CERN

Test Benches for PLC Based Systems

Testing of Safety Functions

ESS - 29/30 August 2013

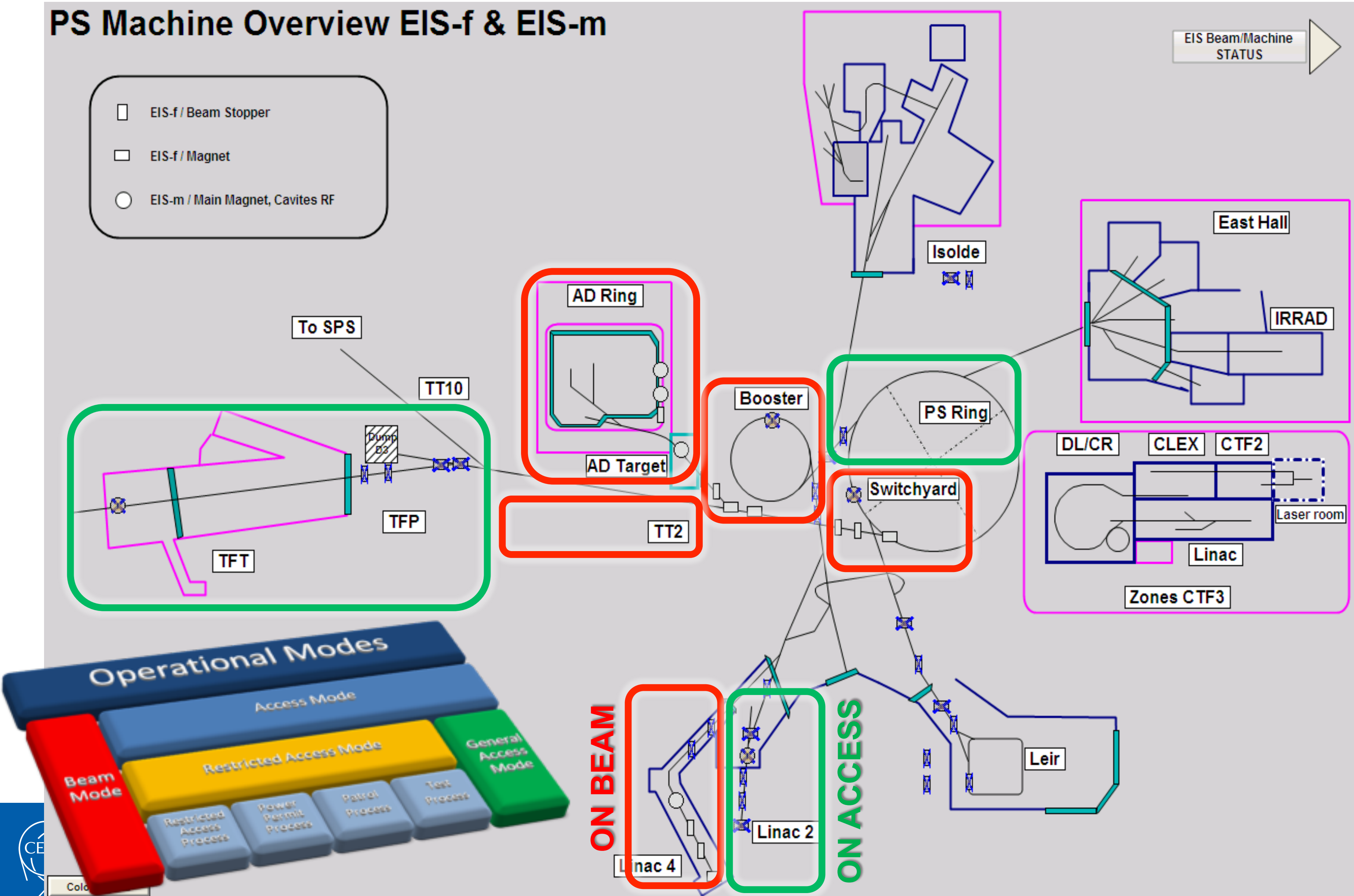
Authors: P. Ninin, F. Valentini

Outline

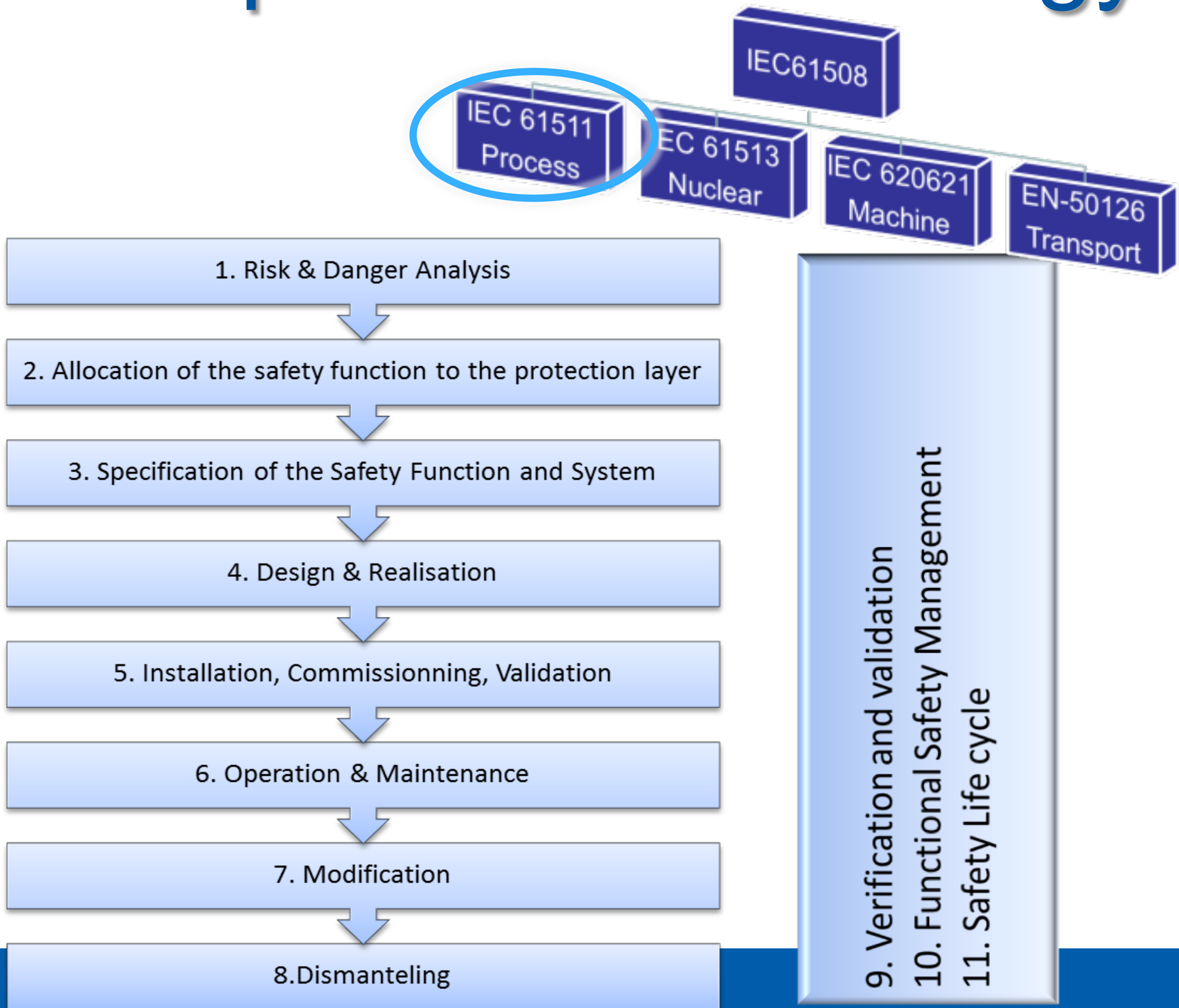
The return of experience of CERN in the development and validation of Safety Personnel Protection Systems showed us that the realization of a performing Test Platform is essential to ensure the quality of the Verification and Validation activities. However the adoption of a Formal Language for the specification of the Safety Functions in another essential Key.

- PS-PPS Project Scope
- Development Methodology / Normative Context
- Safety Test Bench Conception
- Safety Functions – Formal Definition Language
- Major Advantages for Verification & Validation
- Conclusions

