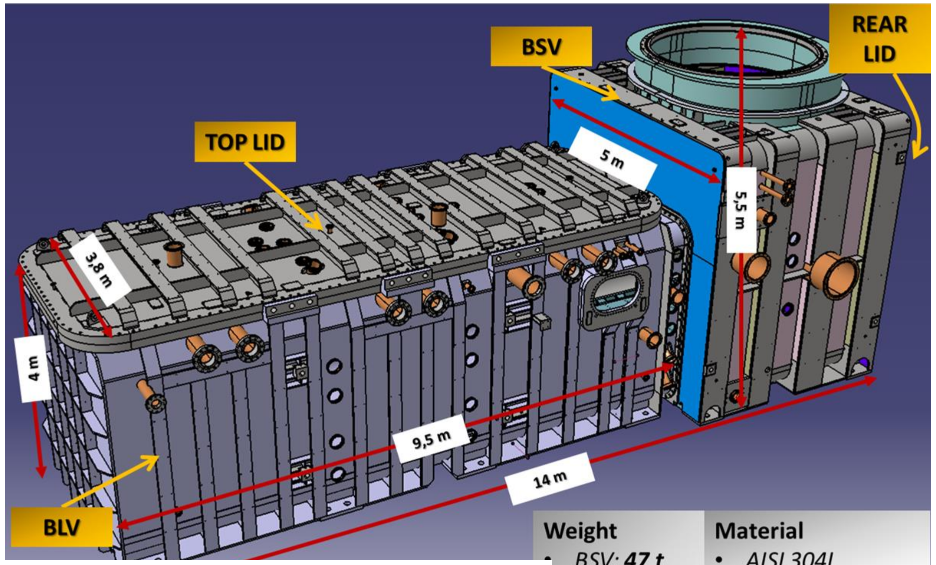
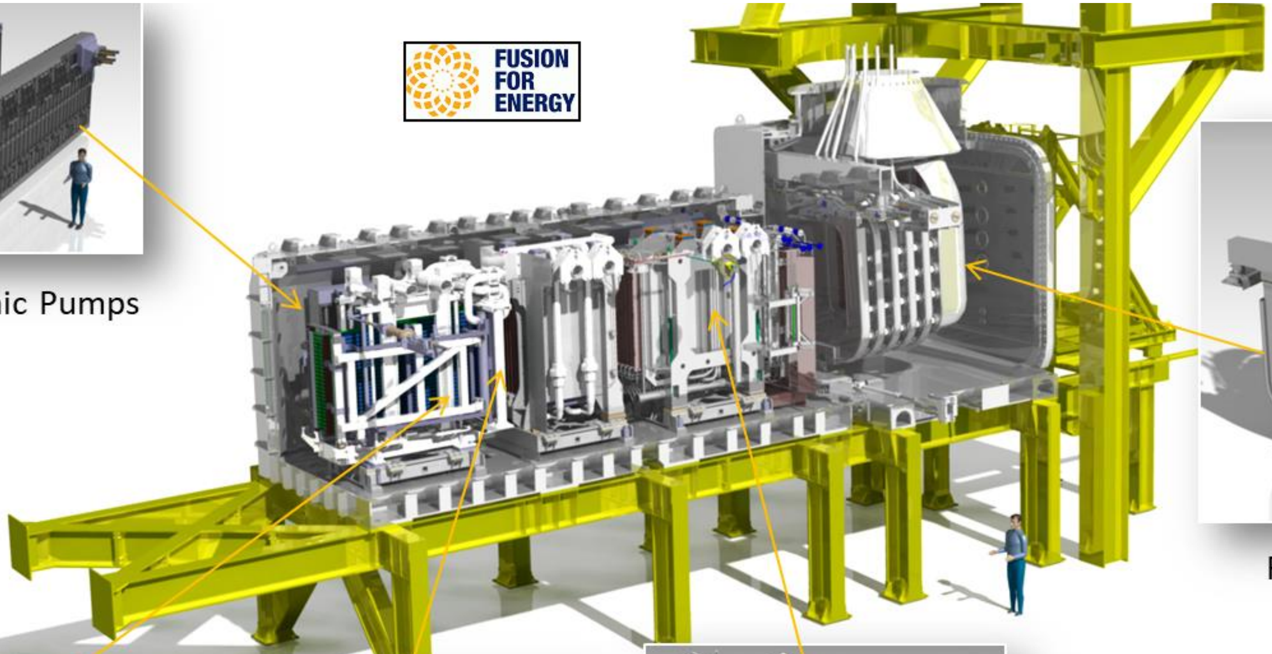


Fig. 5. CAD view of MITICA vacuum vessels.

