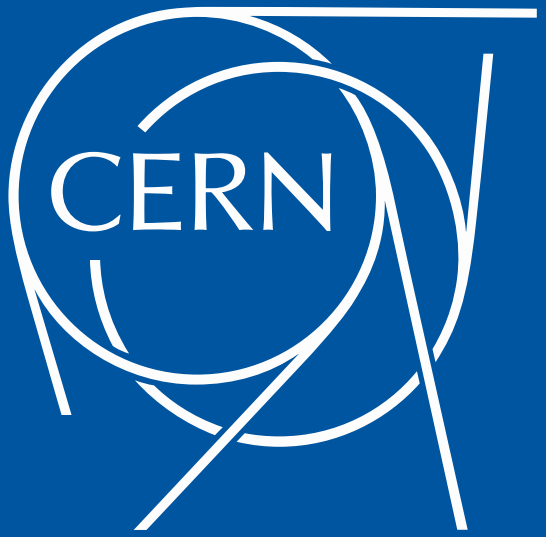

CERN

Engineering of Critical-Safety Systems at CERN

Testing of Safety Functions

ICALEPCS - 06-11 October 2013

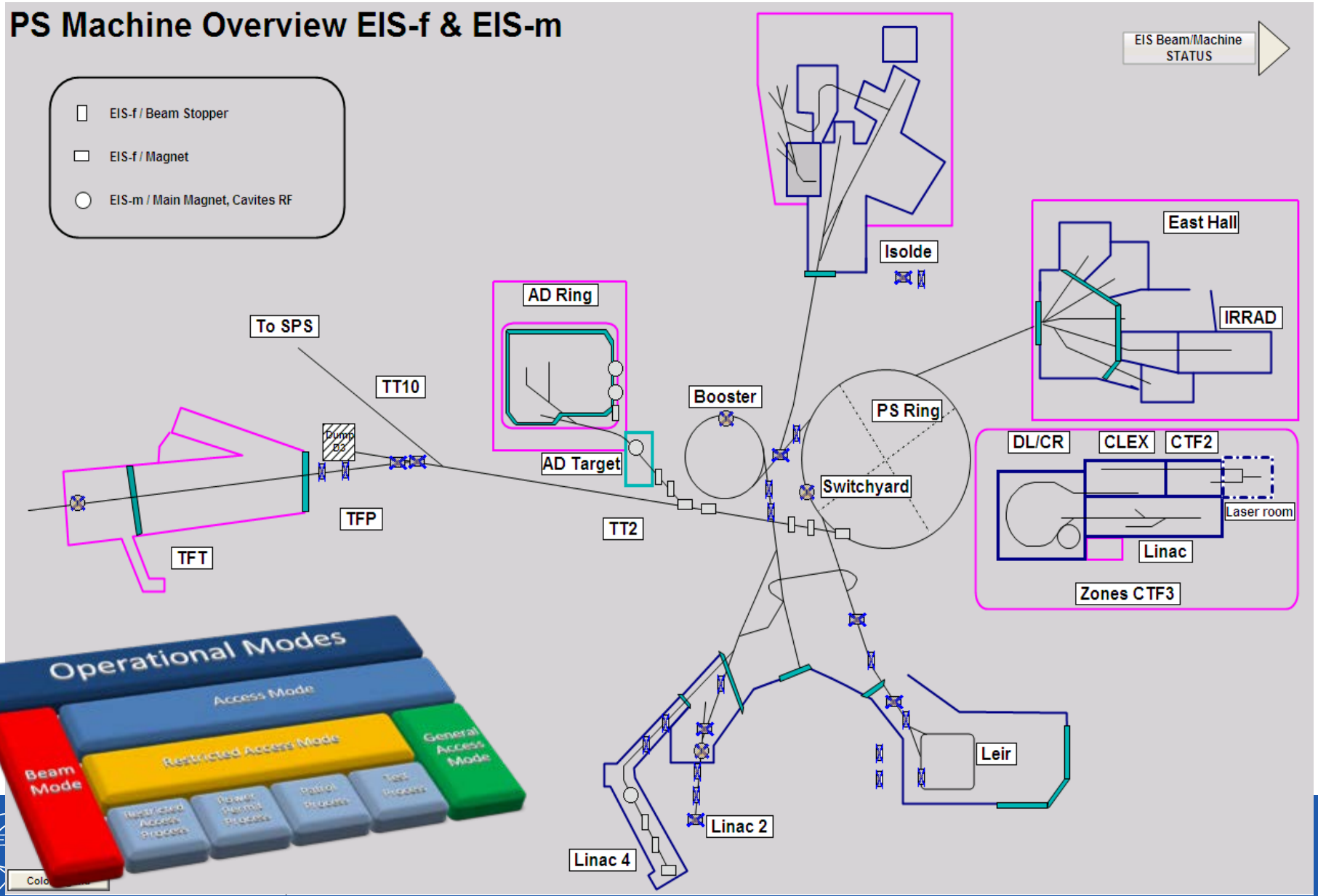
Authors: P. Ninin, F. Valentini

Outline

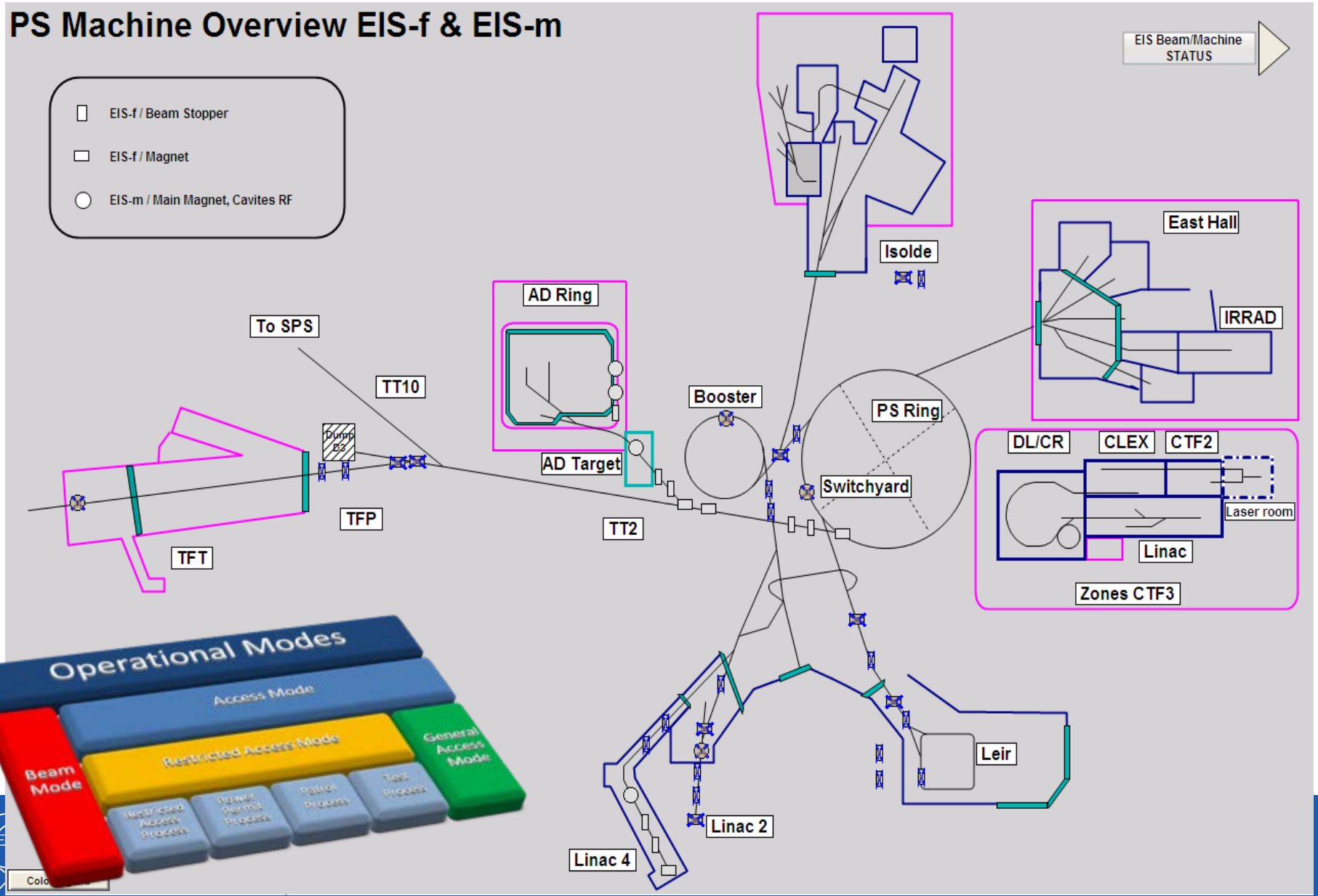
The return of experience of CERN in the development and validation of Safety Personnel Protection Systems showed us that the realization of a performing Test Platform is essential to ensure the quality of the Verification and Validation activities. However the adoption of a Formal Language for the specification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

- PS-PPS Project Scope
- Safety Test Bench Conception
- Safety Functions – Formal Definition Language
- Model-Based Testing Approach for Validation
- Conclusions