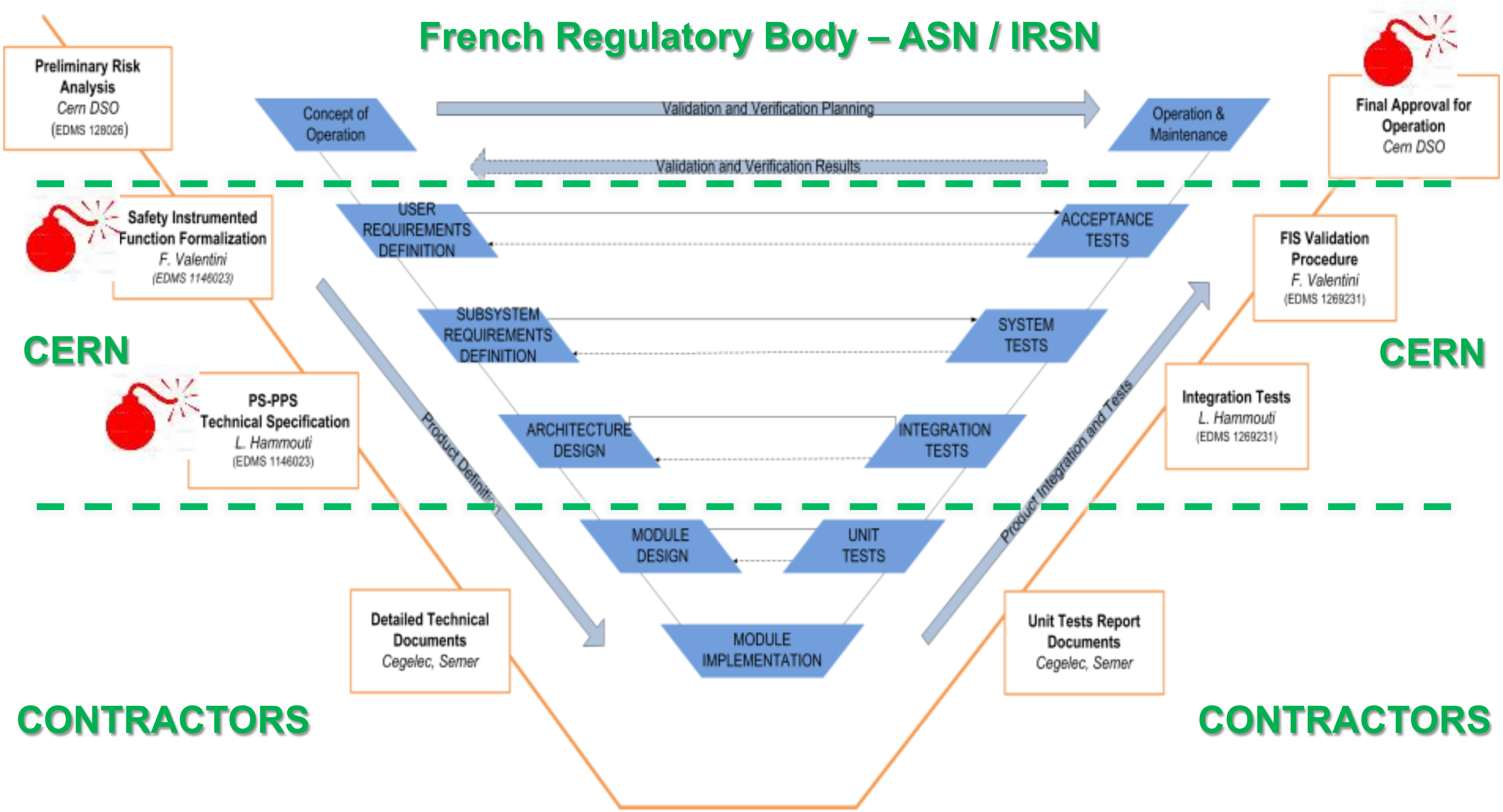
PS-PPS Project Scope



Development Methodology

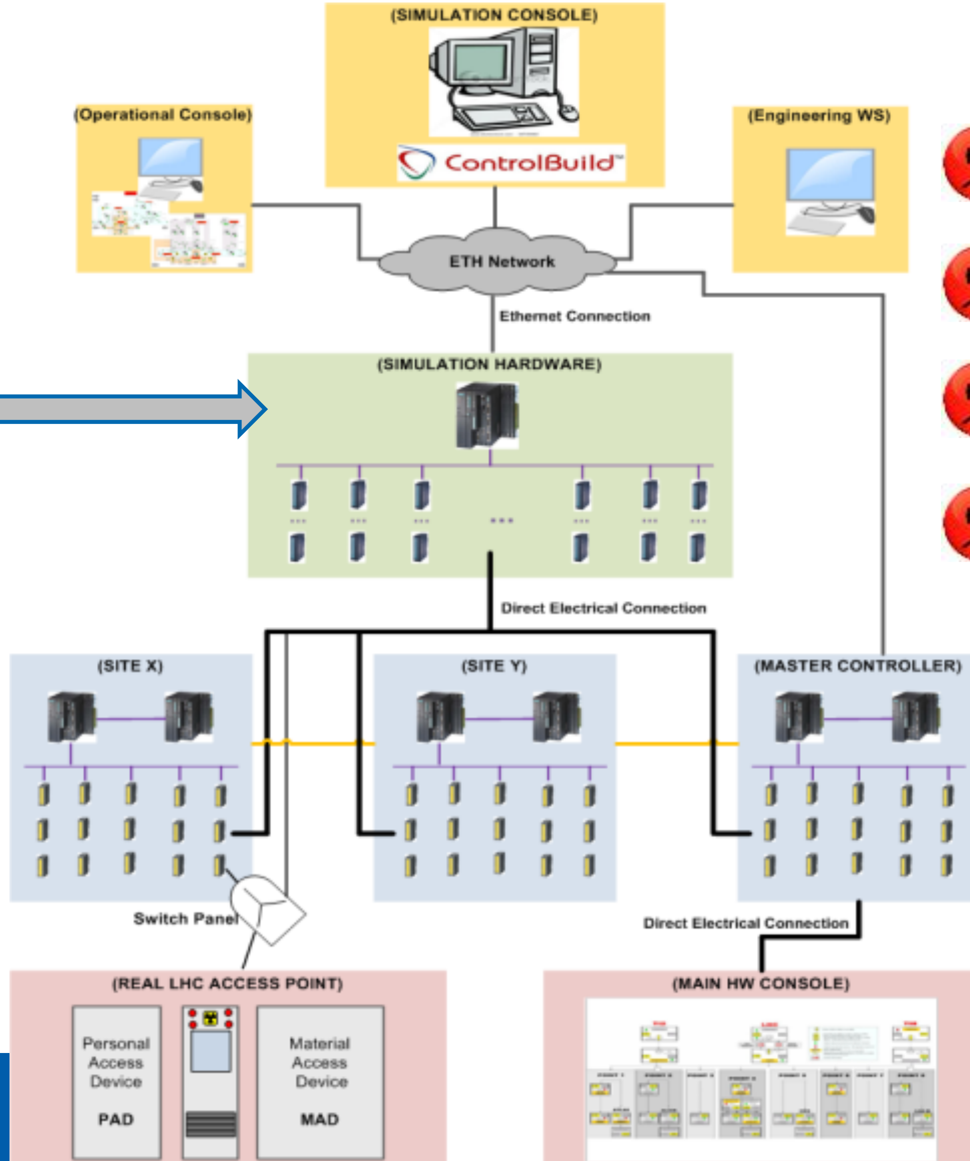


Development Methodology



Safety Test Bench Conception

Classic Architectural Model Example



- Low Scalability / Flexibility
- Simulation Constraints
- Hard integration of real equipment
- Platform reconfiguration complex and time consuming

Safety Test Bench Conception

FIRST STEP: Clear fixing of the Platform objectives!!

Safety

1. **Validate Safety Software of each local controller.**
2. **Validate safety communication between local controllers (min. 3).**

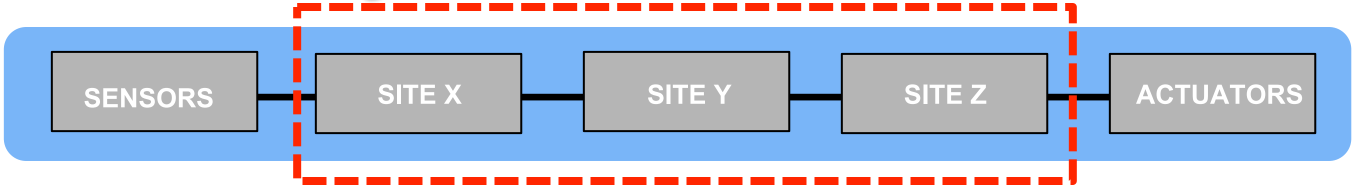
Operation

3. **Validate all operational synoptics.**
4. **Integrate real access devices (PAD/MAD) within the simulated signals.**