Overview of MITICA Plant Systems (beam source and line)

Fig. 6. Cryogenic Pumps



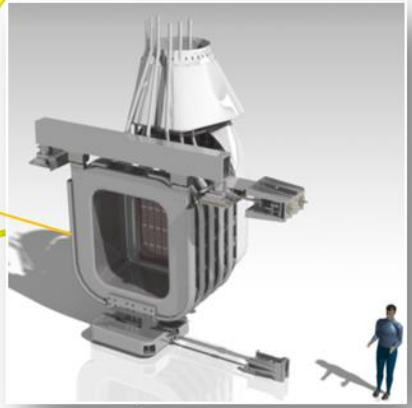


Fig. 9. Beam Source

Fig. 7. Calorimeter

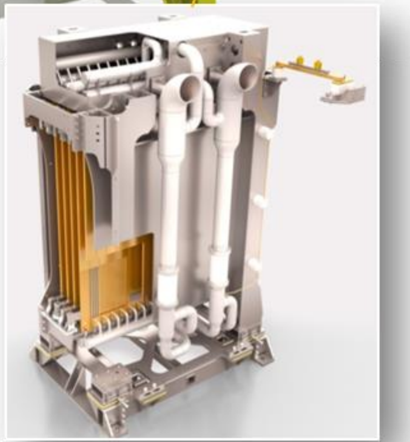


Fig. 7. Residual Ion Dump

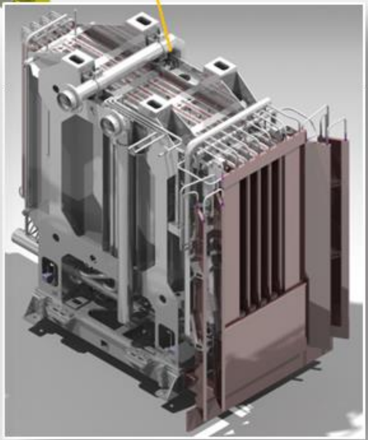


Fig. 8. Neutralizer

- **BS**: procurement started in 2018. Delivery end 2022
- **BLC:** Now mini-competition among three selected company is under preparation
- Signature of procurement contract is expected in Oct 2019

Overview of MITICA Plant Systems (power supply)

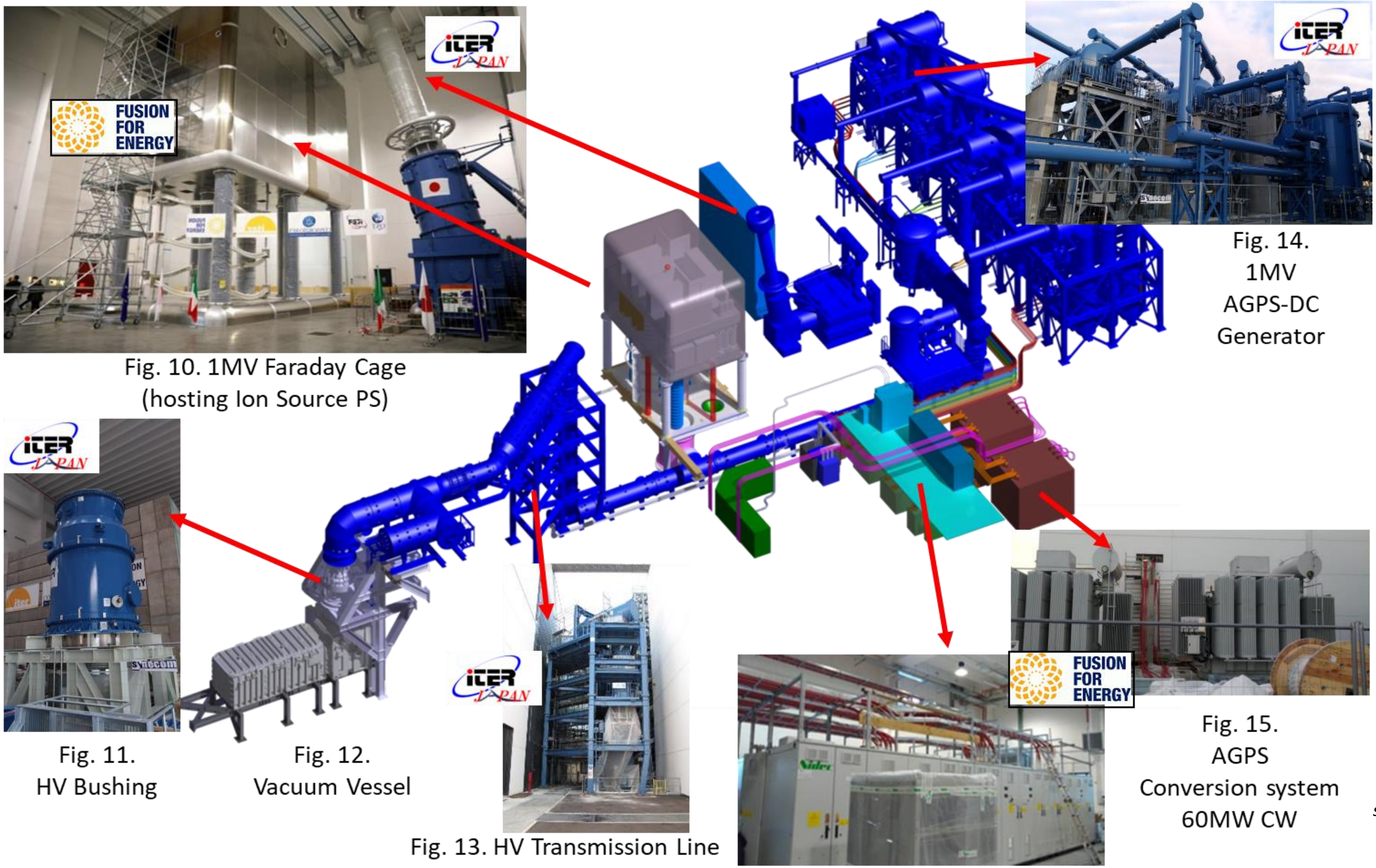


Fig. 10. 1MV Faraday Cage
(hosting Ion Source PS)