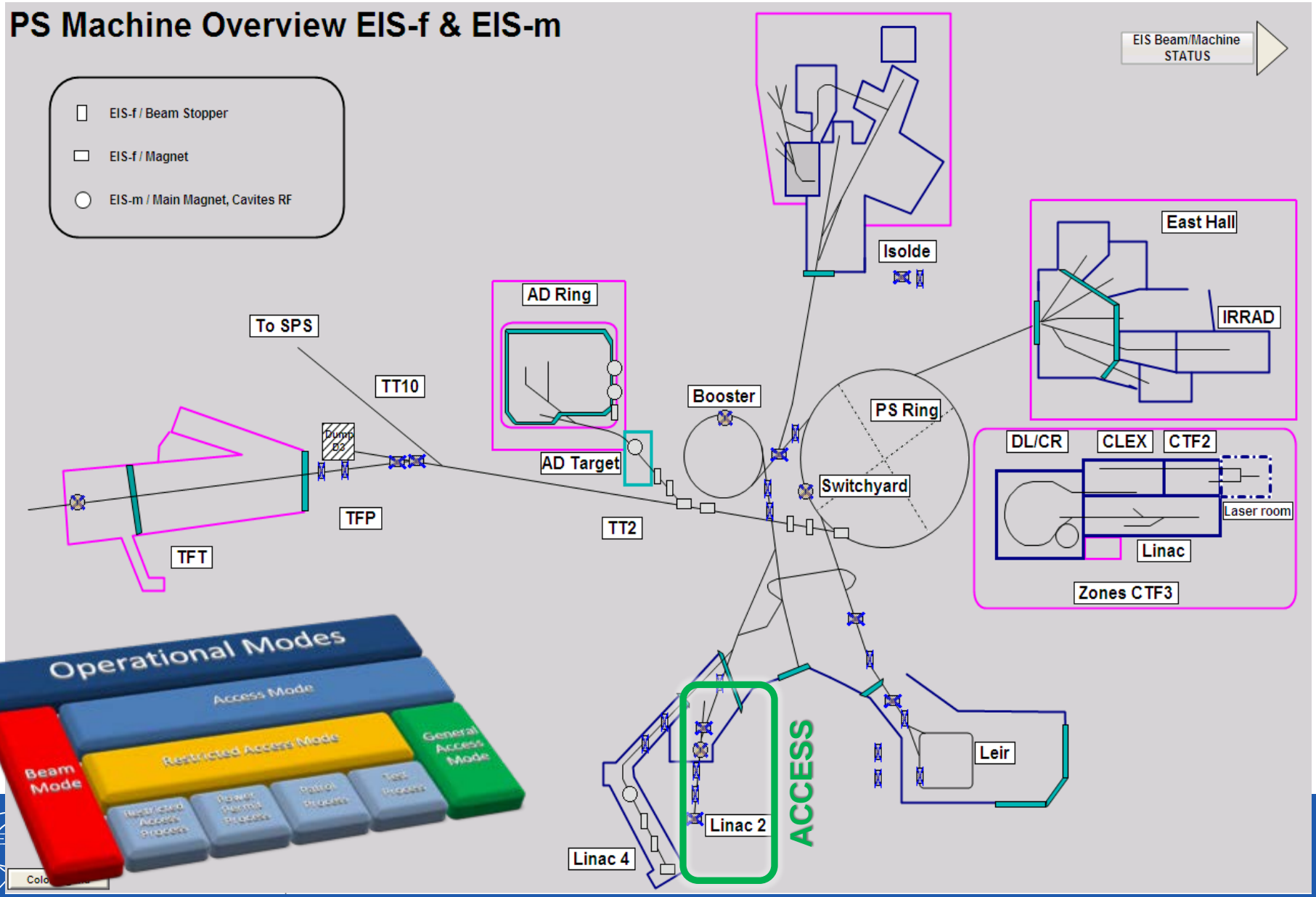
PS-PPS Project Scope



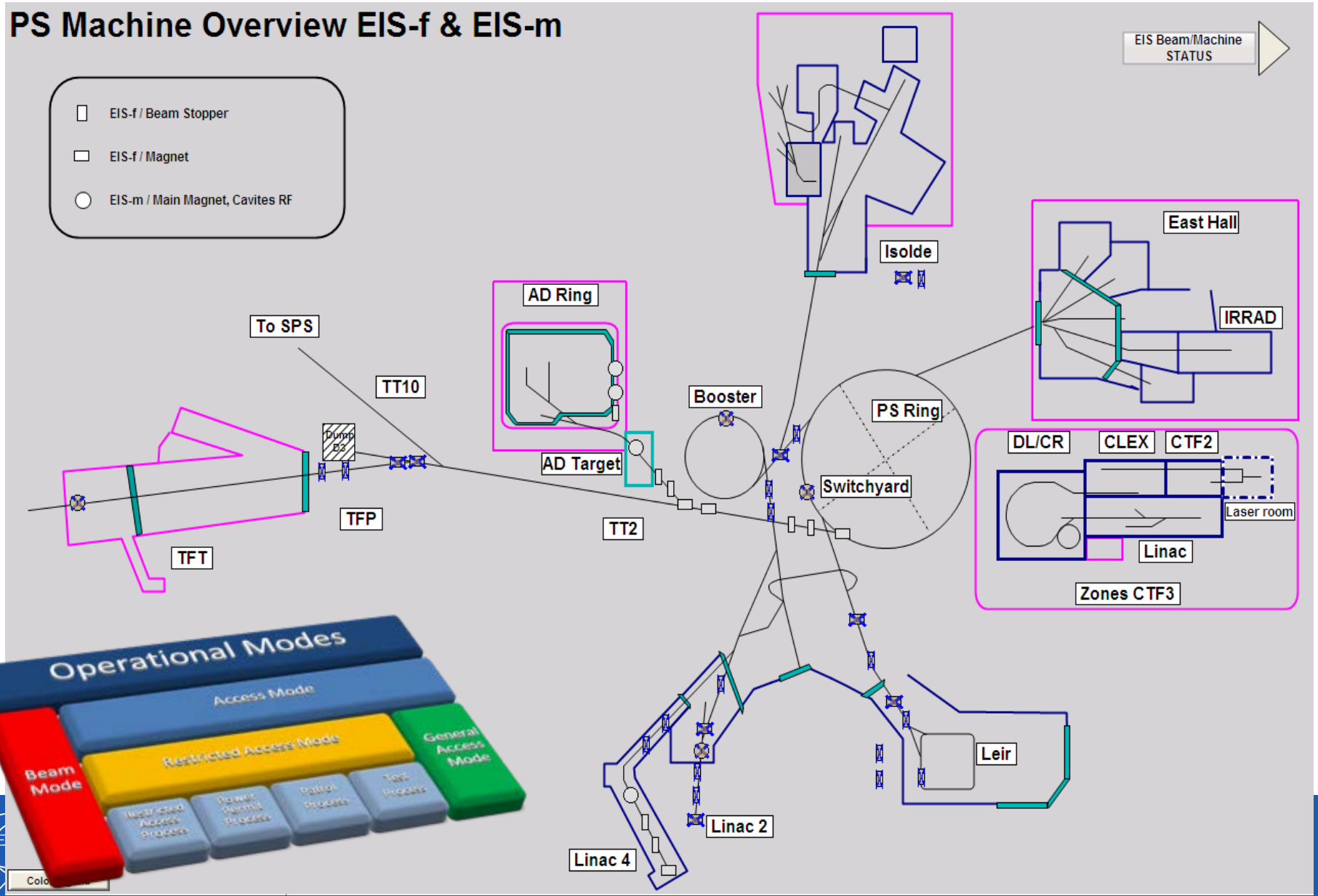
PS-PPS Project Scope



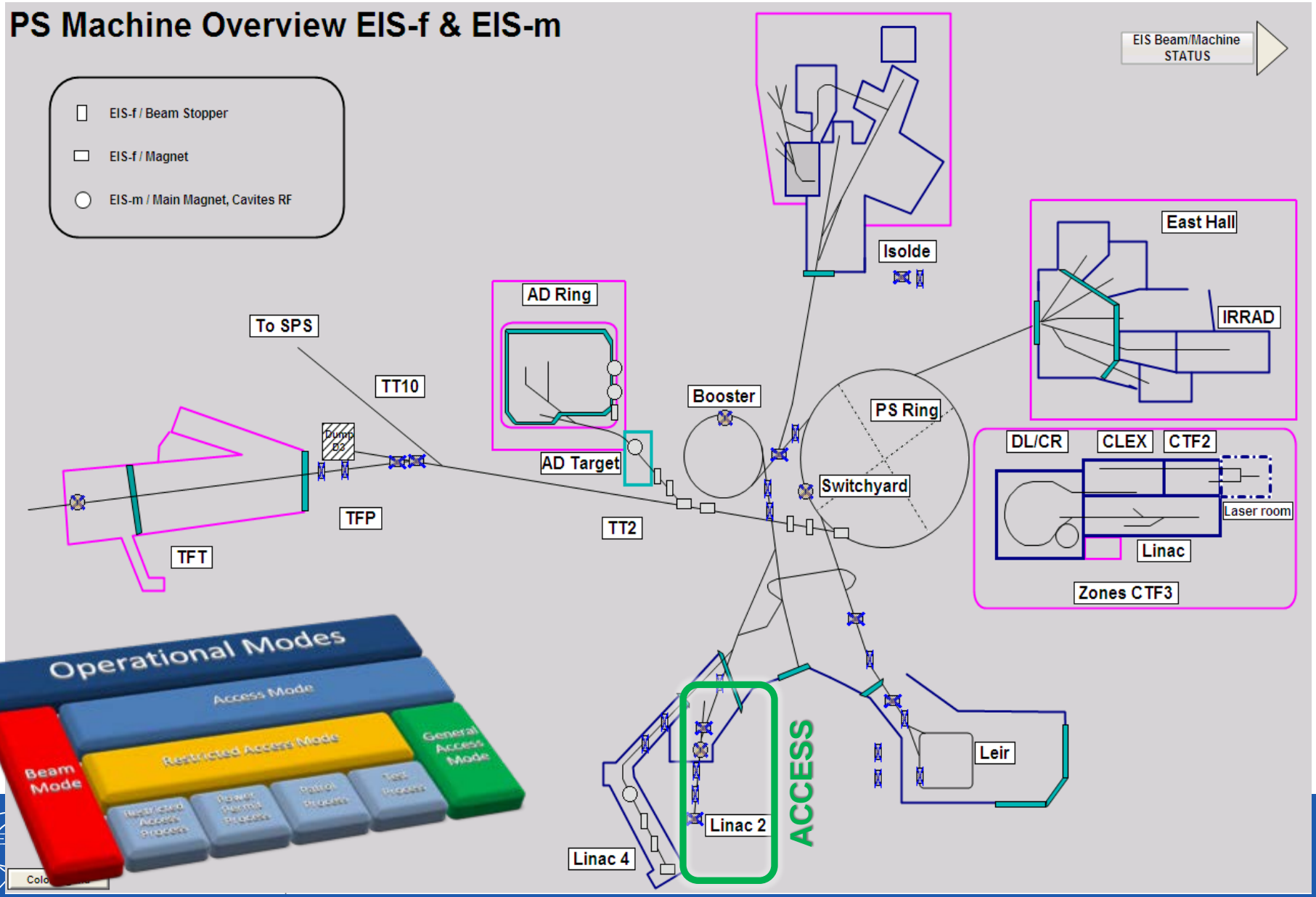
PS-PPS Project Scope



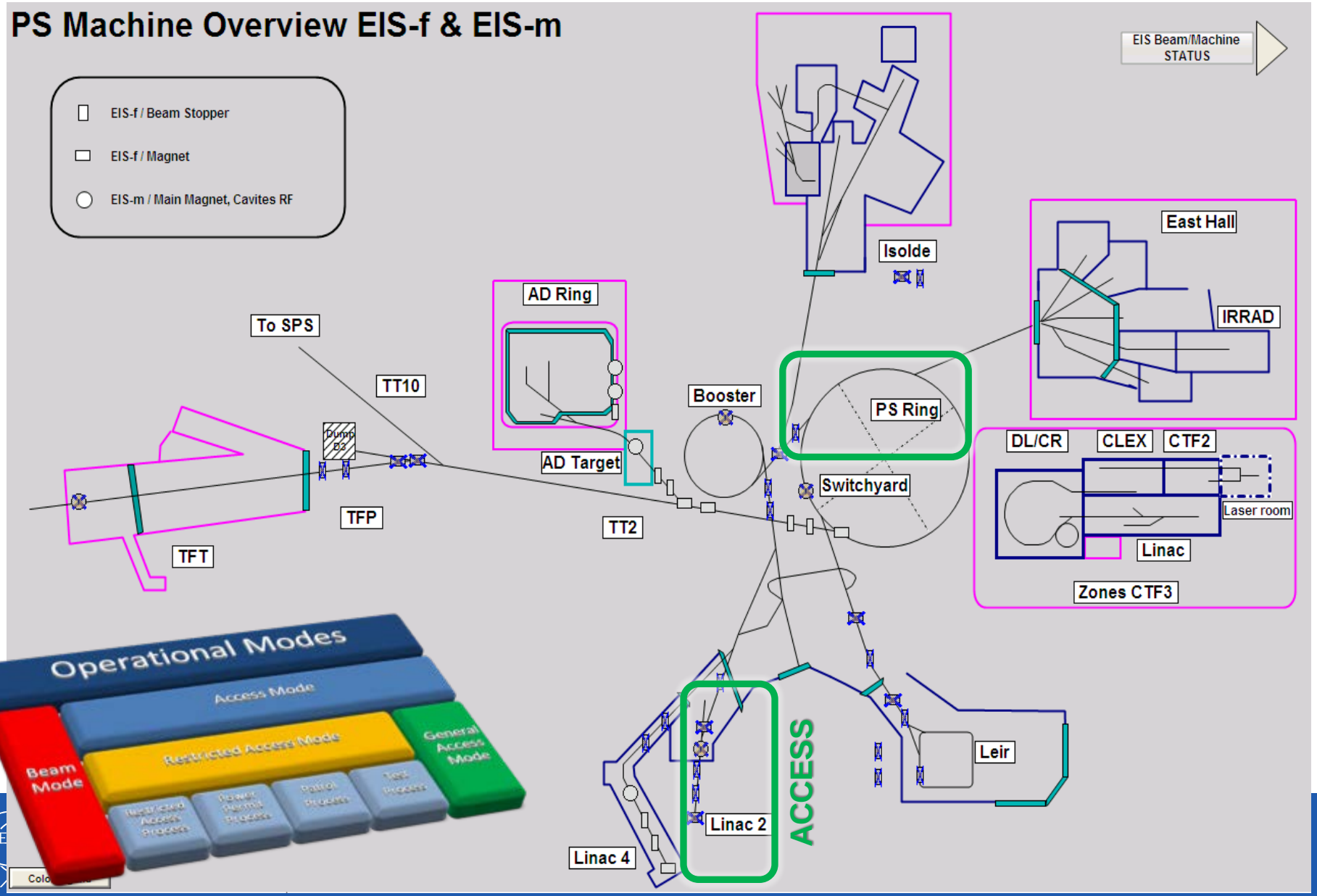
PS-PPS Project Scope