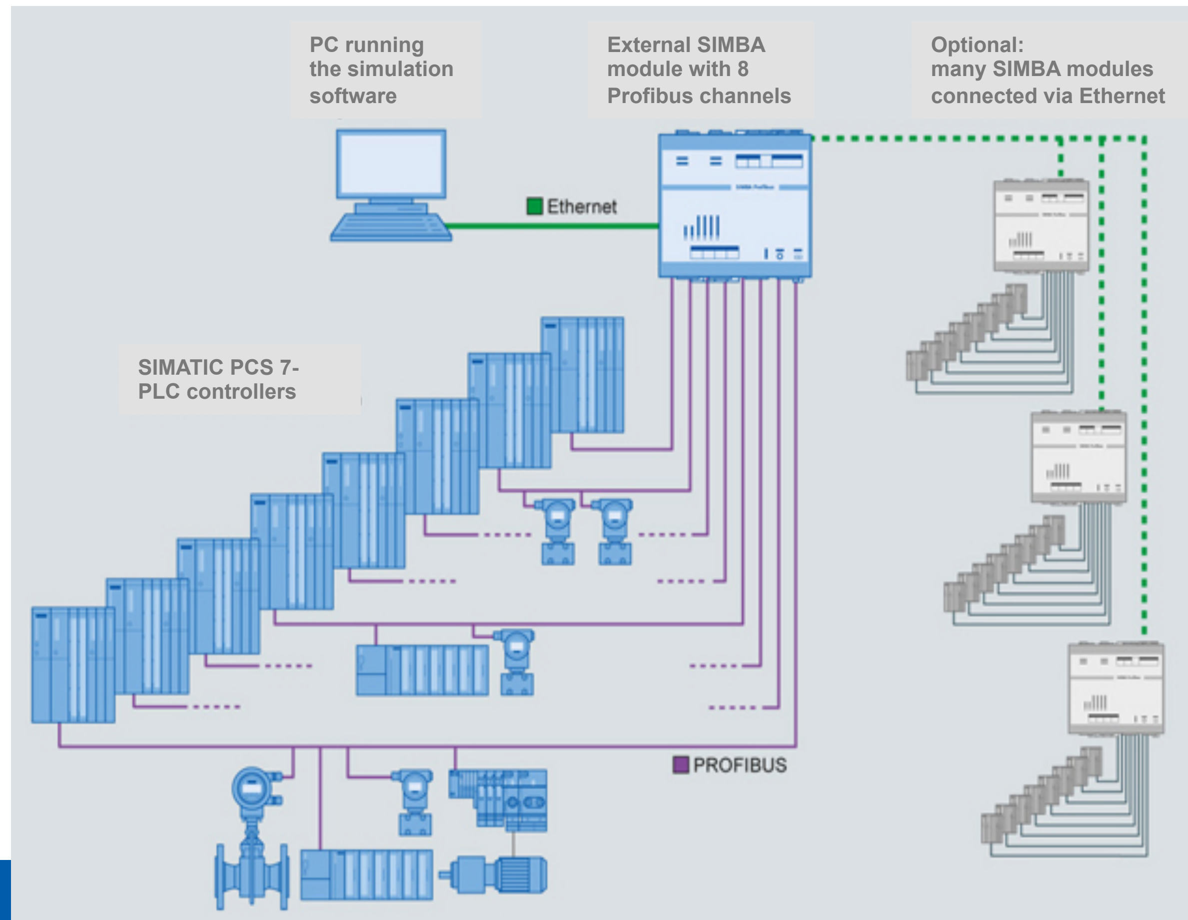
USABILITY

5. **Quick reconfiguration of the Platform (max. 2h to load new PS sites).**
6. **Quick modification of Platform architecture** ***(ADD/REMOVE access devices).***
7. **Be able to run automatic test case scenarios.**