Fig. 14.
1MV
AGPS-DC
Generator

Fig. 11.
HV Bushing

Fig. 12.
Vacuum Vessel

Fig. 13. HV Transmission Line

Fig. 15.
AGPS
Conversion system
60MW CW

C
Ric

search

MITICA I&C - Architectural Constraints

- As for ITER I&C:
  - three tiers
  - two layers

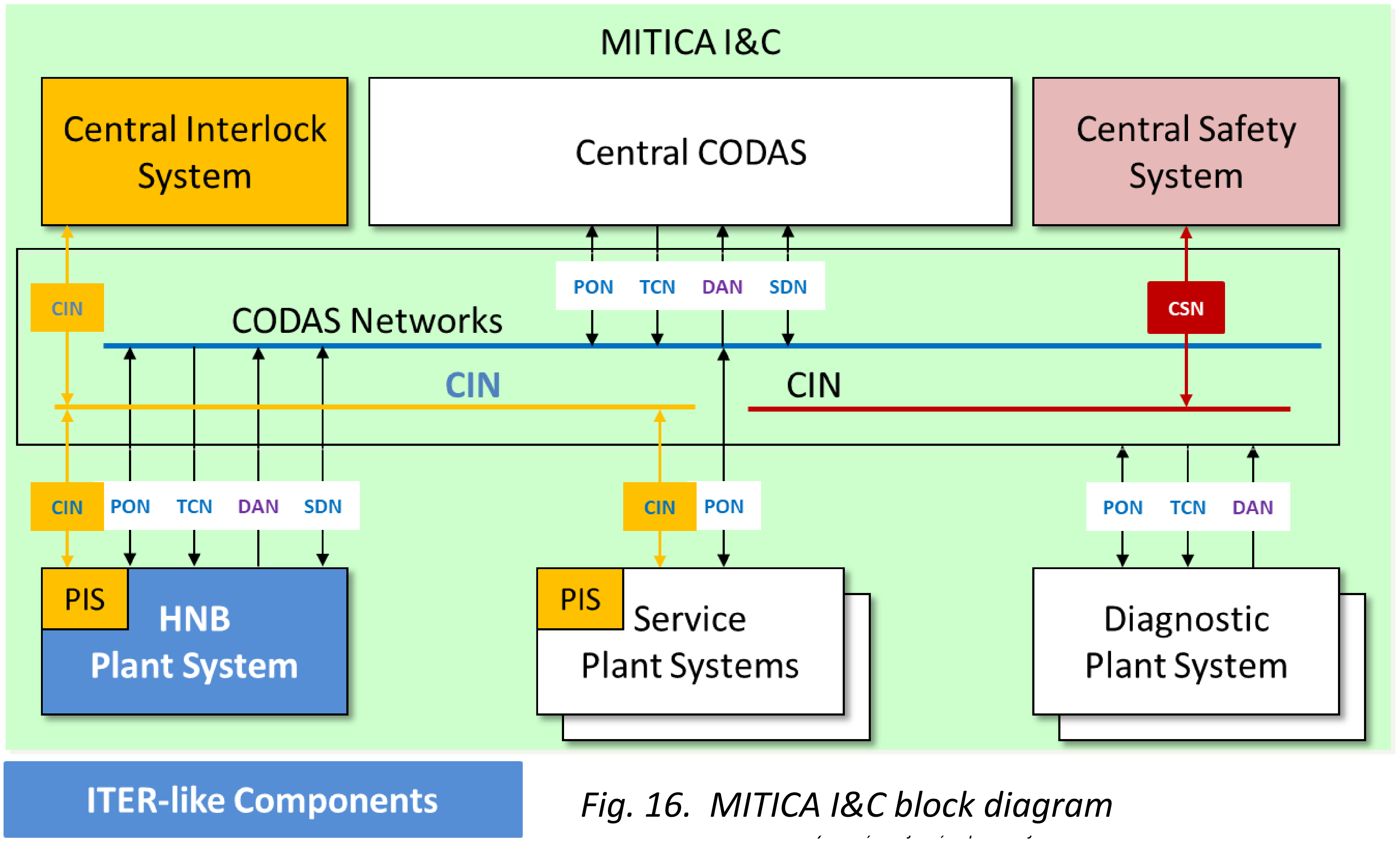


Fig. 16. MITICA I&C block diagram

MITICA I&C Architectural Constraints
HNB Plant System

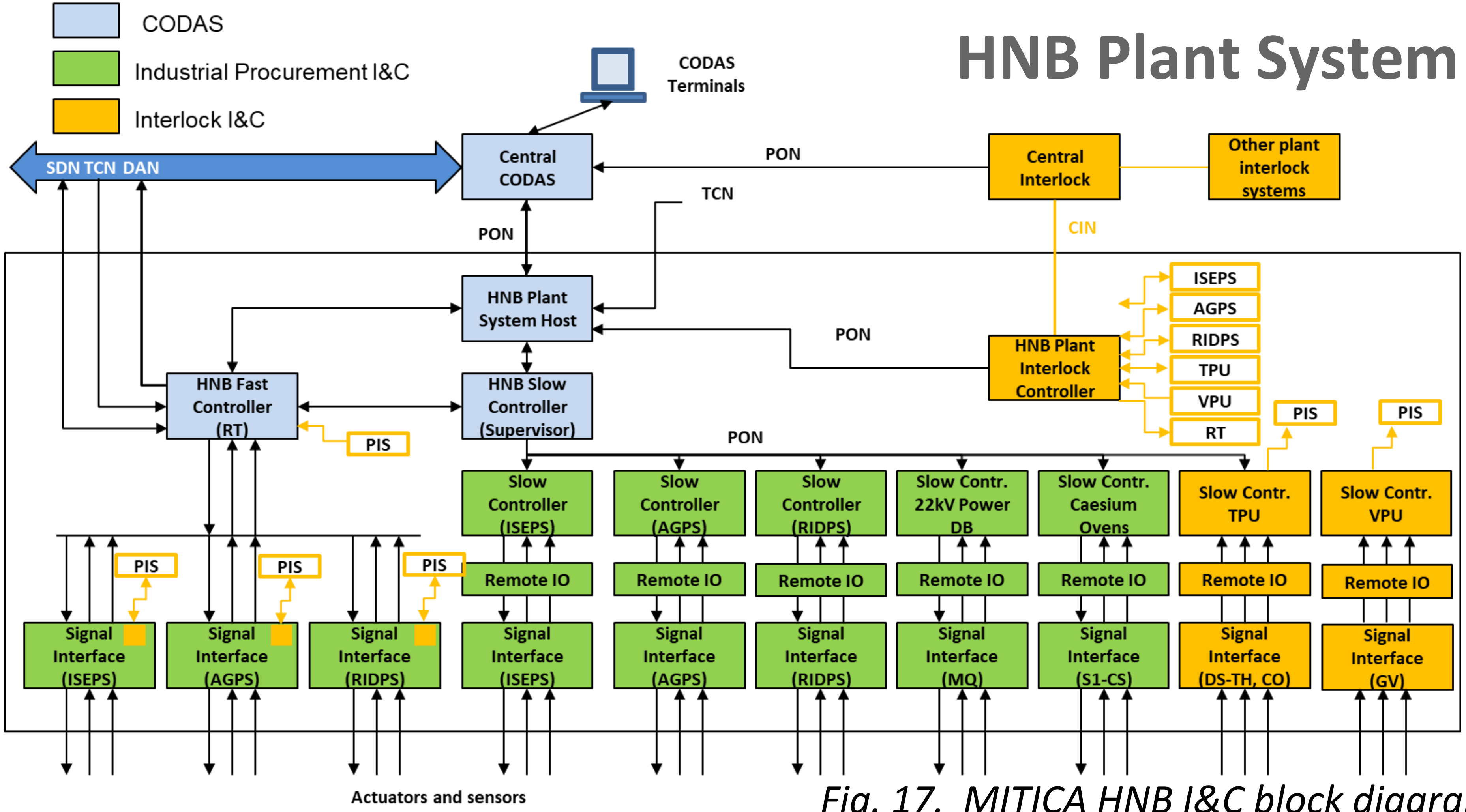


Fig. 17. MITICA HNB I&C block diagram

LEGEND

AGPS	Acceleration Grid Power Supply	PIS	Plant Interlock System	TCN	Time Communication Network
DAN	Data Archiving Network	PON	Plant Operation Network	TPU	Thermal Protection Unit
HNB	Heating Neutral Beam	RIDPS	Residual Ion Dump Power Supply	VPU	Vacuum Protection Unit
ISEPS	Ion Source Power Supply	SDN	Synchronous Databus Network		

CONSOR Ricerca Formazic

MITICA HNB Interlock – Functional Constraints - Fast Interlock

- Power supply protection
- 10 μs reaction time from fault detection to actuator commands
- Fiber-optics digital I/0 (about 40xI / 20xO)
- Pulse trains signals (safe, no signals on level)
- Breakdown management (next slide)