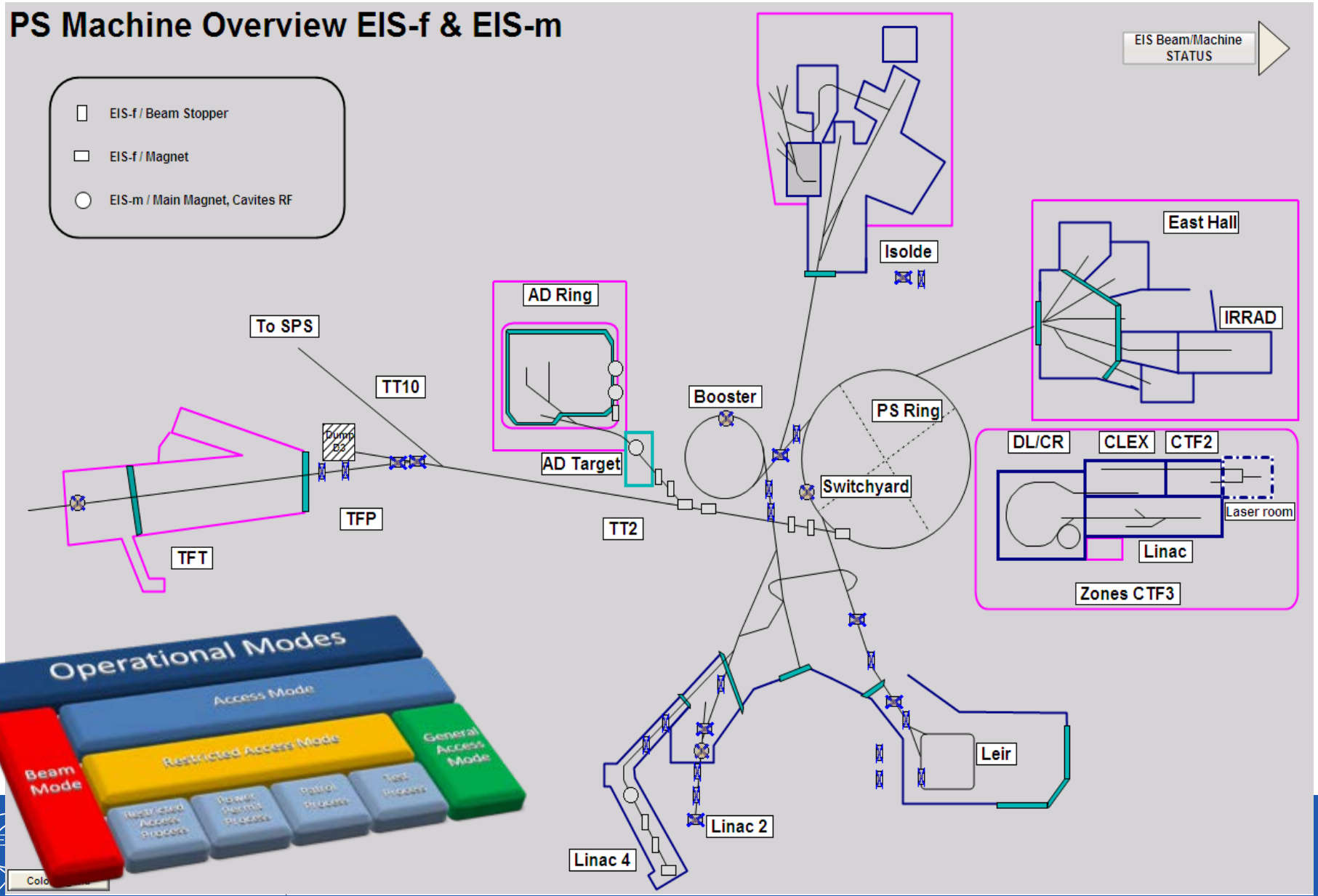
PS-PPS Project Scope



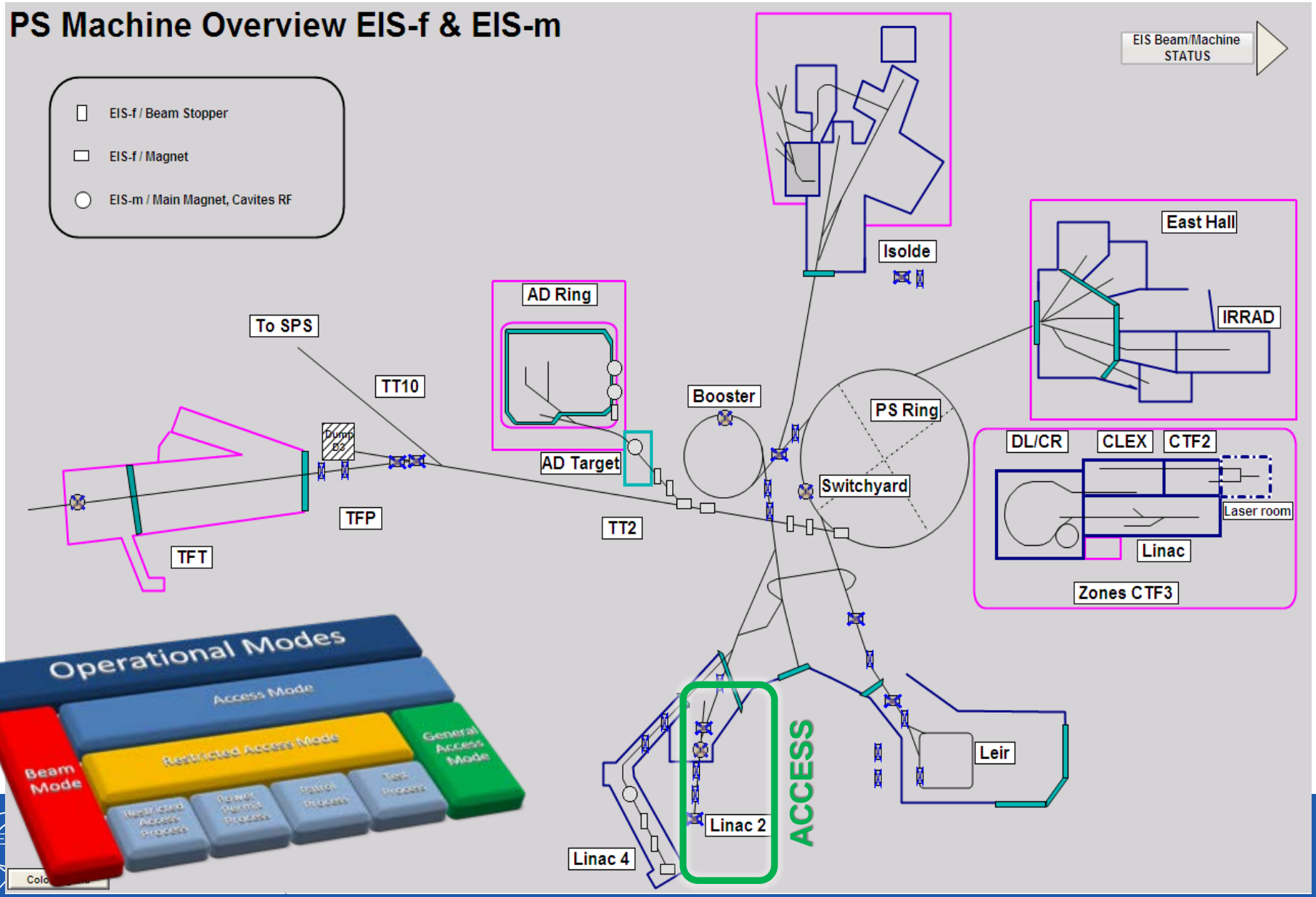
PS-PPS Project Scope



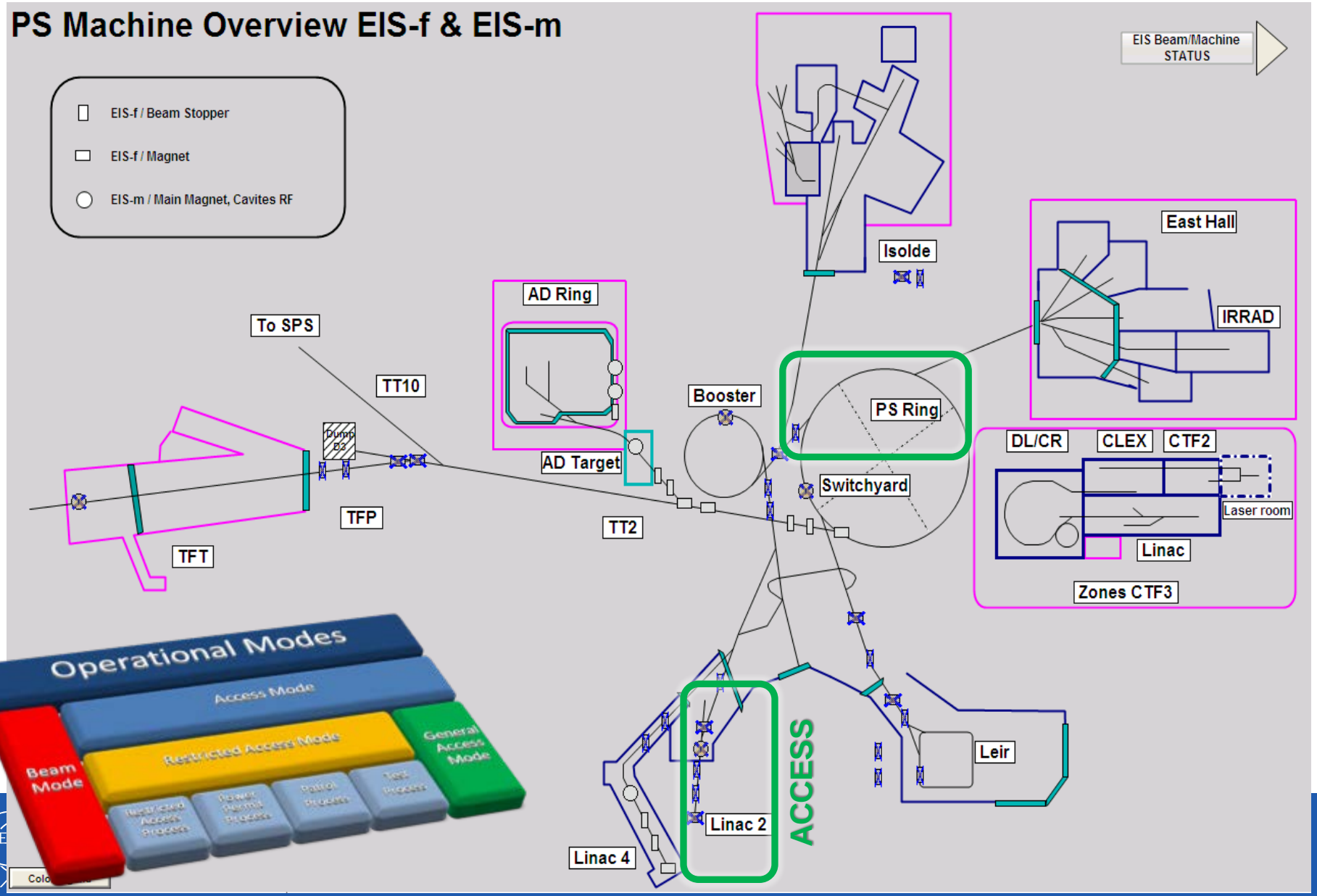
PS-PPS Project Scope



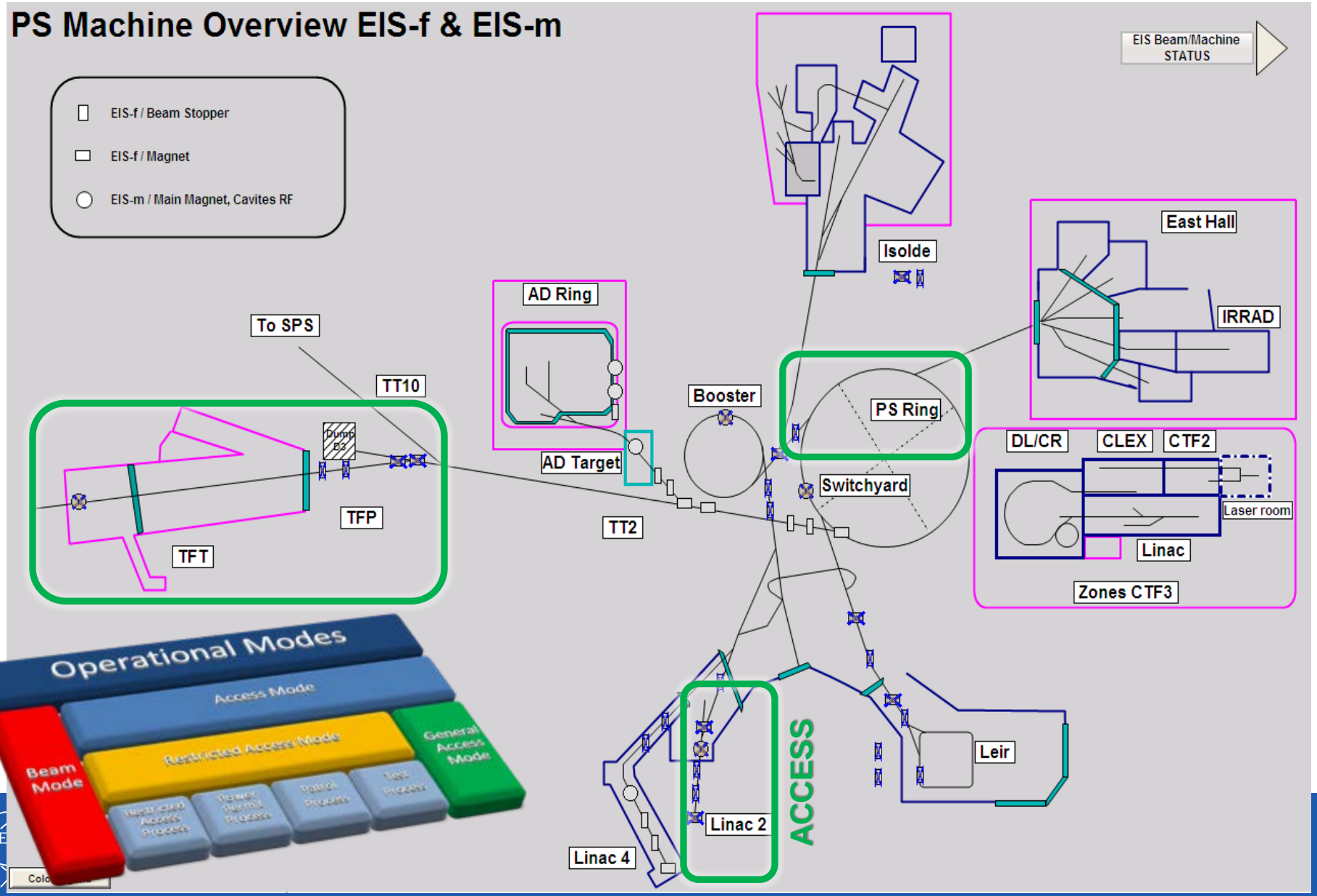
PS-PPS Project Scope



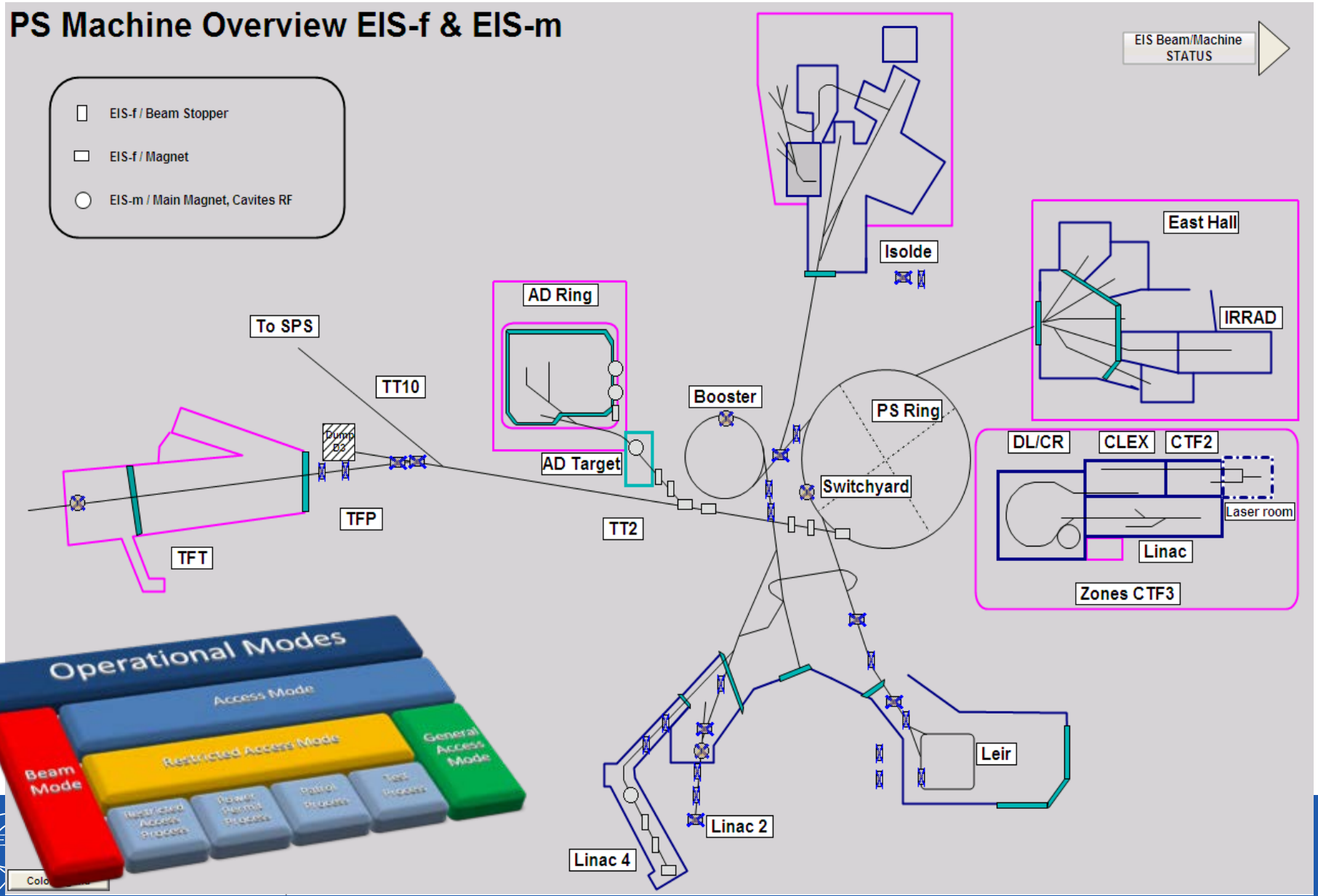