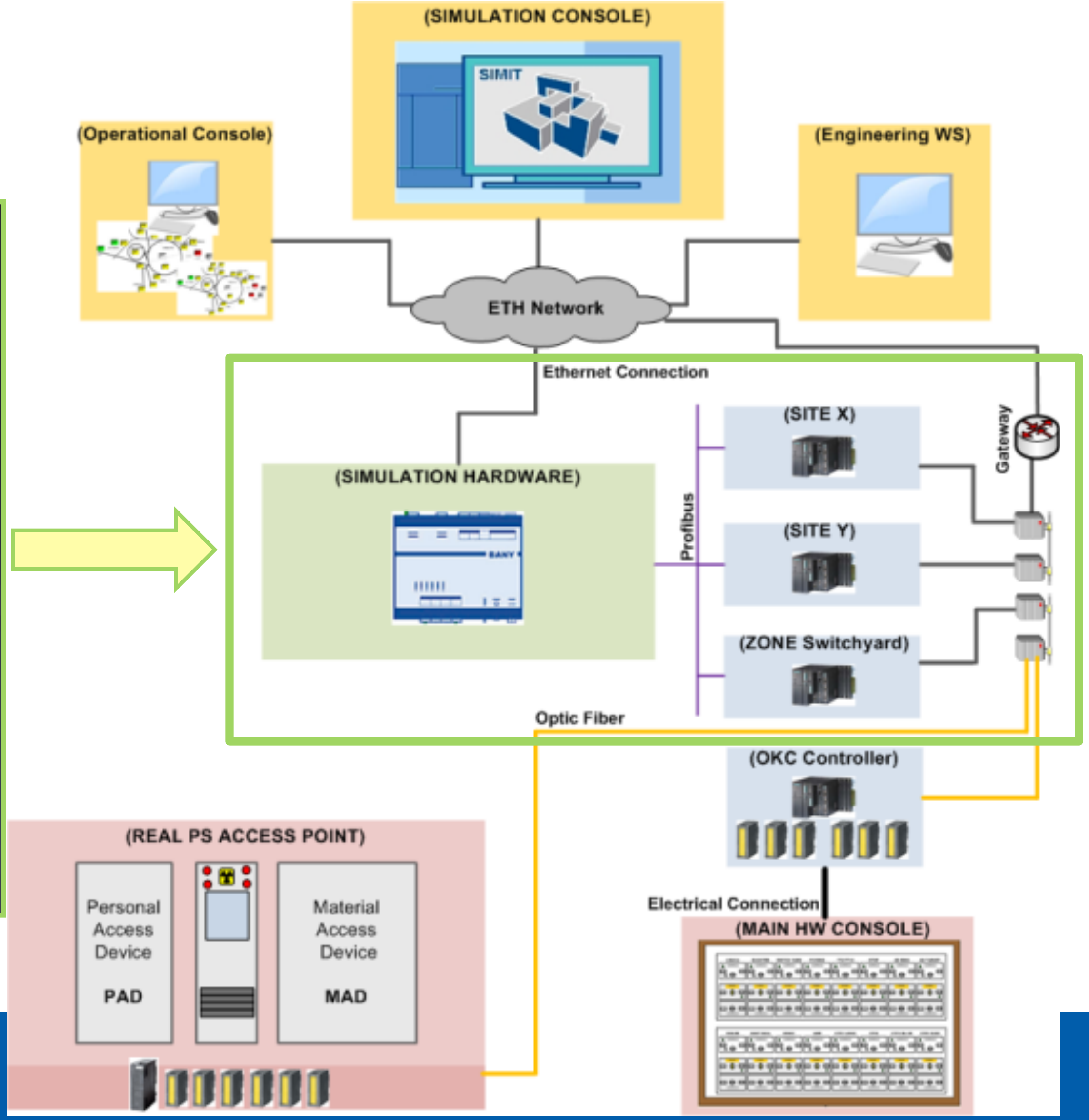
Safety Test Bench Conception



SIEMENS SIMBA Box



Safety Test Bench Conception



FIS – Formal Definition Language

Main Objective: *Specify each FIS in a 3 sections structure*

SECTION 1: FIS Informal Presentation

FIS CODE	SIL TARGET	OPERATING MODE	PROBABILITY	REDUNDANCY
FIS_1	SIL3	CONTINUOUS	PFH	1oo2

MITIGATED HAZARDS: Exposition to radiations coming from injected/circulating beam, activated materials or radiation coming from a source (LINAC4). Other risks covered are related to the exposition to X-Rays from RF cavities, SEPTA Electrostatic Magnets (PS RING and BOOSTER), working KLISTRONS or Deflecting Cavities (CTF3-DL-CR).

Exposition Conditions: unintended start of the Beam. Intrusion during Beam operations.

SAFETY ACTIONS: Computation of REPLI Mode (NO ACCESS/NO BEAM) of the ZIV.
Activation of Evacuation Sirens.
Sending of protection requests to all Upstream ZIVs.
Computation of the Safe State signal (SECU_OK) for all Downstream ZIVs.

GENERAL DESCRIPTION: The function main scope is to ensure that **NO Beam** is permitted when the Access mode is set and **NO Access** is granted when Beam is allowed in the ZIV. In case of loss of this invariant condition (ex. intrusion during beam mode or loss of the Safe state of at least 1 *EIS beam* during access) the function disables the current exploitation mode and activates the REPLI MODE (No Access – No Beam) described by the **FIS_17**.

During the REPLI MODE, the Function asks to all upstream ZIVs to put in SAFE state all their *EIS_b* if at least 1 *EIS_b* of the ZIV is in an UNSAFE position.
The Function starts the EVACUATION sirens if at least 2 *EIS_b* are in an UNSAFE position.

Additionally, this FIS computes continuously the signal SECU_OK sent to all downstream zones to inform that all the EIS-beams of the ZIV are SAFE.

Logic Solver Technology:	*Safety PLC Wired System*	**Reaction Time:**	*2s*	**Spurious Trip Frequency:**	*< 1/year*
Failsafe Behavior:	*Application of REPLI Mode for the ZIV.*	**By-pass needs:**	*FIS_2*	**Periodical Tests frequency:**	*1/year*

FIS – Formal Definition Language

Main Objective: *Specify each FIS in a 3 sections structure*

SECTION 2: FIS Input / Output Interface

3.1.1 FIS INPUT SIGNALS

VARIABLE	SIGNAL	SOURCE	PLC Type
EISa_Safe	Position (SAFE/UNSAFE) resultant for all EIS-access of the ZIV. Refer to the specific definition of SAFE/UNSAFE state given for the different models of EIS-A: **EISa_Safe=0** → 1 EISa is UNSAFE	2 Mechanical switches	FDI
EISb_Pos	Position of all EIS-beam of the ZIV: **EISb_Pos=1** → All EIS-beam are SAFE	2 Mechanical switches	FDI
KEY_Out	Position of all keys used to put out of chain the Downstream ZIVs. **KEY_Out=1** → The ZIV is out of chain	2 Micro-switches	FDI
MODE_Bea	The Beam mode status of the ZIV: **MODE_Bea=1** → ZIV in BEAM ON	Network (OKC PLC)	INT VAR
MODE_Acc	The Access mode status for the ZIV: **MODE_Acc=1** → ZIV in ACCESS ON	Network (OKC PLC)	INT VAR
MODE_Tra	Status of TRANSITION RFA/RFB Mode: **MODE_Tra=1** → ZIV in RFA/RFB Mode	Network (OKC PLC)	INT VAR
MODE_TFA	Status of TRANSITION FROM ACCESS Mode: **MODE_TFA=1** → ZIV in TFA mode	Program	INT VAR
ACCE_Tst	Status of the mode TEST EIS-b for the ZIV: **ACCE_Tst=1** → TEST mode authorized	Program	INT VAR
ACCE_TfT	Status of the mode TFT for the ZIV: **ACCE_TfT=1** → TFT Mode activated	Program	INT VAR
SECU_Dwn	Request from downstream ZIV for setting all EIS-b of the ZIV in a SAFE state: **SECU_Dwn=0** → Safety requested	Cabled signal from downstream PLC	FDI
ZIV_Srch	Search state for the ZIV: **ZIV_Srch=1** → ZIV Search is Armed	Program	INT VAR