Fast Acquisition Unit

Fast Logic Solver

Optical Interface Unit

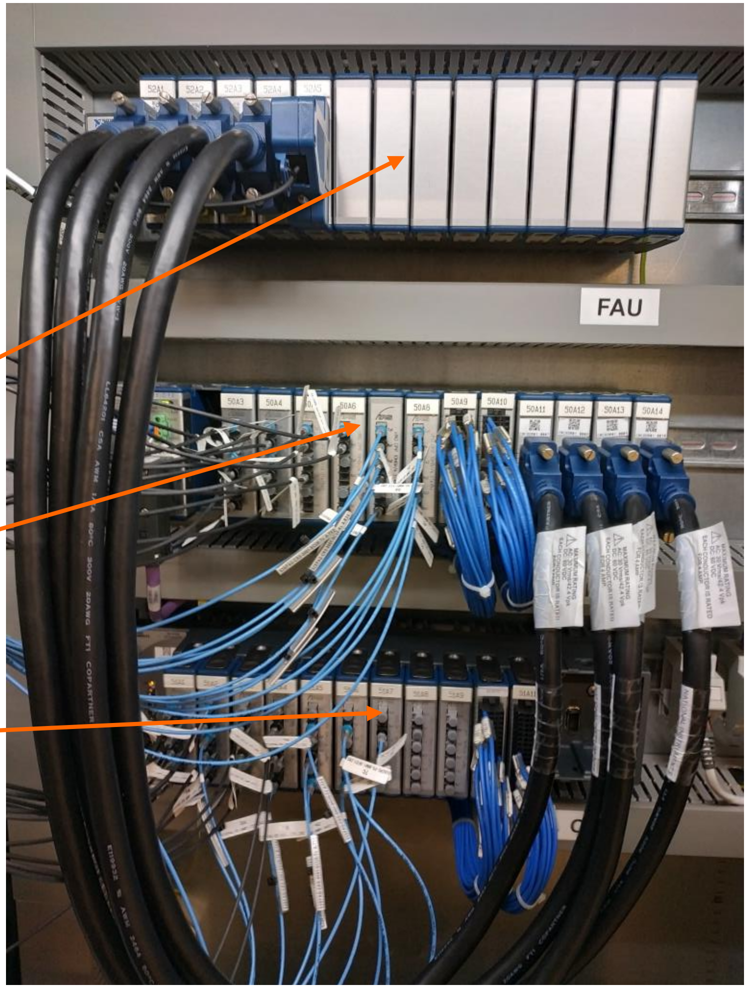


Fig. 18. Fast interlock prototype based on Compact RIO

MITICA Interlock – Functionality Constraints – Breakdown (BD) Management

- Flashover between grids or between grids and vessel
- Routine event due to grid high potential and short distances
- No real faults, but to be managed timely (<10 μs) to avoid damage
- Occurrence rate to be monitored and beam to be shut down in case of exceeding of a predefined threshold (<10 BD event/s)
- BD management is implemented in the MITICA HNB Interlock