PS-PPS Project Scope



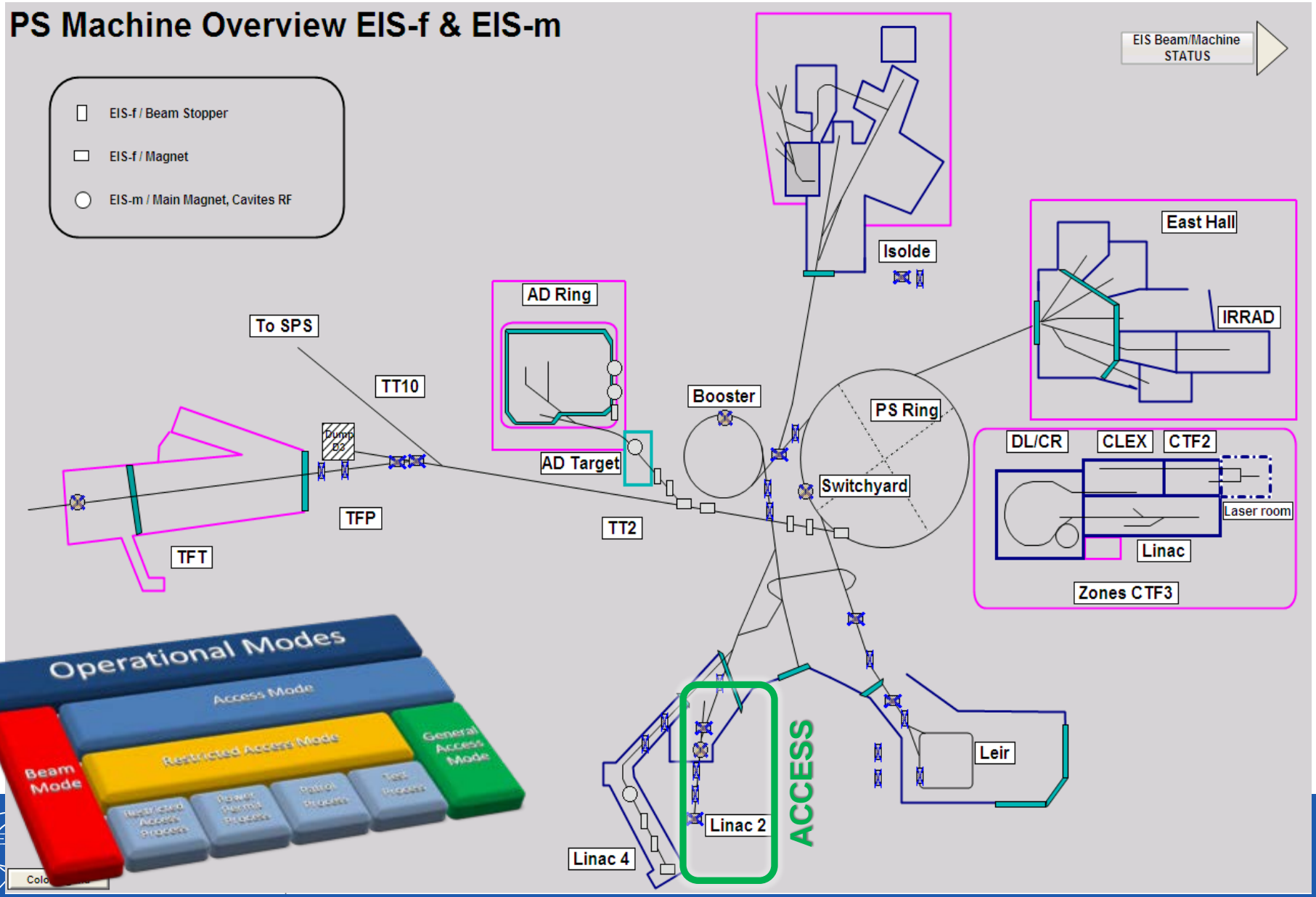
PS-PPS Project Scope



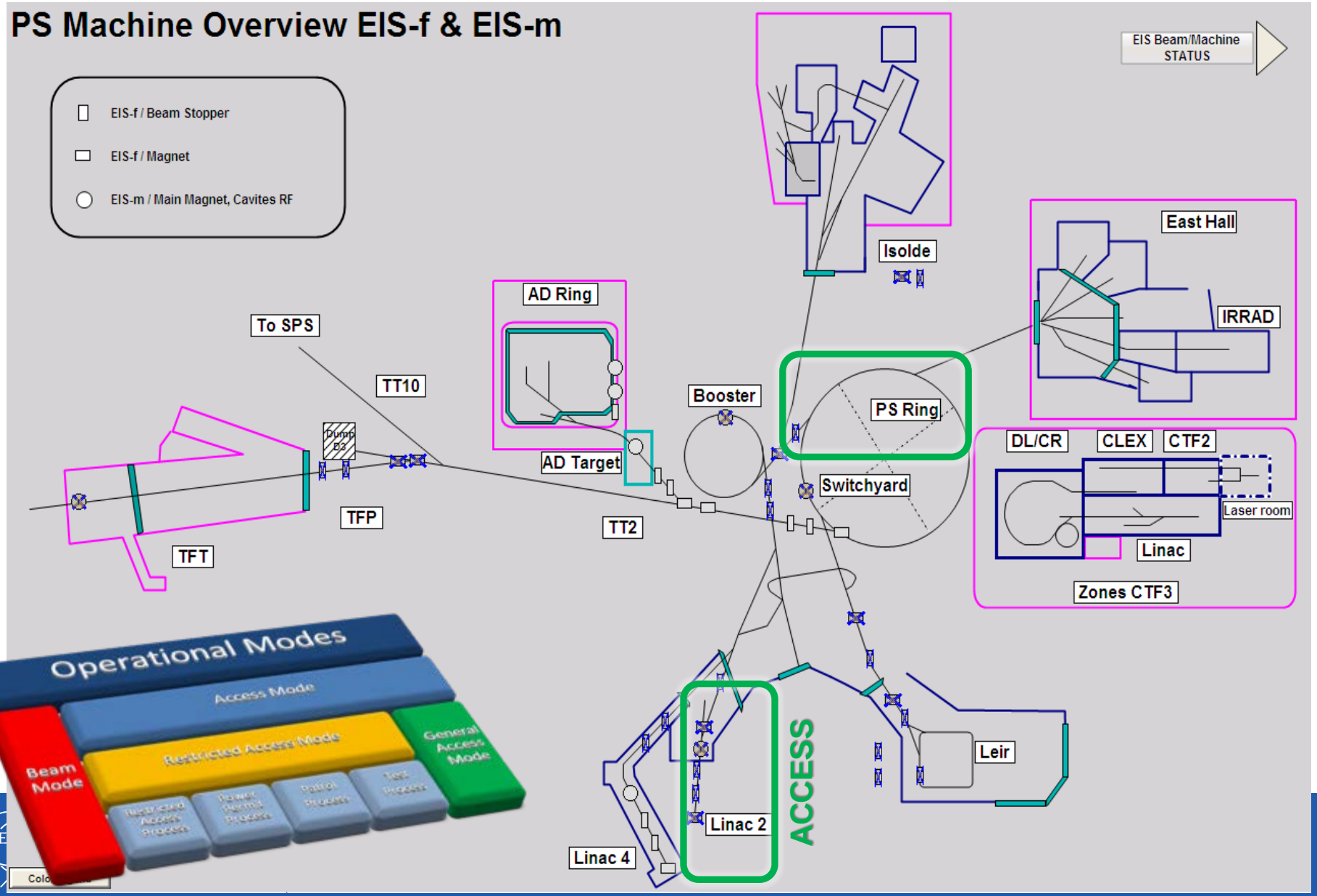
PS-PPS Project Scope



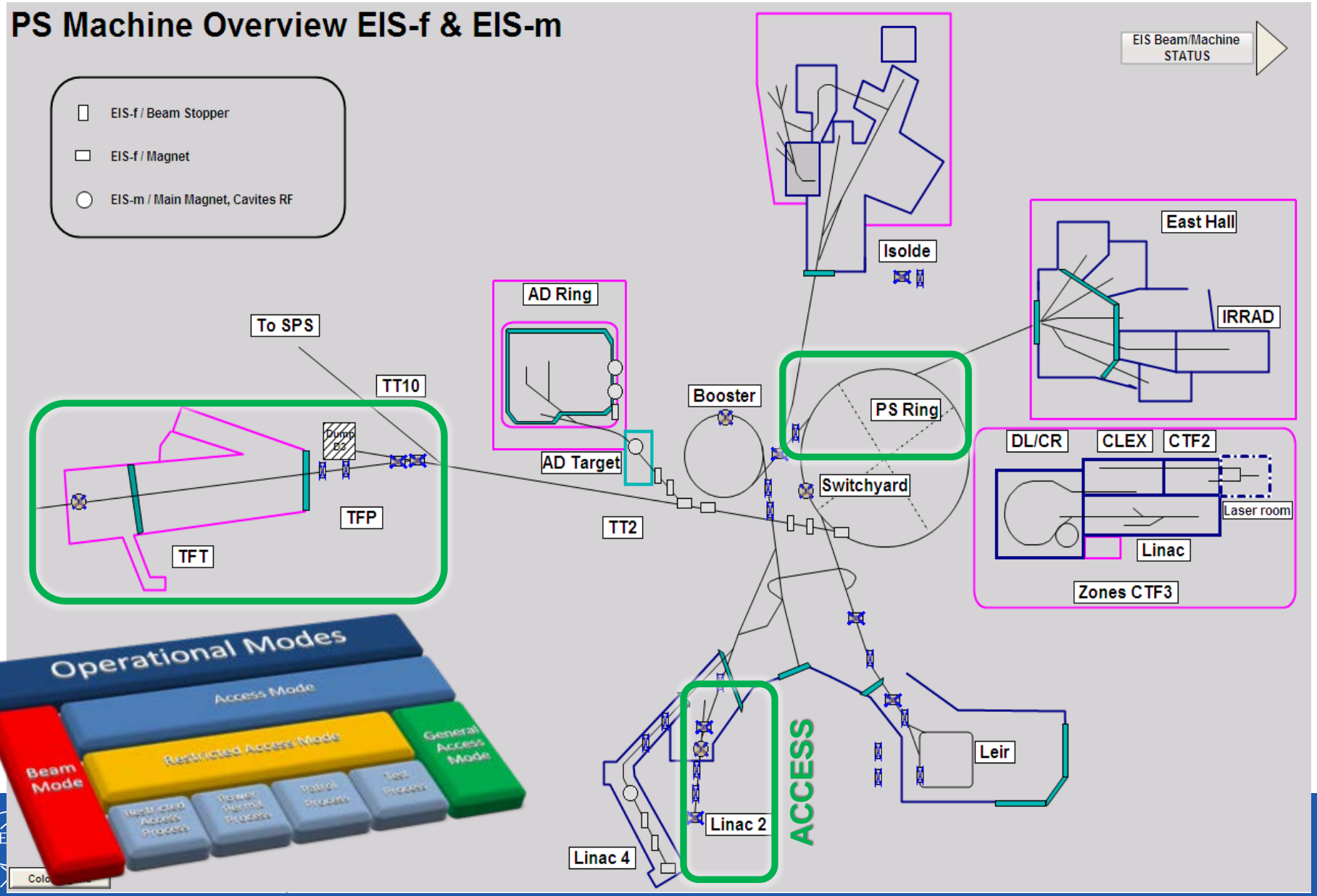
PS-PPS Project Scope



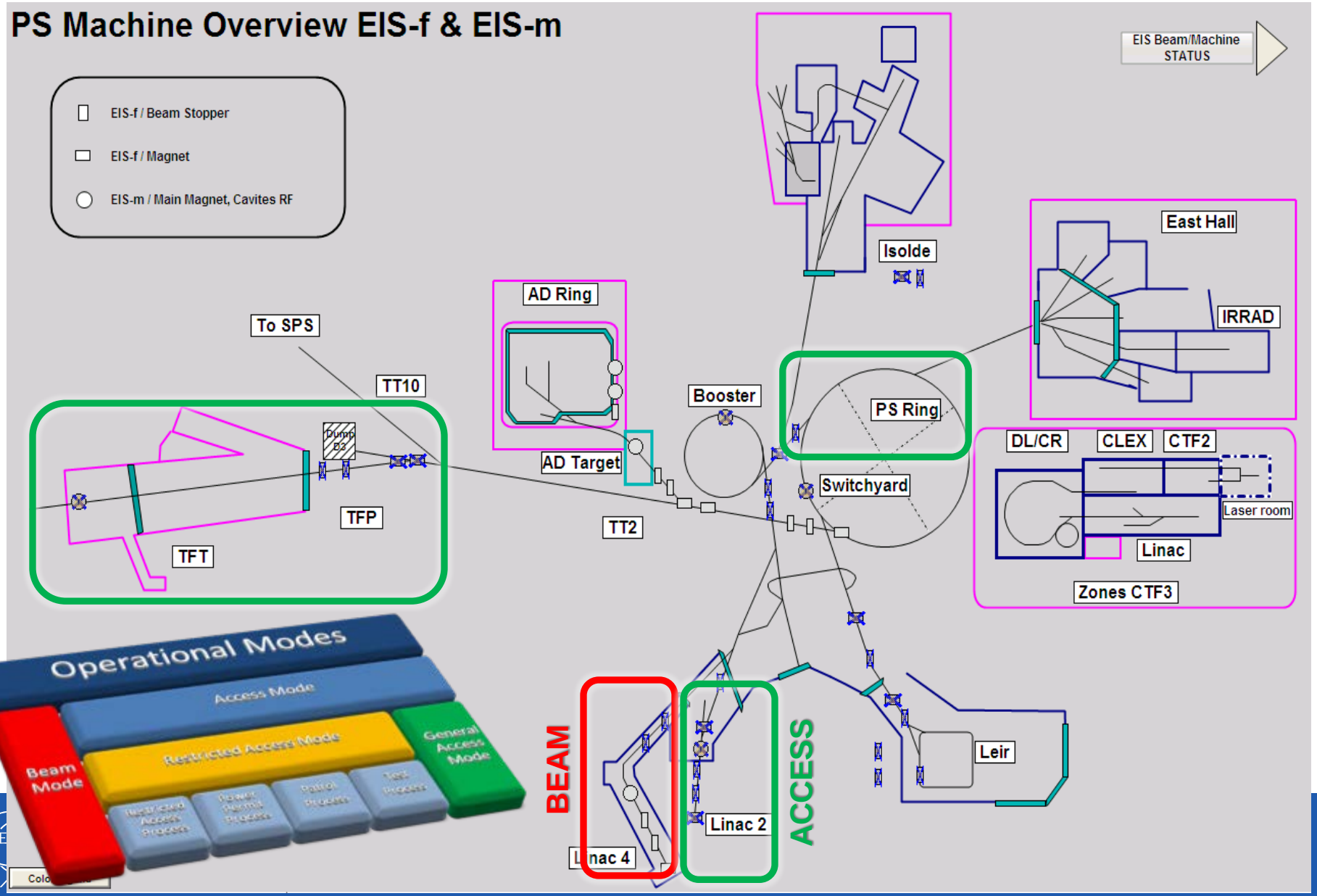
PS-PPS Project Scope