3.1.2 FIS Output Signals

VARIABLE	SIGNAL	SOURCE	PLC Type
MODE_Rep	The REPLI mode status for the ZIV: **MODE_Rep=1** → ZIV in REPLI Mode	PLC Program	INT VAR
EVAC_Cmd	Command to the BIW system to start the Evacuation sirens: **EVAC_Cmd=1** → Evacuation activated	PLC output	FDO
SECU_Ok	Signal sent to all downstream ZONES to inform that all EIS beam of the ZIV are safe: **SECU_Ok=1** → All EIS-beam are SAFE	PLC output	FDO
SECU_UP	Signal sent to all upstream Zones to ask them to put in SAFE state their EIS beam: **SECU_Up=0** → Safety Request activated	PLC output	FDO

FIS – Formal Definition Language

Main Objective: *Specify each FIS in a 3 sections structure*

SECTION 3: FIS Formal Description

TRIGGERING EVENT- ACTIVATION OF THE REPLI MODE FOR THE ZIV:

((MODE_Acc = **1** V MODE_TFA = **1** V MODE_Tra = **1**) Λ ACC_Tst = **0** Λ ACC_TfT = **0** Λ EISb_Pos = **0**) V
(MODE_Acc = **0** Λ EISa_Safe = **0**)

OUTPUT → **MODE_Rep** = 1

TRIGGERING EVENT- ACTIVATION OF THE EVACUATION SIREN FOR THE ZIV:

((MODE_Bea = **1** V MODE_TFB = **1**) Λ ZIV_Srch = **0**) V
(MODE_Rep = **1** Λ EISb_Pos{>1} = **0** Λ EISa_Safe = **0**)

PLC OUTPUT → **EVAC_Cmd** = 1

TRIGGERING EVENT- PROTECTION REQUEST TO ALL THE UPSTREAM ZONES:

(MODE_Rep = **1** Λ EISb_Pos = **0** Λ EISa_Safe = **0**)

PLC OUTPUT → **SECU_Up** = 0

TRIGGERING EVENT- ZIV SAFE STATE SENT TO ALL DOWNSTREAM ZONES:

(EISb_Pos = **1** Λ MODE_Bea = **0**) V (ACC_Tst = **1**) V (ACC_TFT = **1**)

PLC OUTPUT → **SECU_Ok** = 1

Major Advantages

- Simplify communication with the contractors by eliminating many possible sources of ambiguity.
- Simplify the access to the information.
- Production of explicit Formal Proofs of Correctness. Ex via the application of Logic Solvers to the system of Boolean equations.
- **Improve the definition and the quality of the final FIS Validation Test Plan.**

Major Advantages – FIS Validation

PROBLEM: *Validate efficiently all Safety Interlock Functions of the new CERN Personnel Protection System of PS accelerators in order to discover all major bugs before the deployment phase.*

OBJECTIVES:

- Define an Algorithm and a Test Criterion to derive all possible **relevant** tests for a given FIS.
- Perform all needed tests in a reasonable time.
- Demonstrate/Measure the Test Coverage obtained.

TESTING STRATEGY

- **Test Criterion:** *Verify the output values for all possible events triggering the FIS interlock actions.*
- **Test Generation Algorithm:** $T = \{t \mid \varphi(t) = true\}$
- **Test Coverage Proof:** *<# Executed Tests> / <# Total Tests>*

Major Advantages – FIS Validation

FIS CODE	TEST CASE SCENARIO	CATEGORY
FIS_1	ACTIVATION OF THE REPLI MODE FOR THE ZIV	SAFETY

1 — **TEST CASE MODEL:**

$$\Phi\_1\_1 = ((\mathrm{MODE\_Acc} = 1 \lor \mathrm{MODE\_TFA} = 1 \lor \mathrm{MODE\_Tra} = 1) \land \mathrm{ACC\_Tst} = 0 \land \mathrm{ACC\_TfT} = 0 \land \mathrm{EISb\_Pos} = 0) \lor (\mathrm{MODE\_Acc} = 0 \land \mathrm{EISa\_Safe} = 0)$$

2 — **TEST CASE RESTRICTIONS:**

$R_1 = (\mathrm{MODE\_Acc}=1 \land \mathrm{MODE\_TFA}=1) \lor (\mathrm{MODE\_Acc}=1 \land \mathrm{MODE\_Tra} = 1) \lor (\mathrm{MODE\_TFA}=1 \land \mathrm{MODE\_Tra} = 1)$