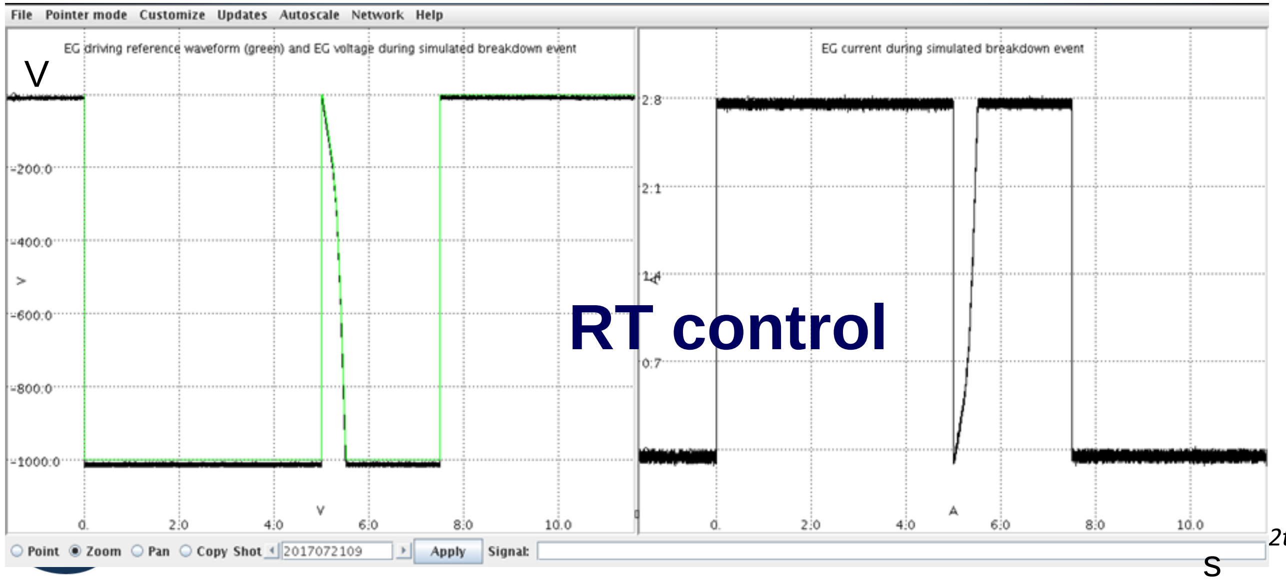


Fig. 19. Breakdown measurements

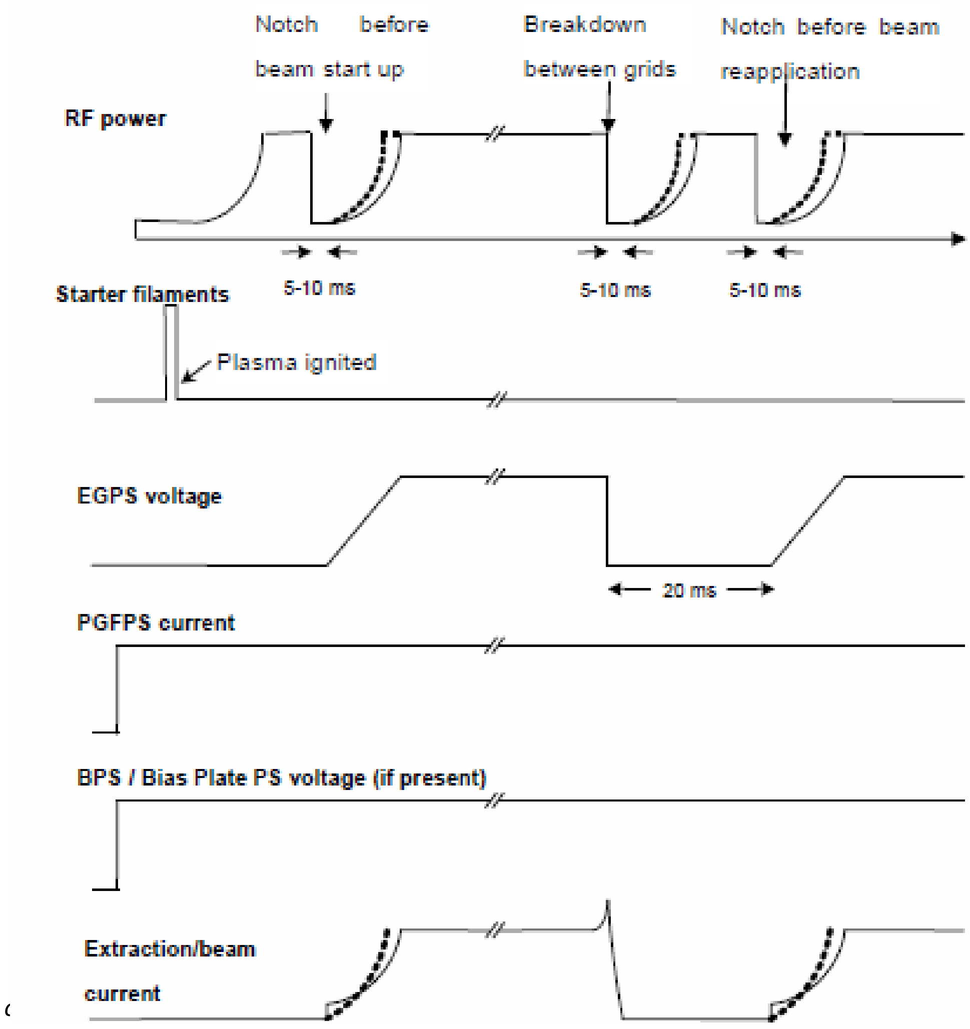


Fig. 20. Breakdown management

MITICA Interlock – Methodology Constraints - FMECA

- The Failure Mode, Effects, and Criticality Analysis (**FMECA) method** was considered. It is well codified and widely adopted in industry, electrical and nuclear plants.

- FMECA is a bottom-up analysis:
  - **System is divided into functional blocks**
  - **Failures are elementary functions lacking or out of specification**
  - **Each failure is recognized and evaluated for relevance**
  - **Actions to reduce/eliminate failures in design and production phases are proposed**

- A first FMECA analysis was developed in 2007 in the framework of the preliminary design of the NBTF facility. Another FMEA analysis was carried out for SPIDER in 2010.
- MITICA FMECA revised in 2017
- The present work proceeds from those analyses, adapting them to MITICA and taking advantage of the information gained and design advancements since then.

MITICA Interlock – Methodology Constraints - FMECA

What can go wrong?
-no function
-partial/over/degraded function
-intermittent function
-unintended function

How bad is it?

How often does it happen?

How good is the detection method?

What can be done?
-design changes
-process changes
-special controls
-changes to procedures ...

Reassessment after action deployment

Subsystem/Function

Potential failure modes

Potential failure effects

Failure severity (S)

Potential causes/mechanisms

Failure occurrence (F)

Current controls

Detectability (D)

Risk priority number

Recommended actions

Action results:
SxFxD
new risk priority number

What are the functions, features, requirements?

What are the effects?

What are the causes?