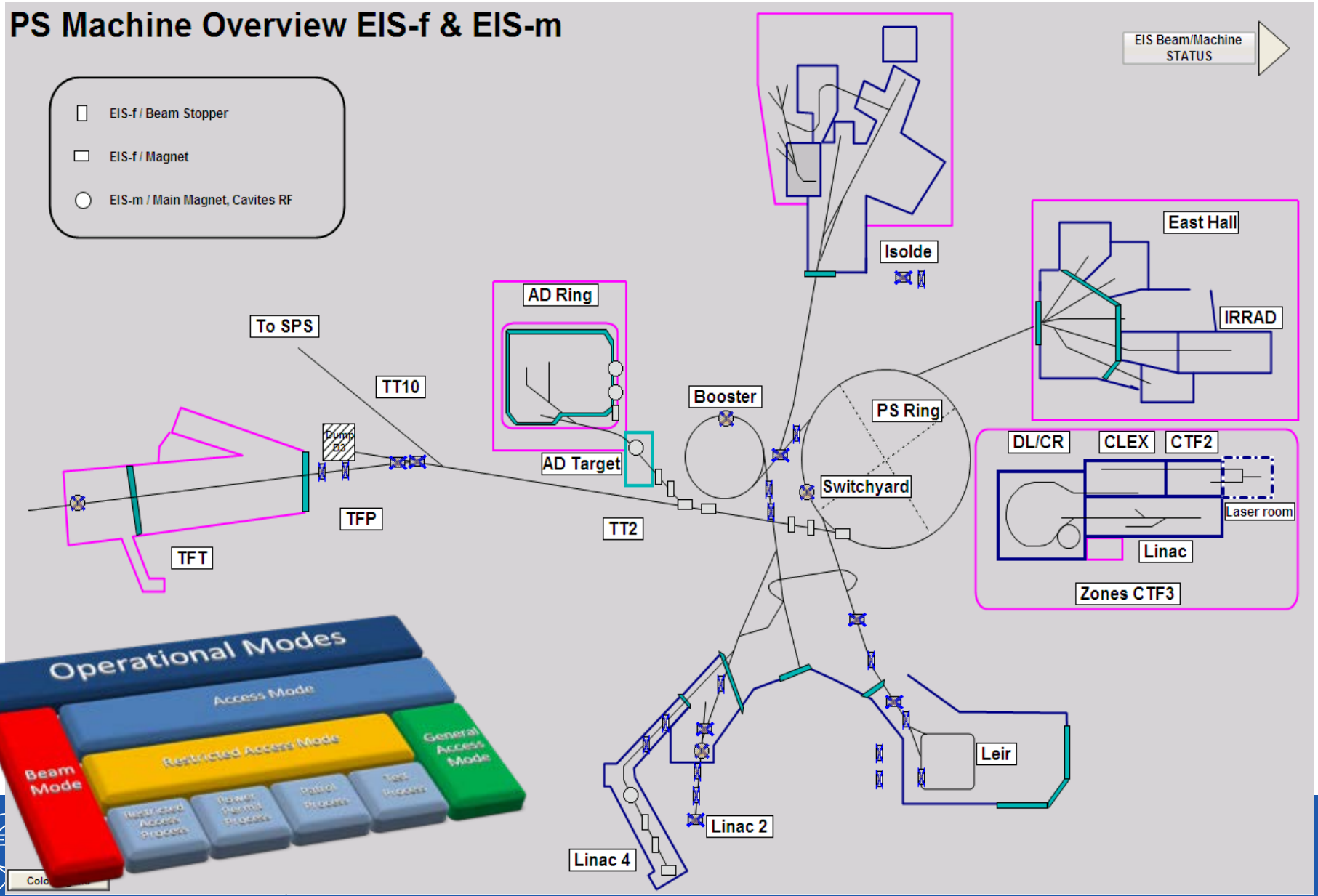
PS-PPS Project Scope



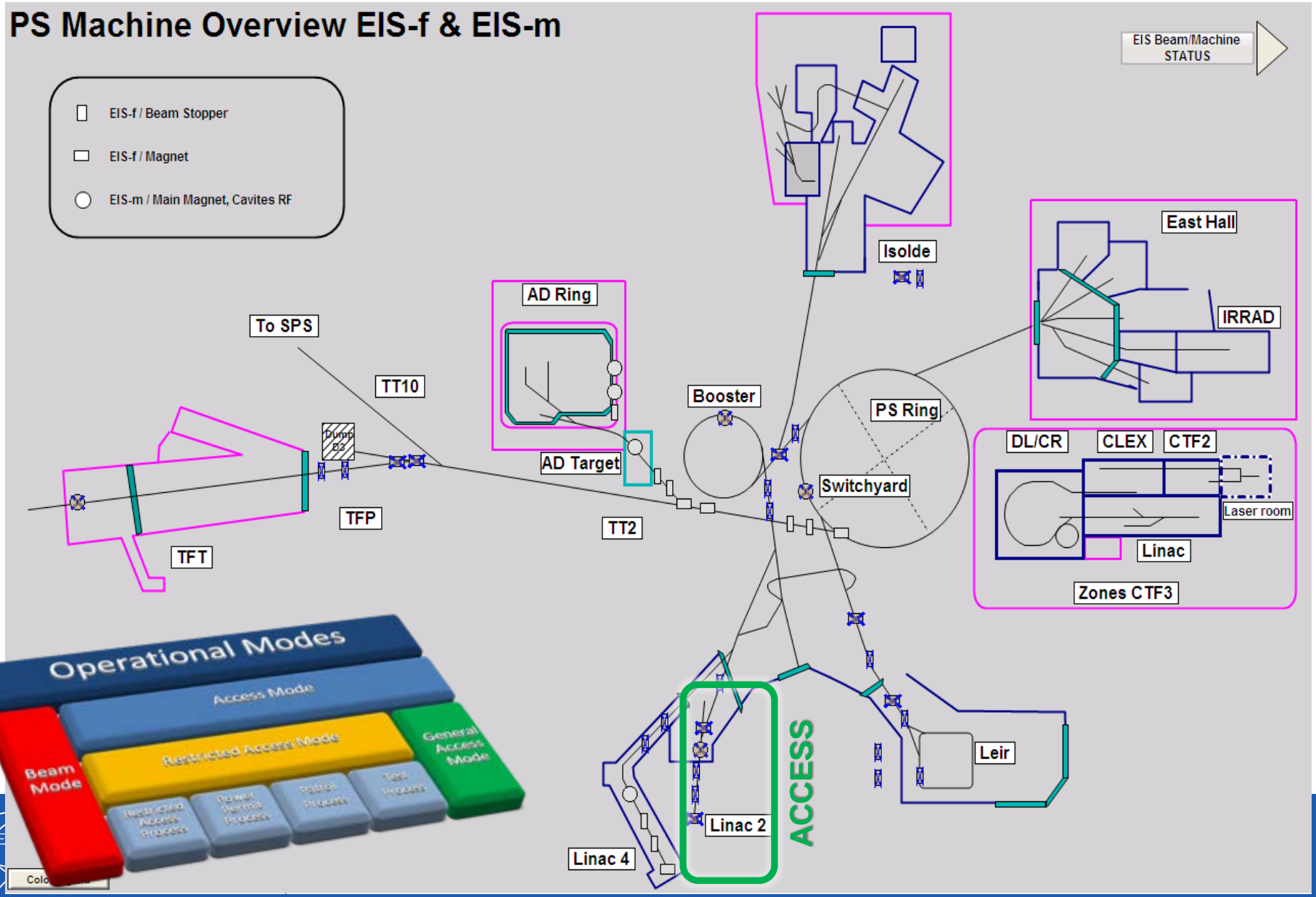
PS-PPS Project Scope



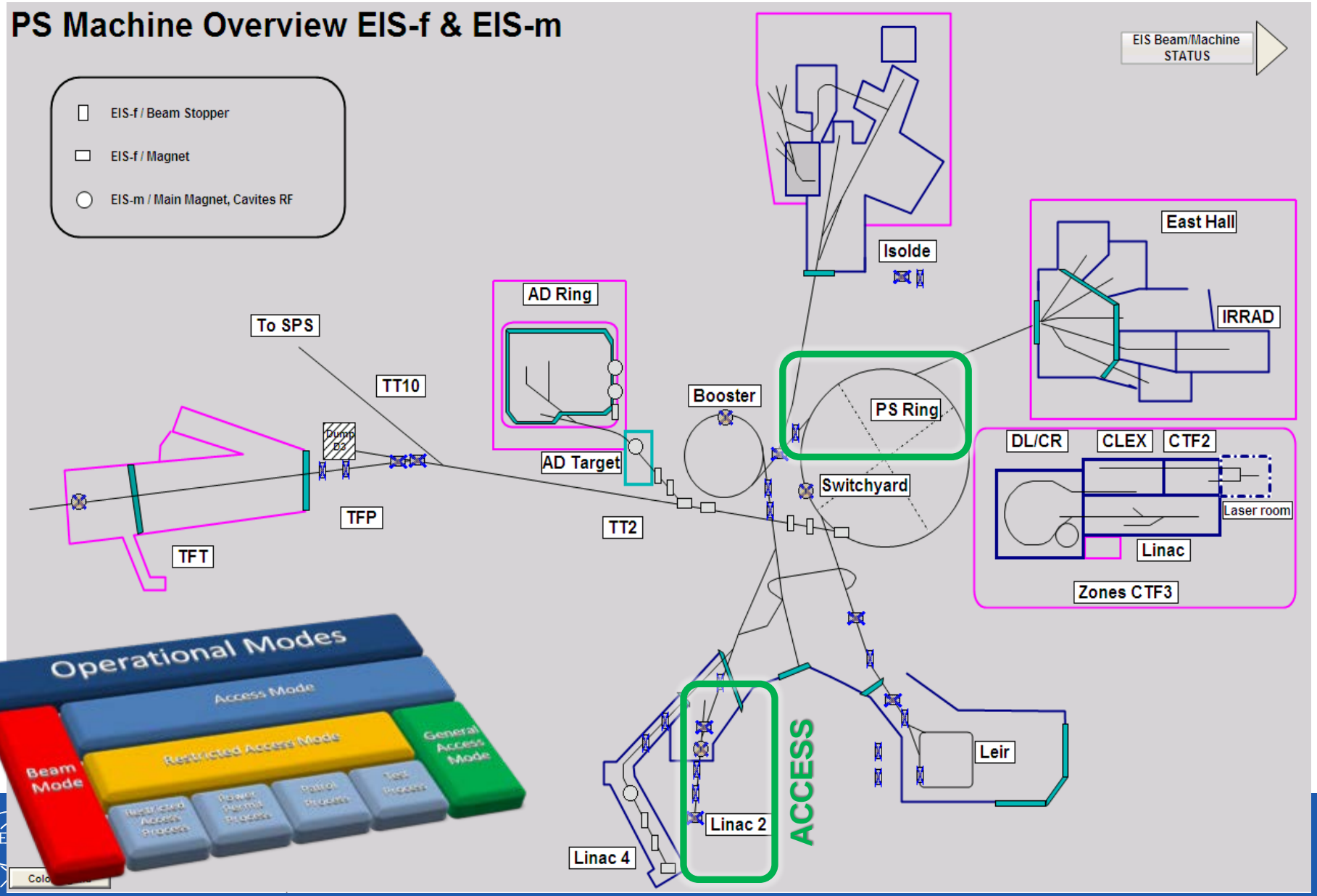
PS-PPS Project Scope



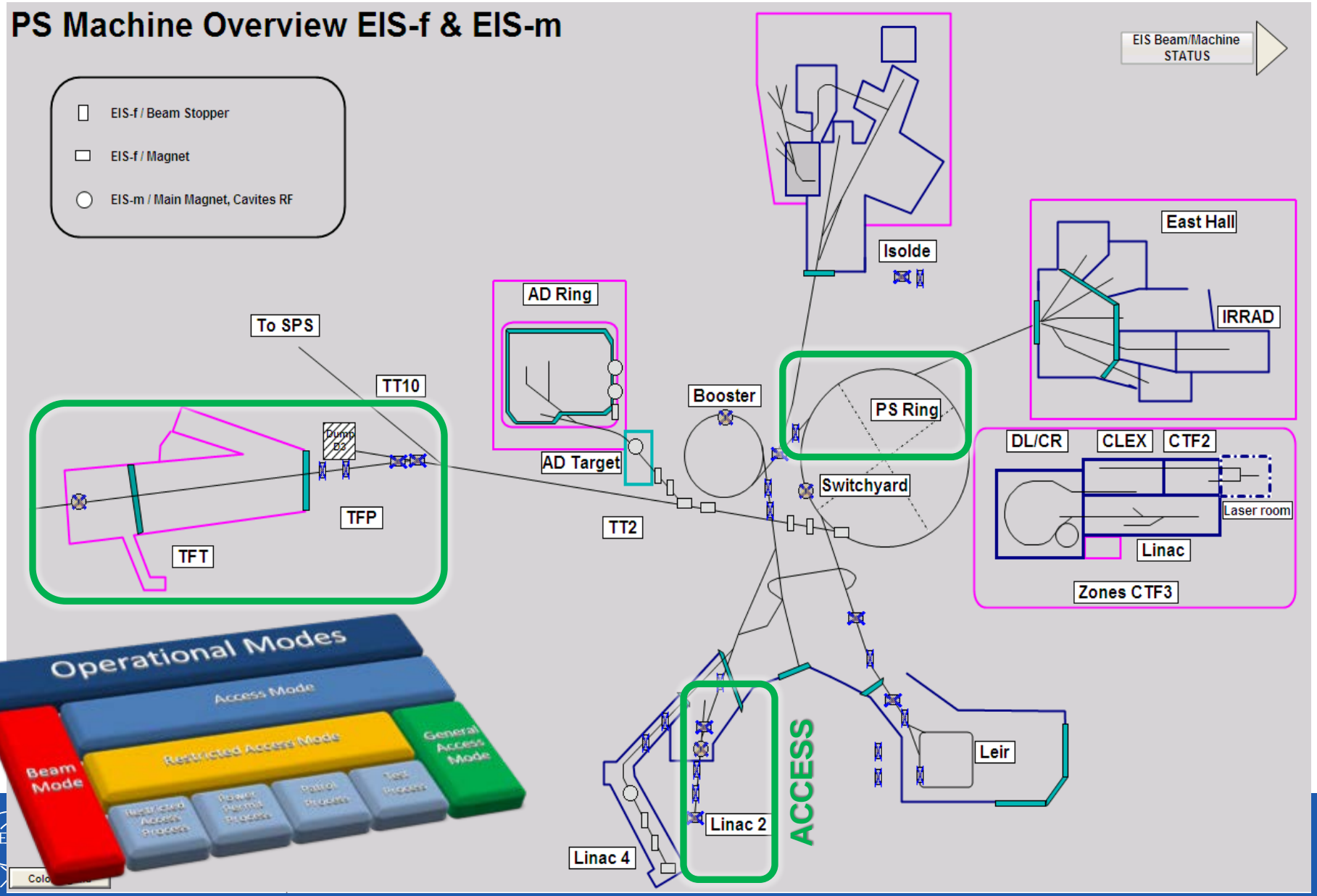
PS-PPS Project Scope