$R_2 = (\mathrm{ACC\_Tst}=1 \land \mathrm{ACC\_TfT}=1)$

$R_3 = (\mathrm{MODE\_Acc}=0) \land (\mathrm{ACC\_Tst}=1 \lor \mathrm{ACC\_TfT}=1)$

3 — **TEST CASE GENERATION MODEL:**

$$(\Phi\_1\_1 = 1) \land (R_1 = 0) \land (R_2 = 0) \land (R_3 = 0)$$

4 — **SYSTEM VERIFICATION PROPERTY:**

$$(\mathrm{MODE\_Rep} = 1)$$

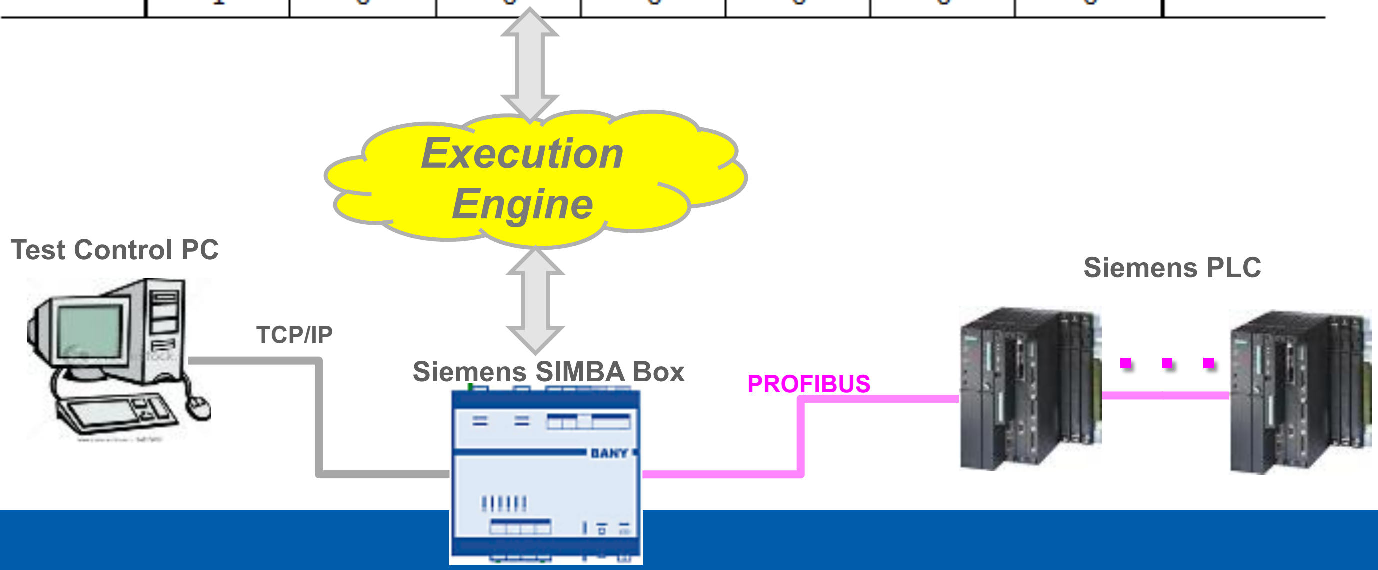
Total Variables:	*7*	**Total State Space:**	*128*	**Scenario State Space:**	*10*
I/O Types:	*DIGITAL*	**Test Impact:**	*PLC ZIVx* *PLC OKC*	**Execution Strategy:**	*MANUAL*

Major Advantages – FIS Validation

Test Instances auto-generated by MATLAB:

	MODE_Acc	MODE_TFA	MODE_Tra	ACC_Tst	ACC_TfT	EISb_Pos	EISa_Safe	RESULTS
Test 1	0	0	0	0	0	1	0	
Test 2	0	0	0	0	0	0	0	
Test 3	0	0	1	0	0	0	1	
Test 4	0	0	1	0	0	0	0	
Test 5	0	0	1	0	0	1	0	
Test 6	0	1	0	0	0	0	1	
Test 7	0	1	0	0	0	0	0	
Test 8	0	1	0	0	0	1	0	
Test 9	1	0	0	0	0	0	1	
Test 10	1	0	0	0	0	0	0	

Future Works



Conclusions

- **It is essential to clearly fix the testing objectives in order to obtain a performant Test Bench for Safety Validation.**

- **The main Test Bench realization principles shall be related to: Scalability, Flexibillity, coherence with the real system, easy operability and maintenability.**

- **It has to be taken in mind that an efficent Test Bench is NOT the only Key for ensuring the quality of the Safety Functions Validation task.**

- **The adoption of Formal Specification Languages for the Safety Functions description will improve the conception and the Quality of the final Verification & Validation.**

www.cern.ch