How can this be prevented & detected?

Provisional ranking =S×F×D

Final ranking less than provisional ranking (HOPEFULLY...)

ITER Risk Classification Severity and Frequency

Frequency	Category	Description	Indicative frequency level (per year)
	Frequent	Events which are very likely to occur in the facility during its lifetime	> 1
	Probable	Events that are likely to occur in the facility during its lifetime	$10^{-1} – 1$
	Occasional	Events which are possible and expected to occur in the facility during its lifetime	$10^{-2} – 10^{-1}$
	Remote	Events which are possible but not expected to occur in the facility during its lifetime	$10^{-3} – 10^{-2}$
	Improbable	Events which are unlikely to occur in the facility during its lifetime	$10^{-4} – 10^{-3}$
	Negligible	Events which are extremely unlikely to occur in the facility during its lifetime	$< 10^{-4}$

Consequence	Category	Injury to people	EURO Loss (Damage to equipment, decontamination)	Downtime (For the process)
	Catastrophic	Scales depend on the type of injury	$> 5 * 10^{7}$	> 6 months
	Major		$10^{6} – 5 * 10^{7}$	4 weeks to 6 months
	Severe		$10^{5} – 10^{6}$	3 days to 4 week
	Minor		$0 – 10^{5}$	< 3 days

CONSORZIO RFX Ricerca Formazione Innovazione

iter china eu india japan korea russia usa

FUSION FOR ENERGY

ITER Risk Classification – Classes

Risk Classes	Risk Class	Interpretation
	I	Intolerable risk
	II	Undesirable risk and tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained
	III	Tolerable risk if the cost of risk reduction would exceed the improvement gained
	IV	Negligible risk

Risk Classification	Frequency	F x C	Catastrophic	Major	Severe	Minor
		Frequent	I	I	I	III
		Probable	I	I	II	III
		Occasional	I	II	III	III
		Remote	II	III	III	IV
		Improbable	III	III	IV	IV
		Negligible / Not Credible	III	IV	IV	IV