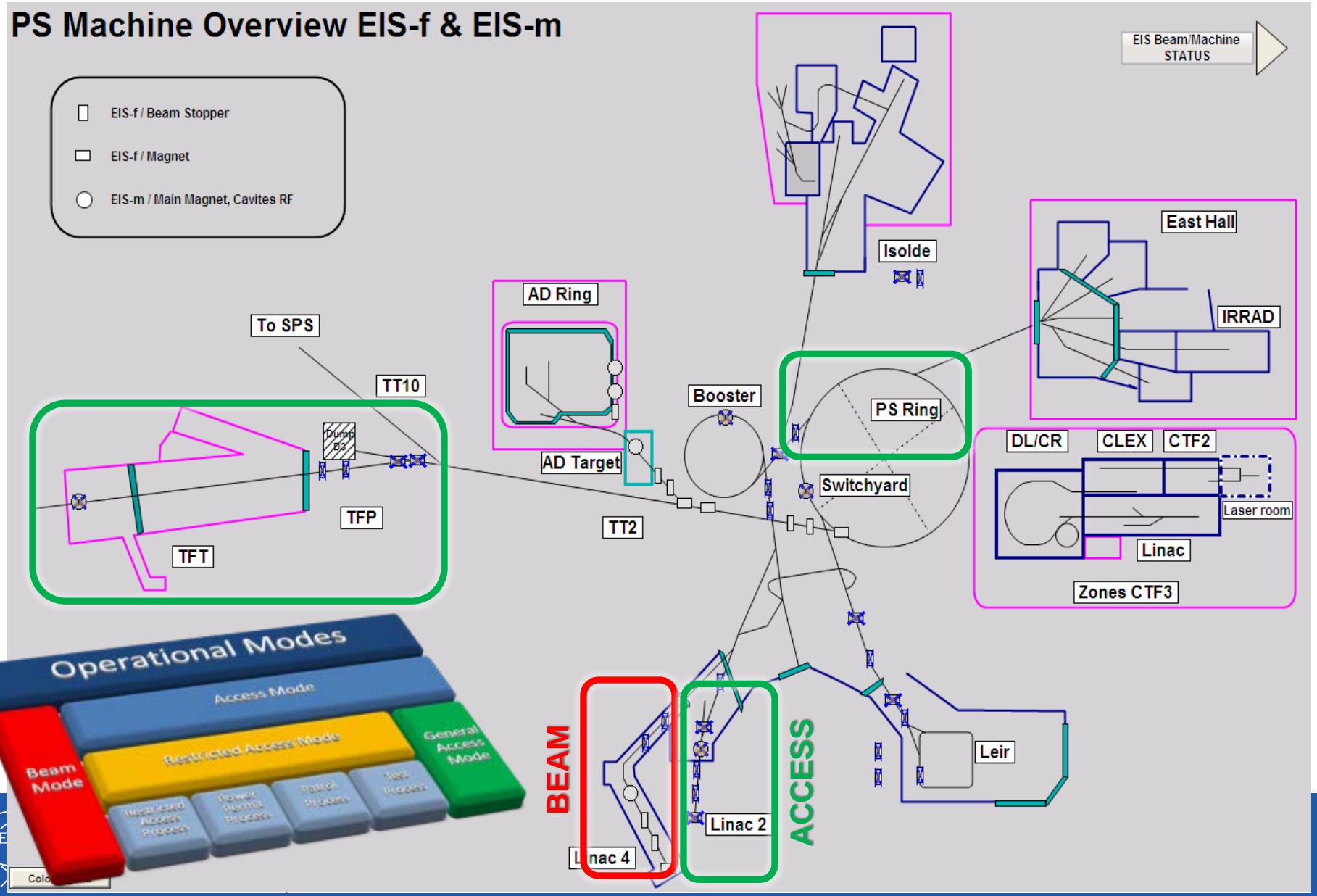
PS-PPS Project Scope



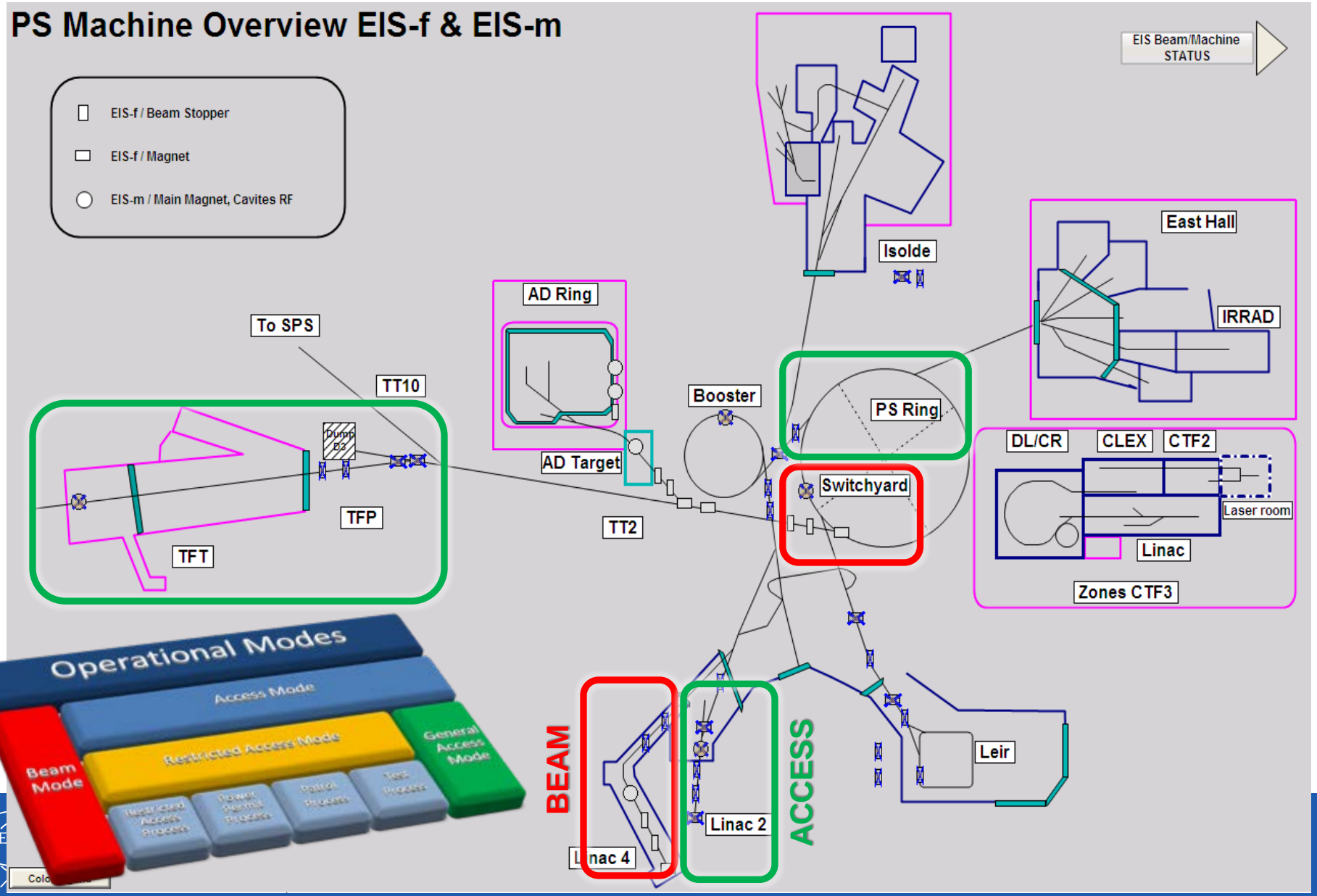
PS-PPS Project Scope



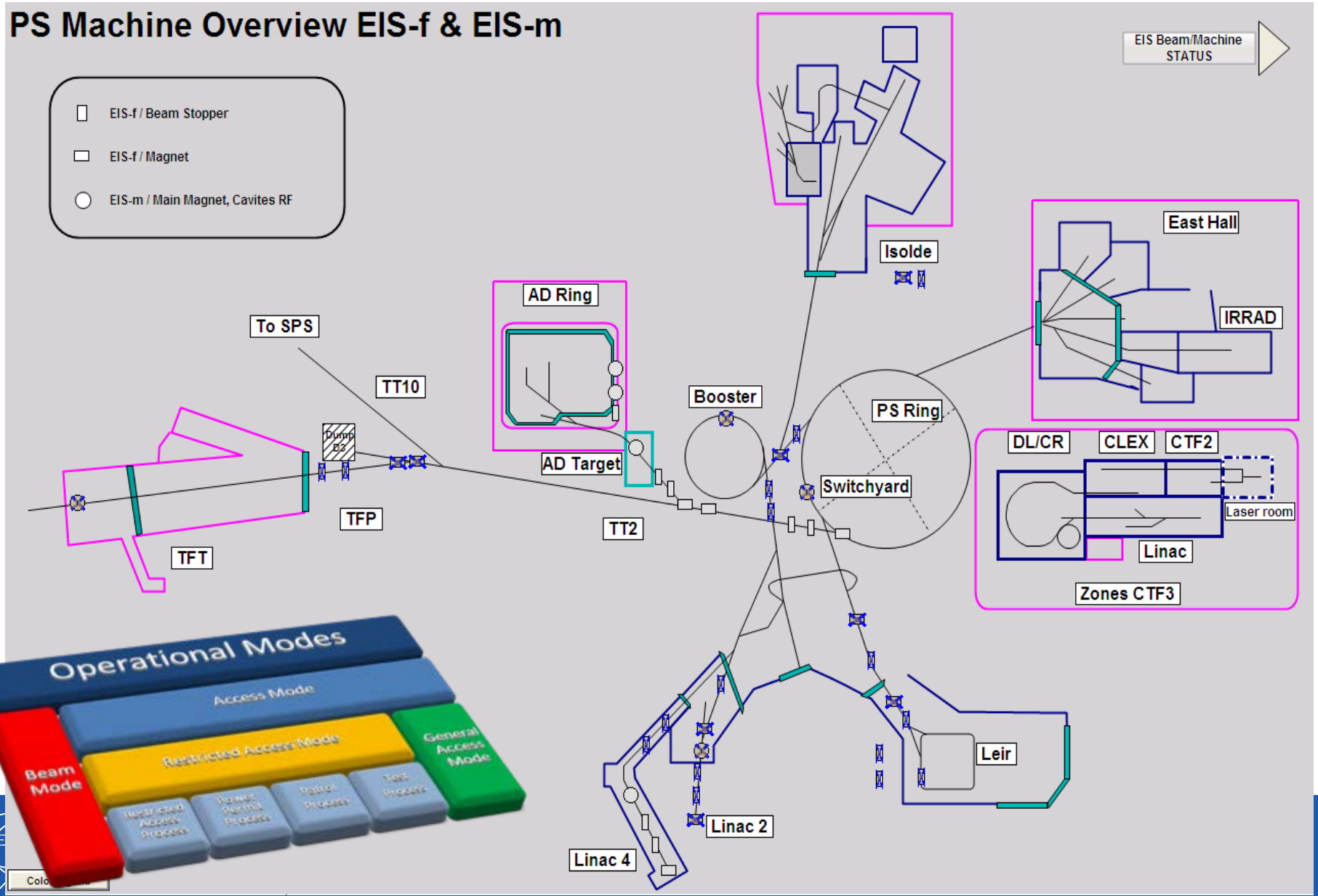
PS-PPS Project Scope



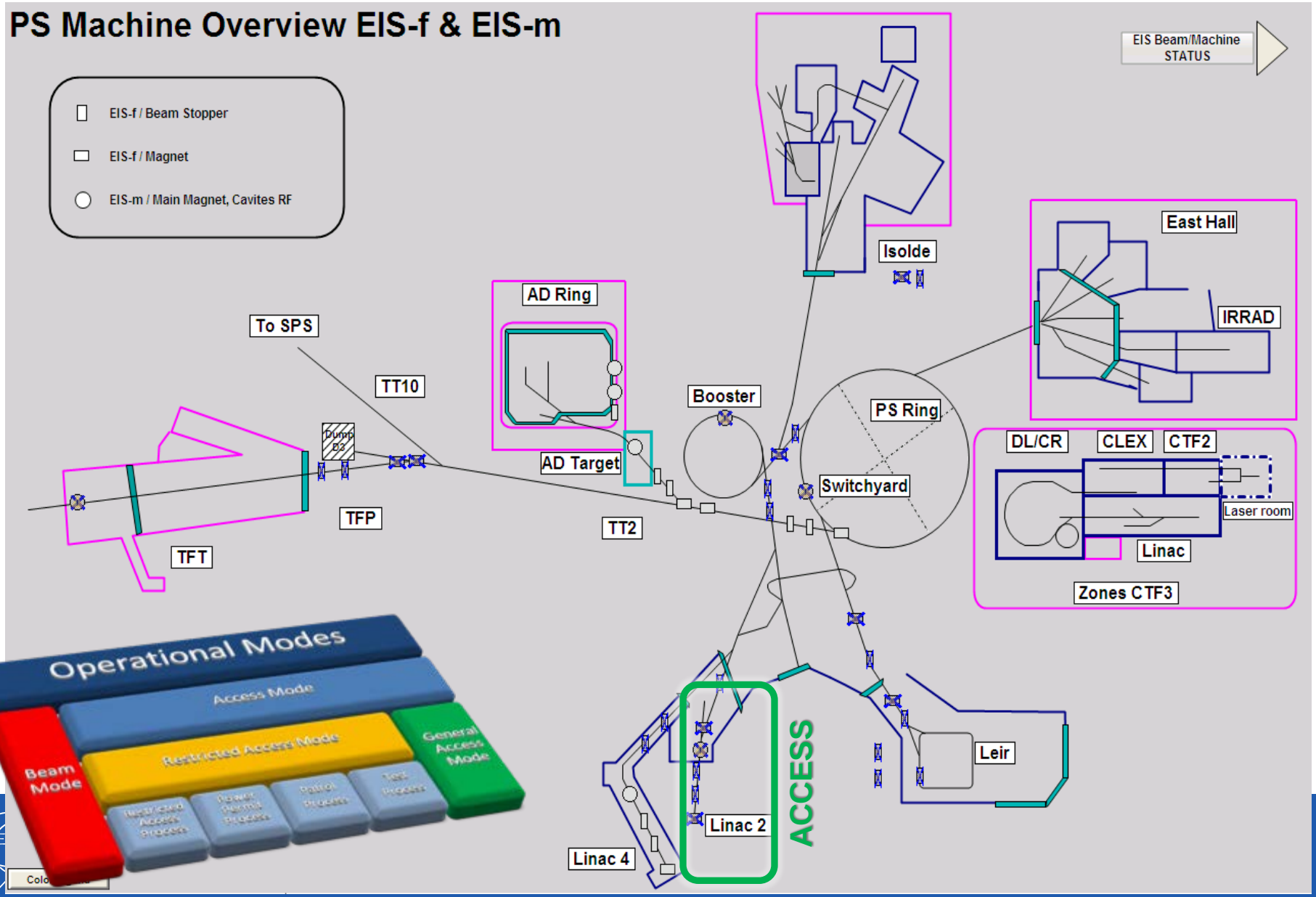
PS-PPS Project Scope



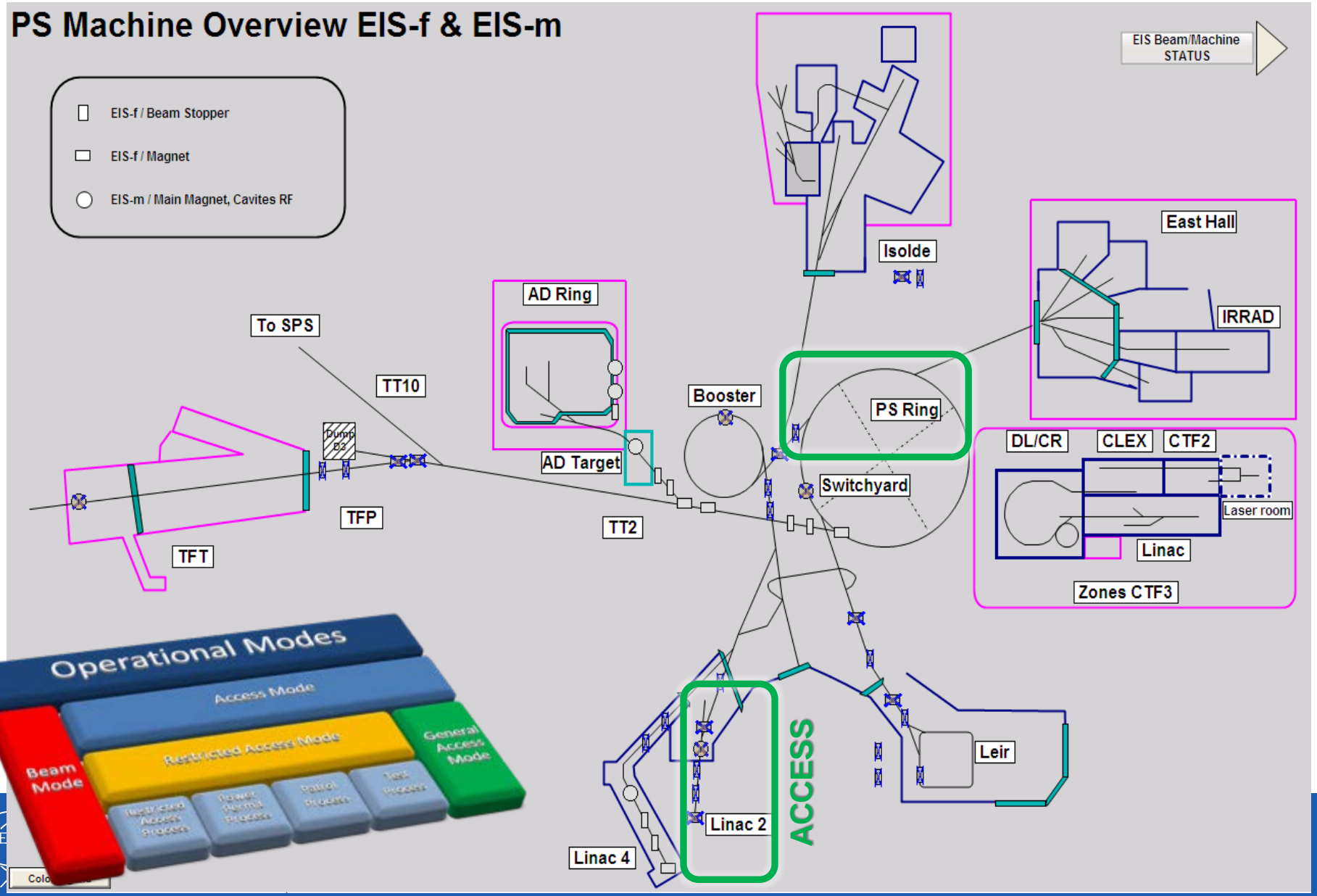
PS-PPS Project Scope



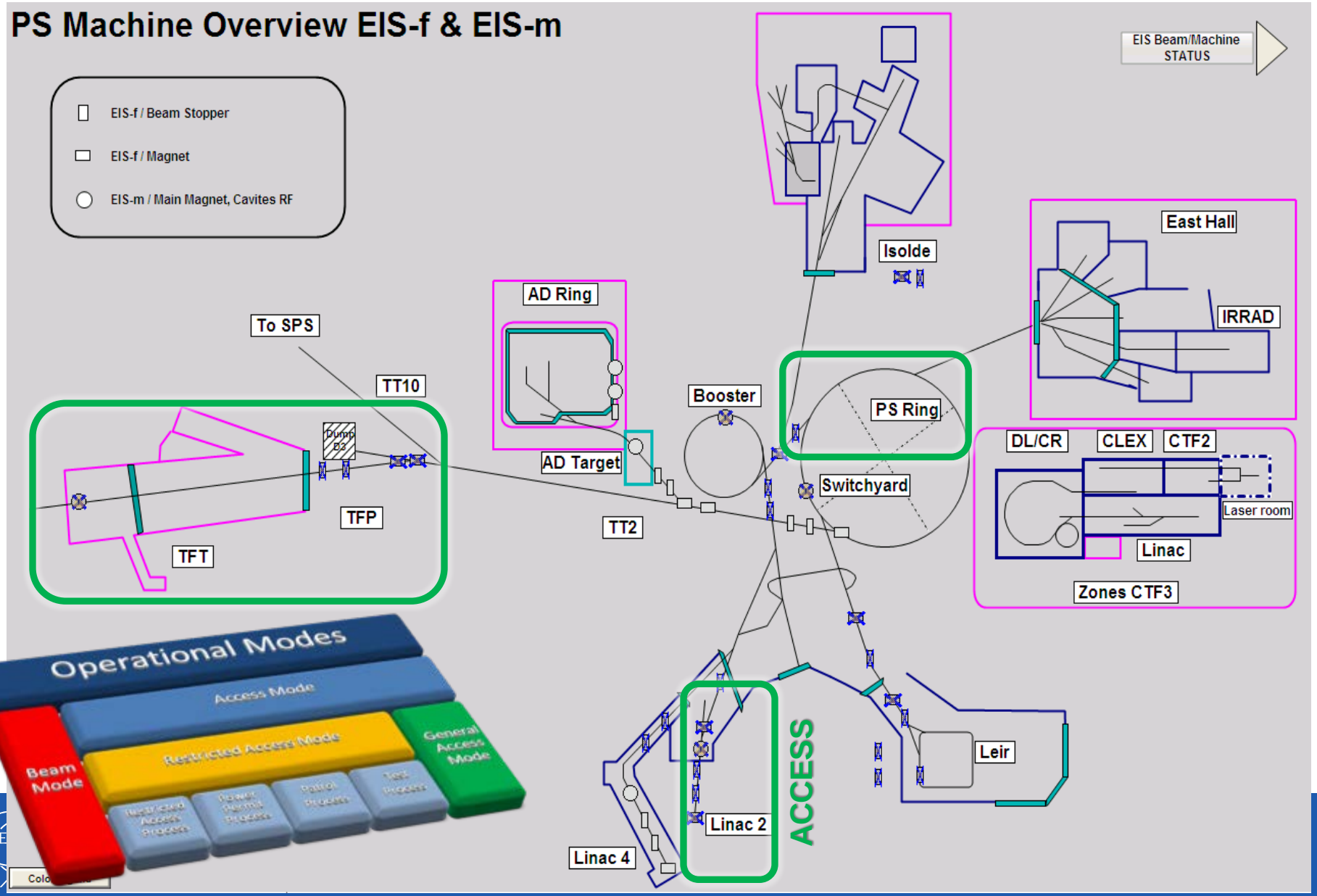
PS-PPS Project Scope



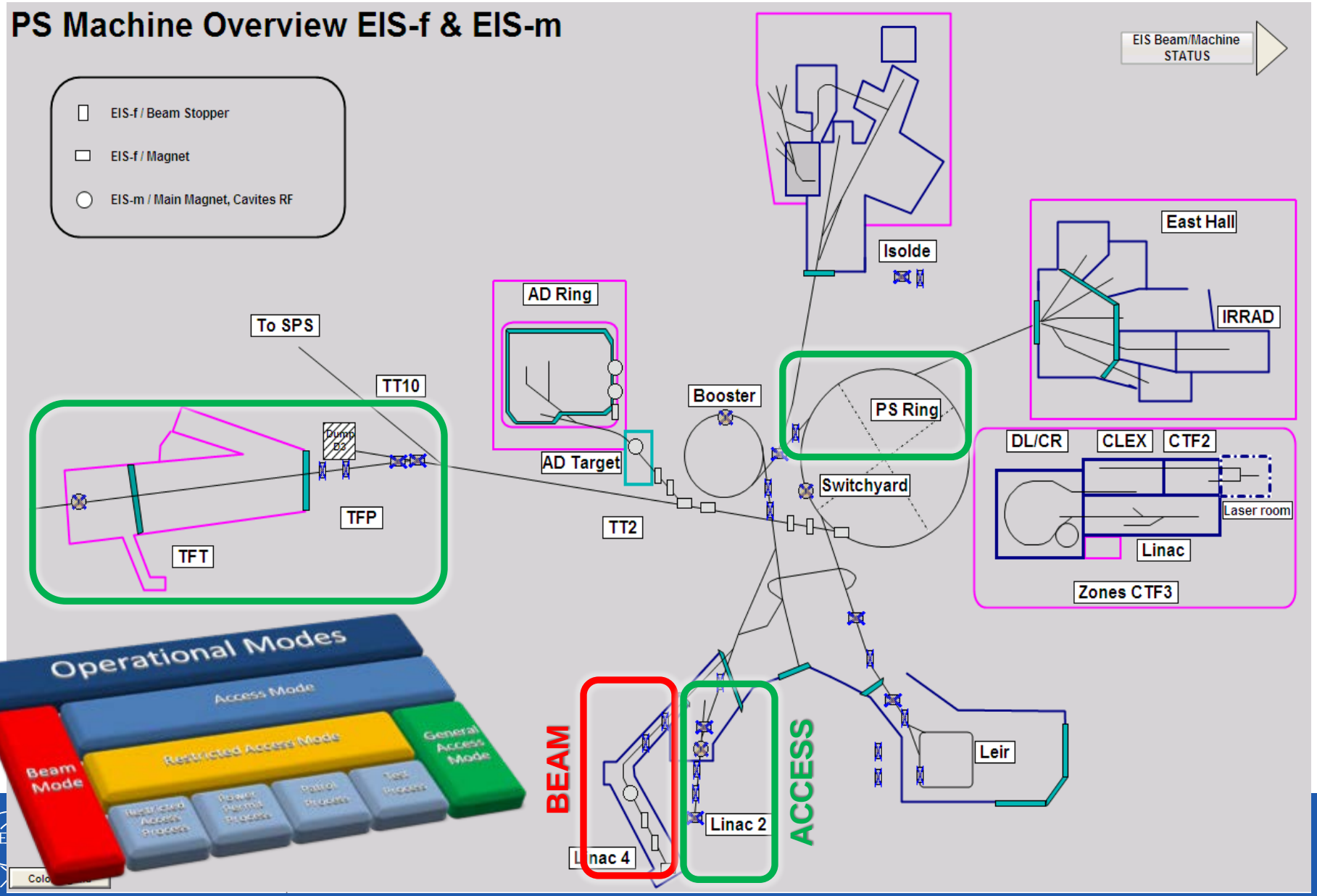
PS-PPS Project Scope



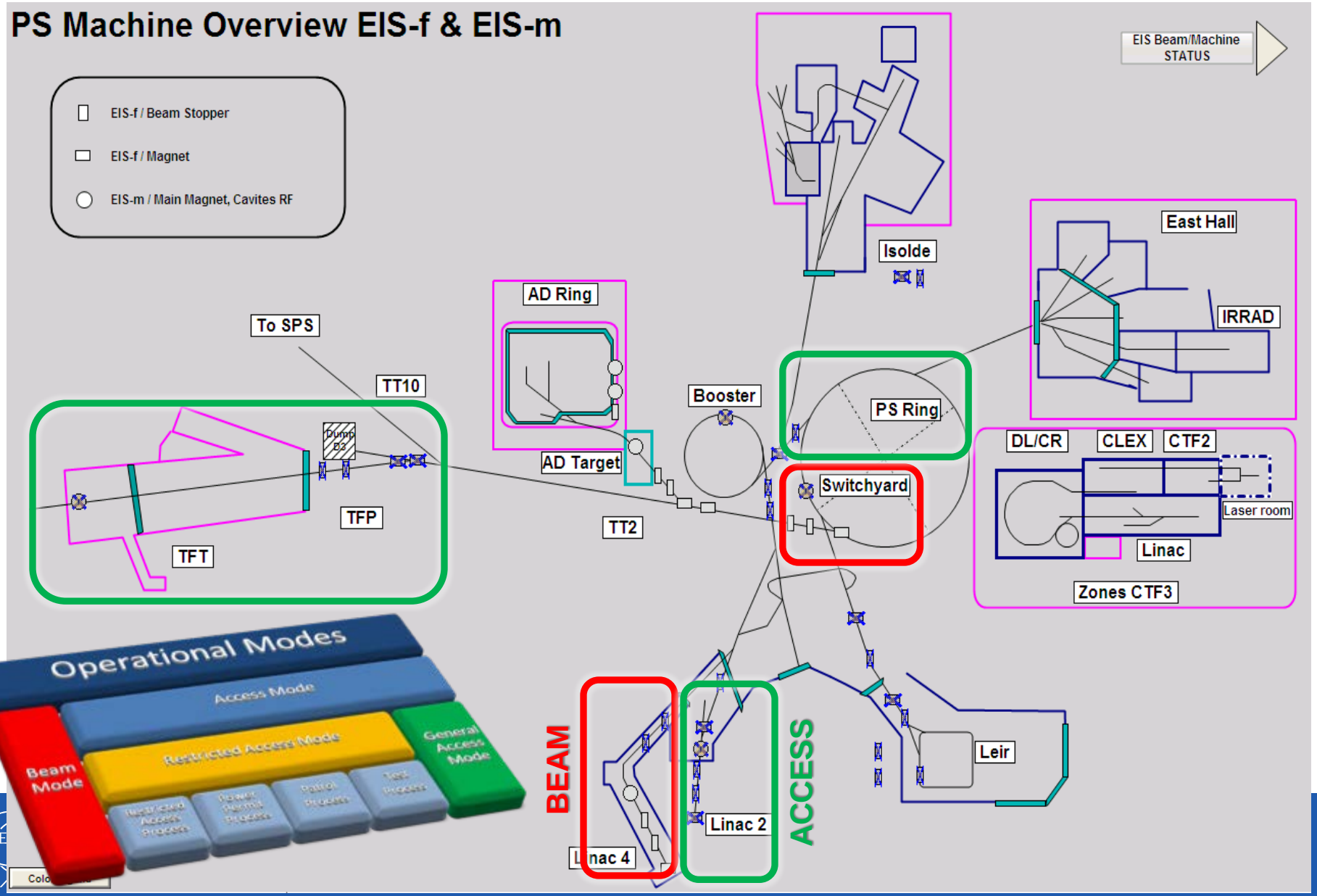
PS-PPS Project Scope



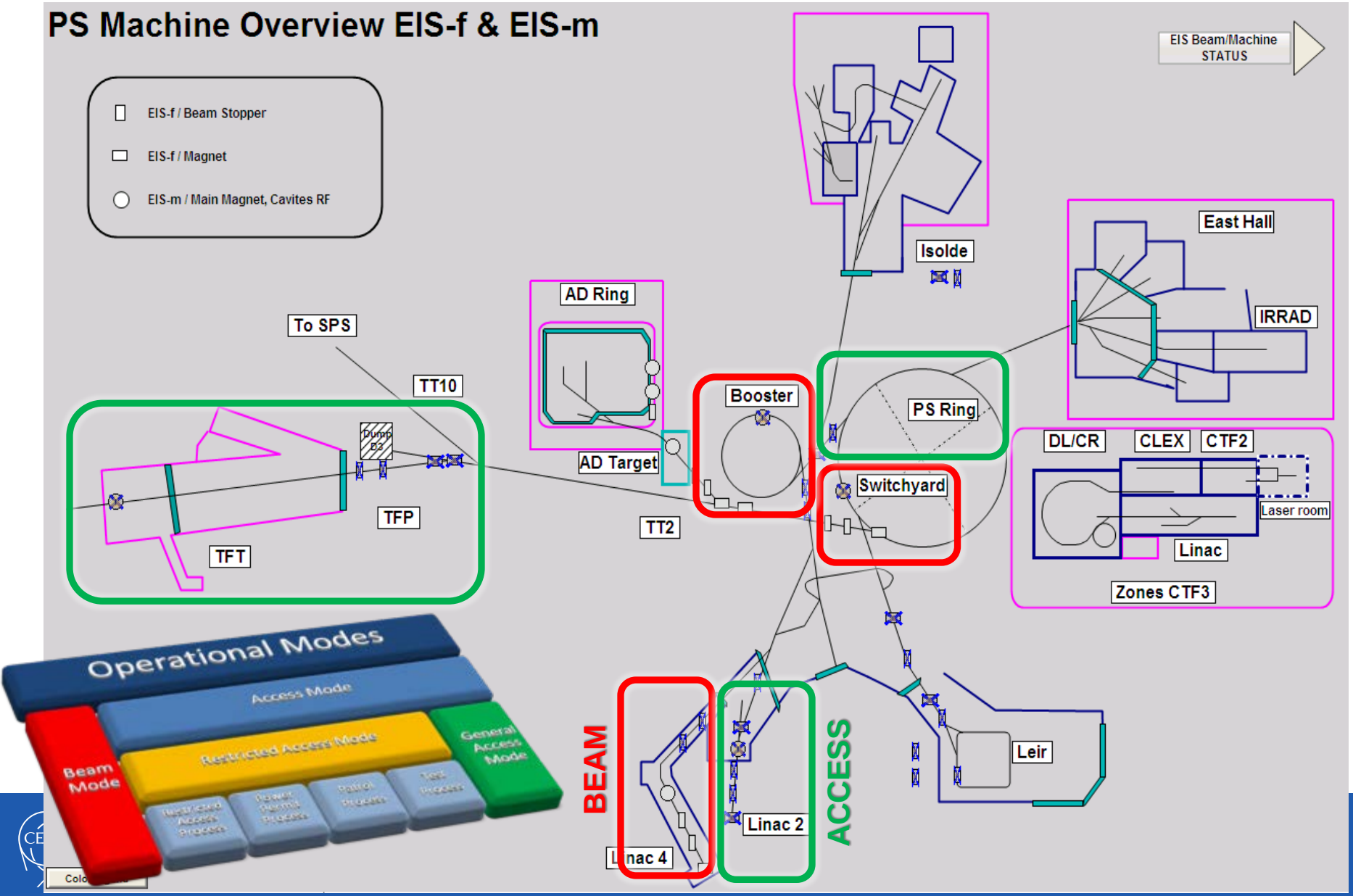