MITICA Most Outstanding Failure Modes

RPN = Risk Priority Number

Item / Function	Potential Failure Mode	Potential Effect(s) of Failure	Severity	Potential Cause(s)/ Mechanism(s) of Failure	Occurrence	Current Machinery Controls Prevention	Current Machinery Controls Detection	Detection	RPN	Recommended Action(s)	ITER RISK Class
Electrical and Mechanical Interface			10	external water leakage from primary circuit	2	Margin in design	Flow measurements, Coolant pressure Measurement	7	140	Margin in design, Safety system detectors	II
			10	external coolant leakage from cryogenic circuit	2	Margin in design	Flow measurements, Coolant pressure Measurement	7	140	Margin in design, Safety system detectors	II
		Absent or incorrect power supply; loss of signals; loss of electrical insulation	7	Short in HV bushing	5	Margin in design and tests	Electric measurements, diagnostics	7	245	Fail safe design of electrical measurements	II
Assuring vacuum tightness	Water Leakage inside vessel	pressure out of range; presence of water vapour; increased probability of breakdown; freezing of coolant inside components;	8	Water leakage from accelerator grids	5	Leakage tests with cryopump OFF	Pressure measurements, RGA	8	320	Margin in design, redundancy and high speed on Pressure Measurements	I
			8	Water leakage from beam line components	5	Leakage tests with cryopump OFF	Pressure measurements, RGA	8	320	Margin in design, redundancy and high speed on Pressure Measurements	I
	Gas (N2 H2 D2 He) leakage inside vessel	pressure out of range; increased probability of breakdown; Presence of flammable and toxic gas outside vessel;	7	Air Leakage from vessel flanges or windows	5	Leakage tests with cryopump OFF	Pressure measurements, RGA	7	245	Fail safe design, redundancy an high speed on Pressure Measurements, real time RGA measurements	II
Producing negative ions	Non uniform distribution	Beam out specification; overload/damage on subsequent components due to electrons	7	malfunction of magnetic PG filter	5		electrical measurements	7	245	periodical check of magnets	II
Extraction of negative ions			8	Short-circuit between EG and PG	5	Overvoltage protections, Breakdown Detector	ISEPS voltage measurements	6	240	Margin in design	I
Acceleration and focussing of negative ions	Incorrect acceleration/focusing	Beam out of specification; perveance mismatch; damage to subsequent components	7	Deformation or misalignment on grids	5		GG temperature measurements, Beam Spectroscopy	7	245	periodic inspection	II
Providing protection against grid breakdown	Loss of protection capability	Increased damage of acceleration grids; decrease of vacuum insulation capabilities	7	Short in grounded grid dumpers	5	Margin in design and tests	Fast Electric measurements	7	245	Fail safe design and Redundancy on Fast Electric Measurements	II

MITICA Interlock – Methodology Constraints
Safety Instrumented Functions - SIL (IEC61508) Allocation

Protection Instrumented Function: Shut down of power supply AGPS and ISEPS

IP Category	Minimum ITER Interlock Integrity Level	Equivalent SIL	I&C Implementation
Catastrophic Category 1	3IL-4	SIL-3	High integrity interlock with diversity (e.g. PLC + hardwired I&C)
Major Category 2	3IL-3	SIL-3	High integrity interlock
Severe Category 3	3IL-2	SIL-2	Low integrity interlock
Minor Category 4	3IL-1 (no interlock)	SIL-1	Conventional Control (no interlock)

SIL – Safety Integrity level (IEC 61508)

3IL - ITER Interlock Integrity Level

- **Protection Instrumented functions definition and 3IL allocation still ongoing**
  - The main difficulty is the lack of certified hardware, in particular sensors for fault detection, which in many cases were custom developed for the NBTF.

MITICA Interlock – Technological Constraints – Slow Interlock – Standard Industrial Solution

- **Component selection postponed – technology evolving**
- **Standard Siemens technology**
- **Ready-off-the-shelf solutions exist up to SIL3 – included in ITER PCDH**
  - **Siemens S7-400FH – Fail safe, high availability (redundant)**
    - **Tools for safety programming: F Systems programming, Safety matrix Tool, Continuous Function Chart (CFC) blocks – certified IEC 61508**
  - **Profibus ET200M – PROFIsafe**
  - **S7-400FH and Profibus: ageing components**
- **Updated Siemens technology – SIL3 – Included in ITER PCDH**
  - **Siemens S7-1516F (F or H available, FH near future?)**
  - **Profinet (ET200SP, F-DI – F-DQ, very good distributed I/O, simplified cabling, limited size, but high power consumption) – PROFIsafe**
  - **Restricted tools for safety programming - Safety Advanced**

- **WinCC-OA SCADA**
  - **NEWS - WinCC-OA equipped with PROFIsafe profile (certificate Jan. 2019)**
  - **NEWS - SIL3 (WinCC-OA Certificate re-emitted, March. 2019)**

MITICA Interlock – Technological Constraints – Fast Interlock

- **Ready-off-the-shelf solutions exist – ITER PCDH**
  - **NI CompactRIO**
    - **Very useful optical I/O modules (IRS) – no ITER catalog**
    - **10 or 20 Mbit/s, 3xin/3xOUT or 2xIN/2xOUT channels**
  - **FPGA on board**
  - **LabView FPGA programming**
    - **No control on executable**
  - **HDL integration possible**

Fig. 21. IRS optical IO module

MITICA Interlock – Technological Constraints
SPIDER Interlock as MITICA HNB Prototype

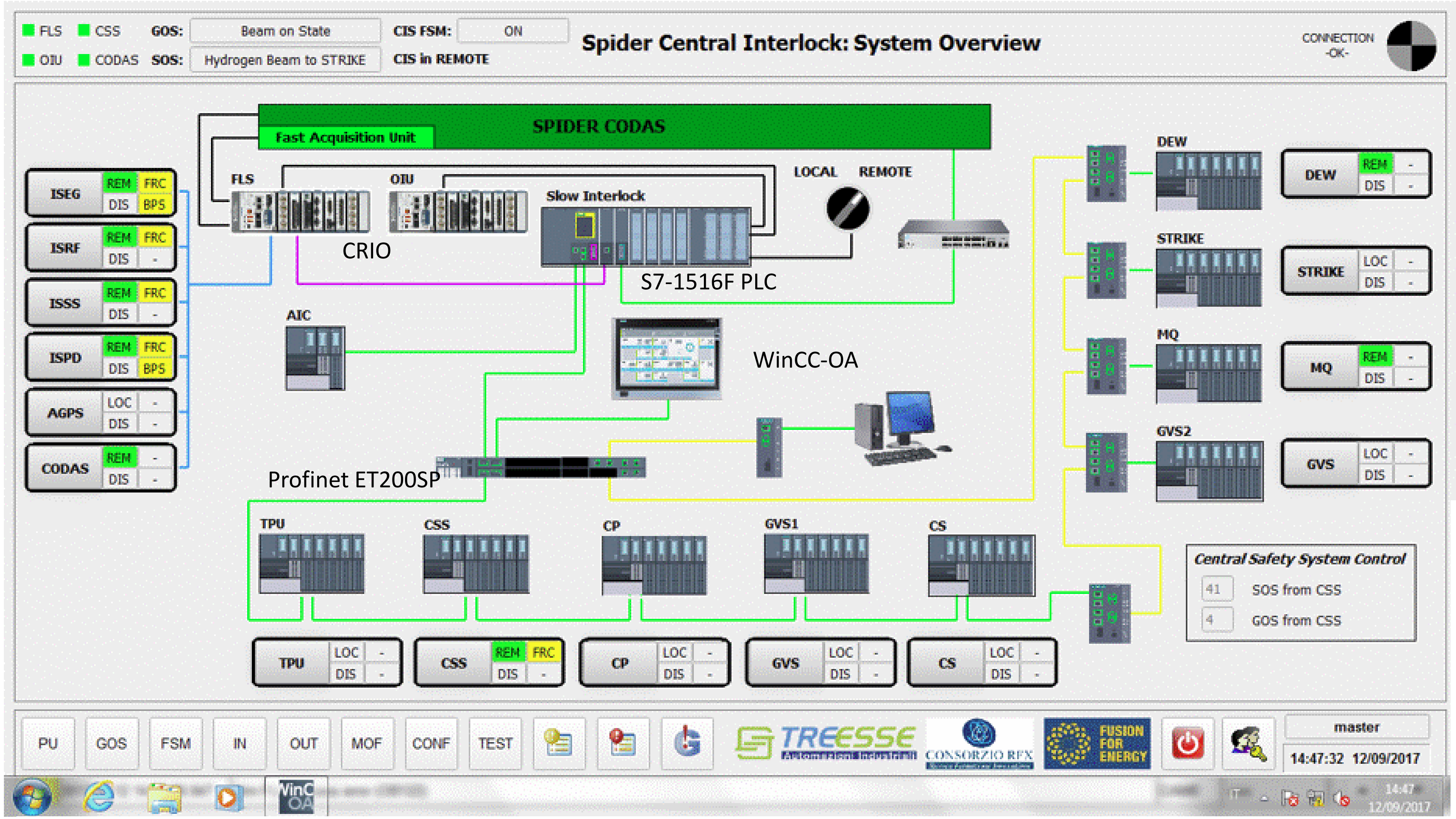


Fig. 22. SPIDER Interlock.

SPIDER inauguration in June 2018

MITICA Interlock – Short-term Solution for Power Supply Integration

- **MITICA operation planned for 2023**
- **MITICA Power Supply Integration planned for Q2 2020**
- **No Time and manpower to develop complete, sound solution**
  - NBTF safety system under construction in parallel
  - SPIDER Operation in parallel
  - MITICA CODAS development in parallel
- **No advantage to anticipate final solution**
  - Start of MITICA Operation expected in 2023

- **Solution: Clone of SPIDER Central Interlock (fast and slow)**
  - Same hardware (S7-1516F, profinet ET200SP, WinCC-OA, CompactRIO)
  - Minimal software/firmware modifications (state vs pulse train signals)
  - Affordable cost (~100 MEuro)
  - Reasonable compromise

Summary

- Design of MITICA Interlock is progressing in parallel with the procurement of MITICA main components
- High level I&C architecture has been defined
- Fault analysis has been carried out
- Protection functions and SIL allocation still ongoing
- HW Component selection is postponed to take advantage of technology evolution
- Temporary solution to manage MITICA power supply integration have been identified
    - Clone of SPIDER Central Interlock

Thank you very much