PS-PPS Project Scope



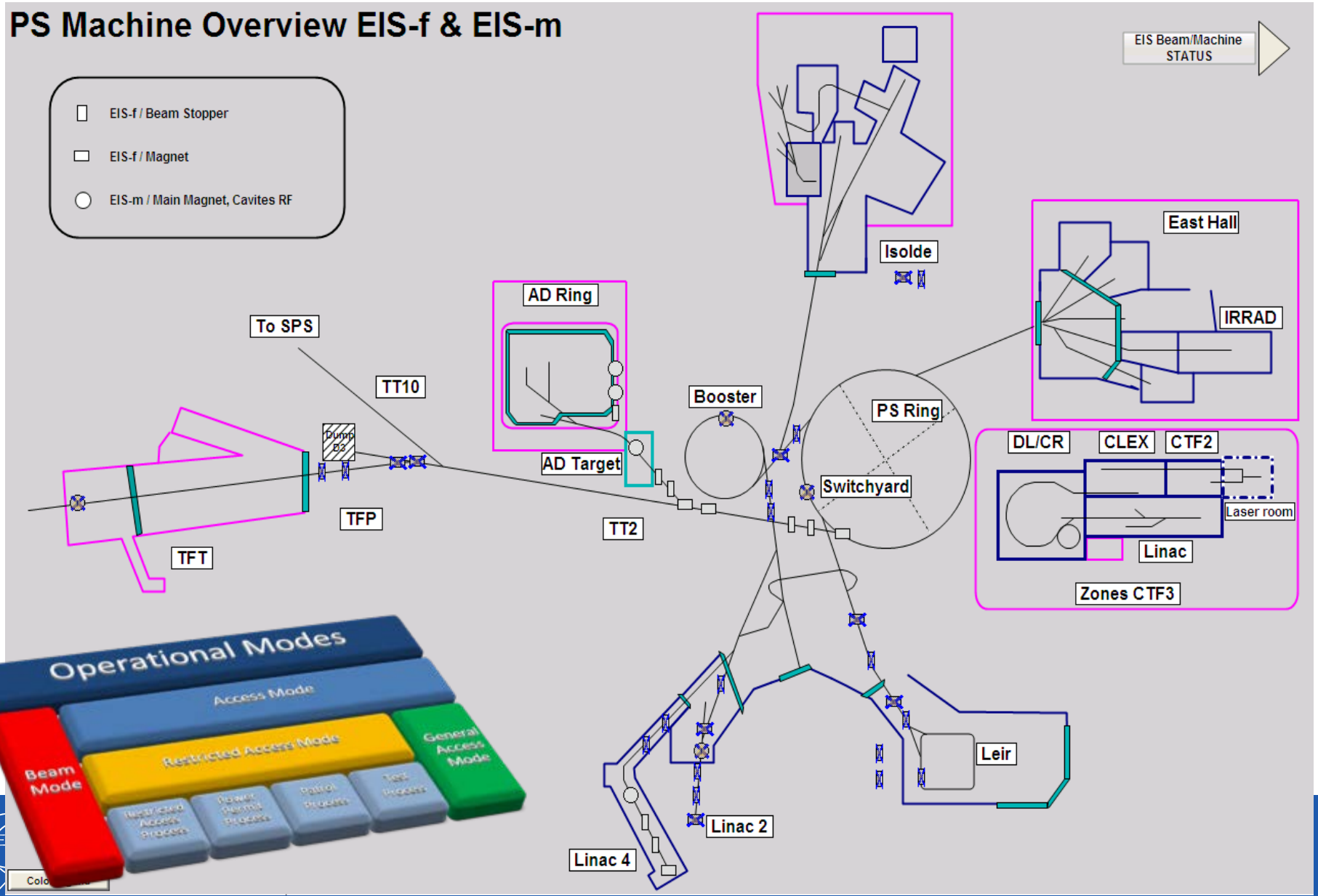
PS-PPS Project Scope



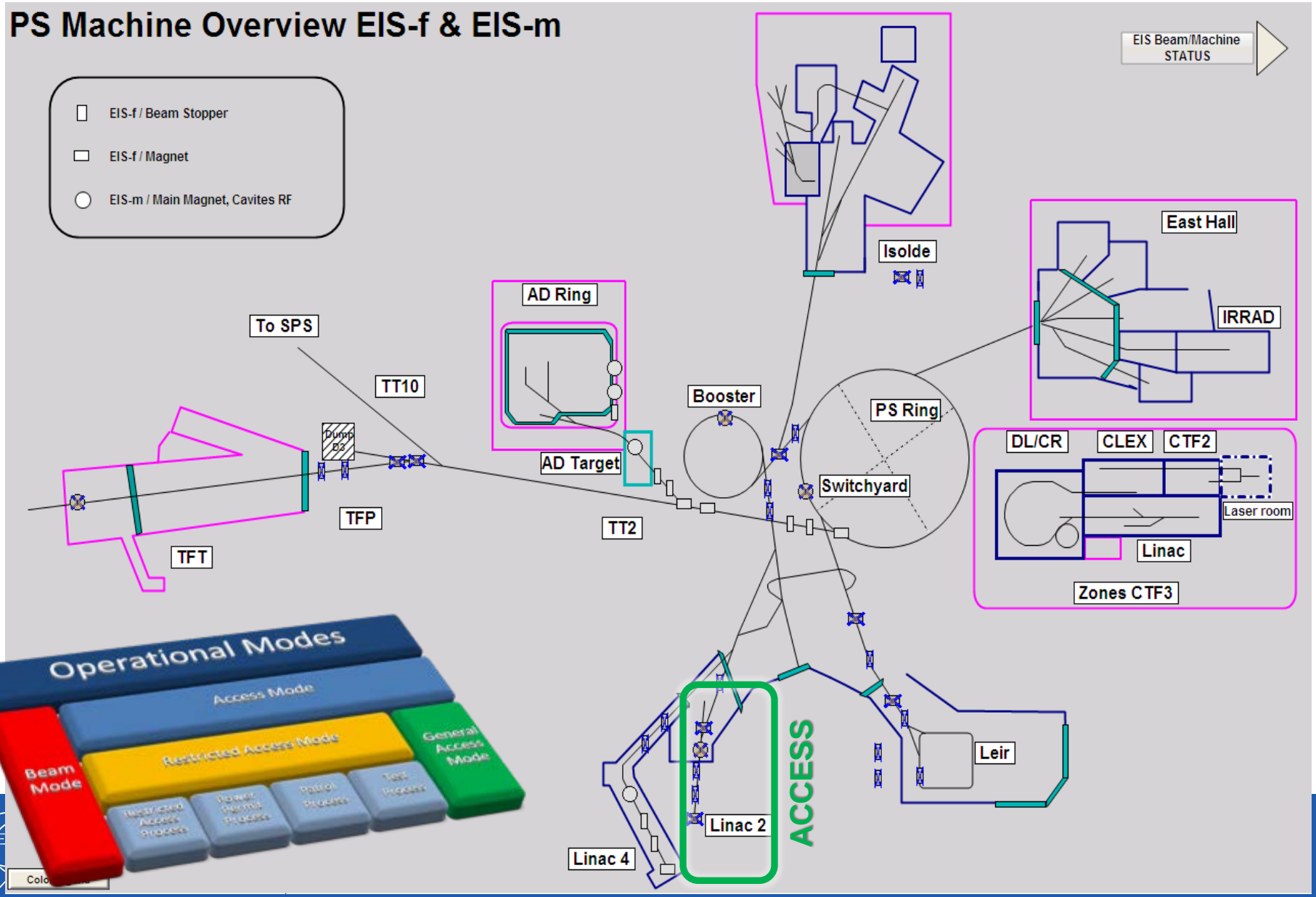
PS-PPS Project Scope



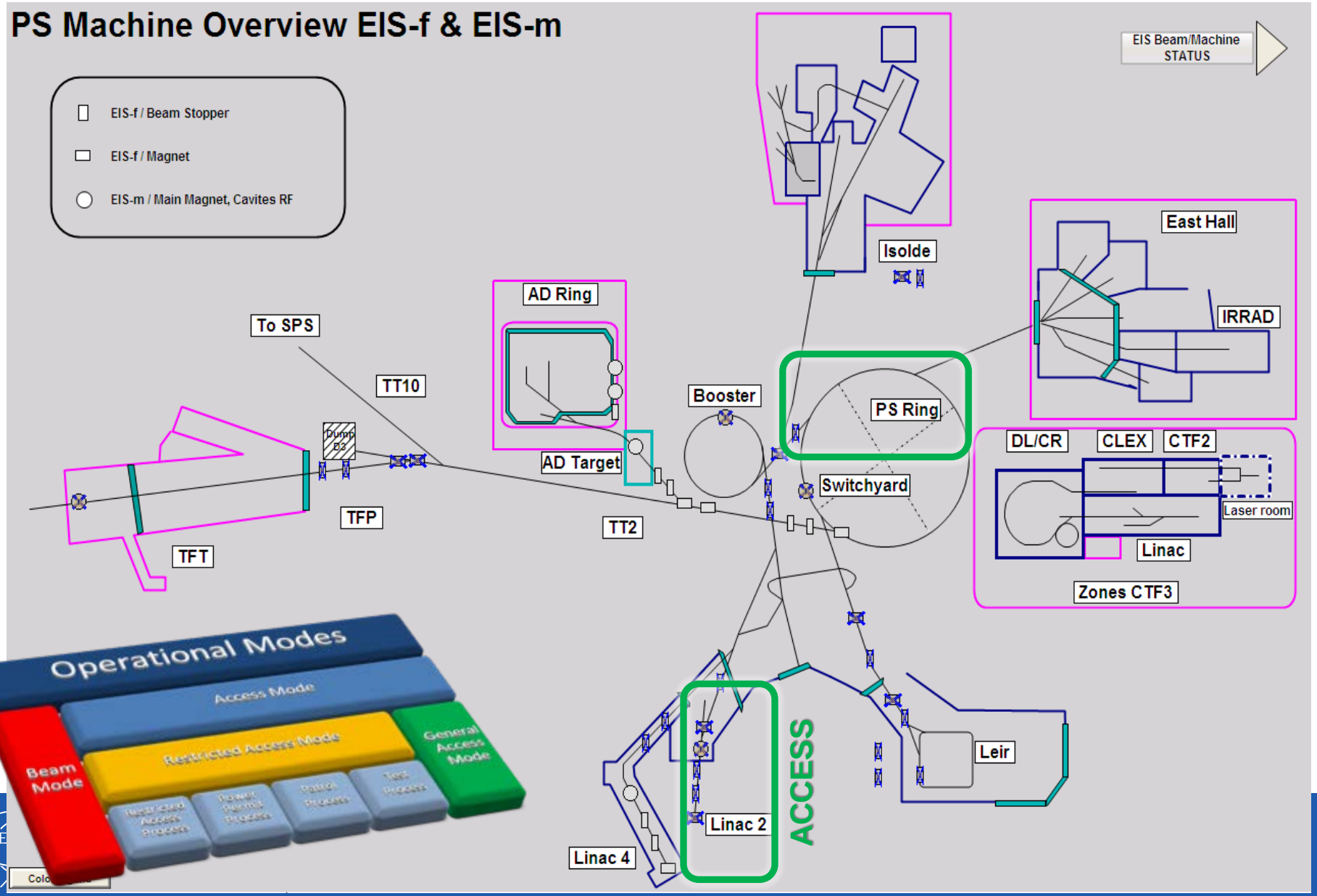
PS-PPS Project Scope



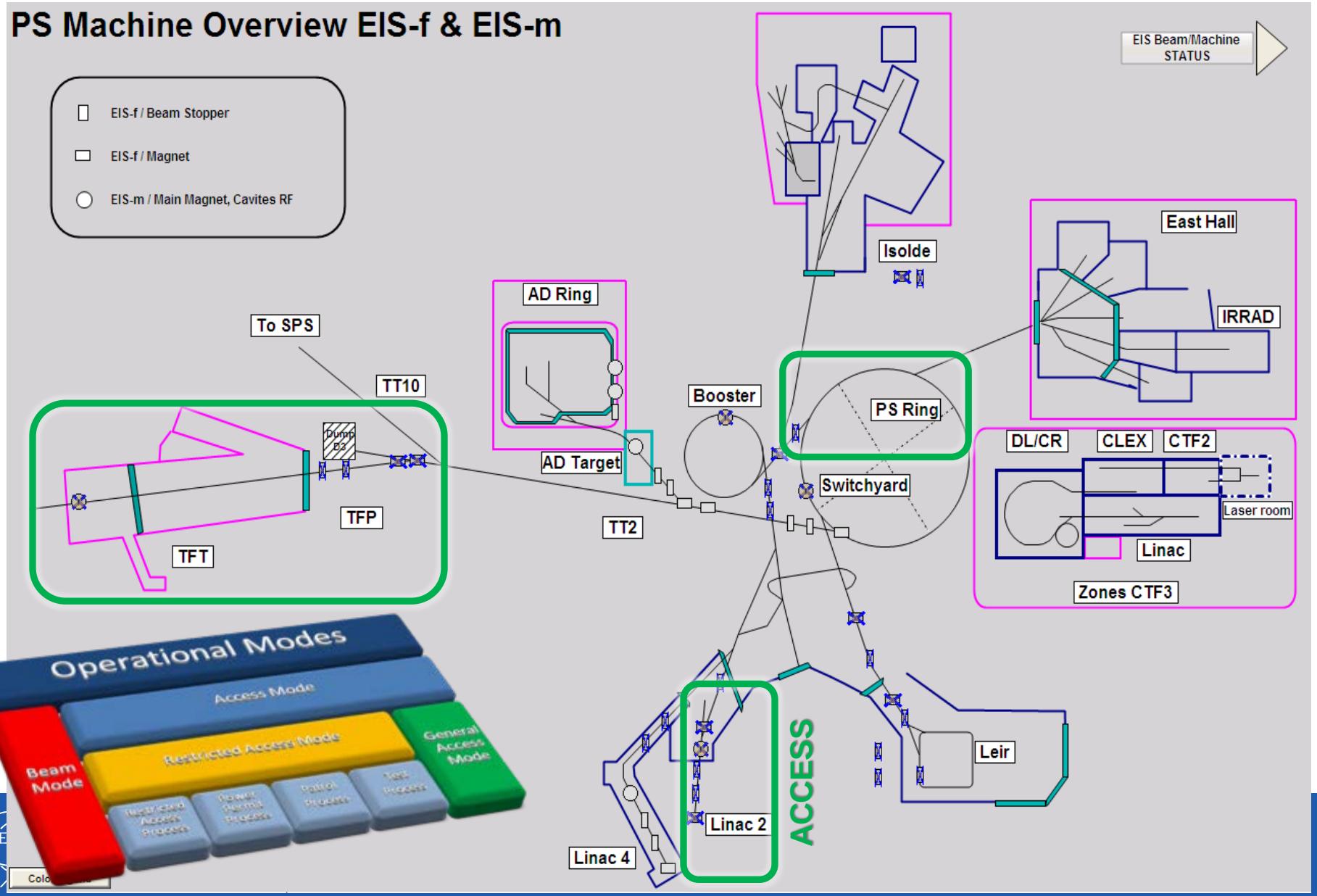
PS-PPS Project Scope



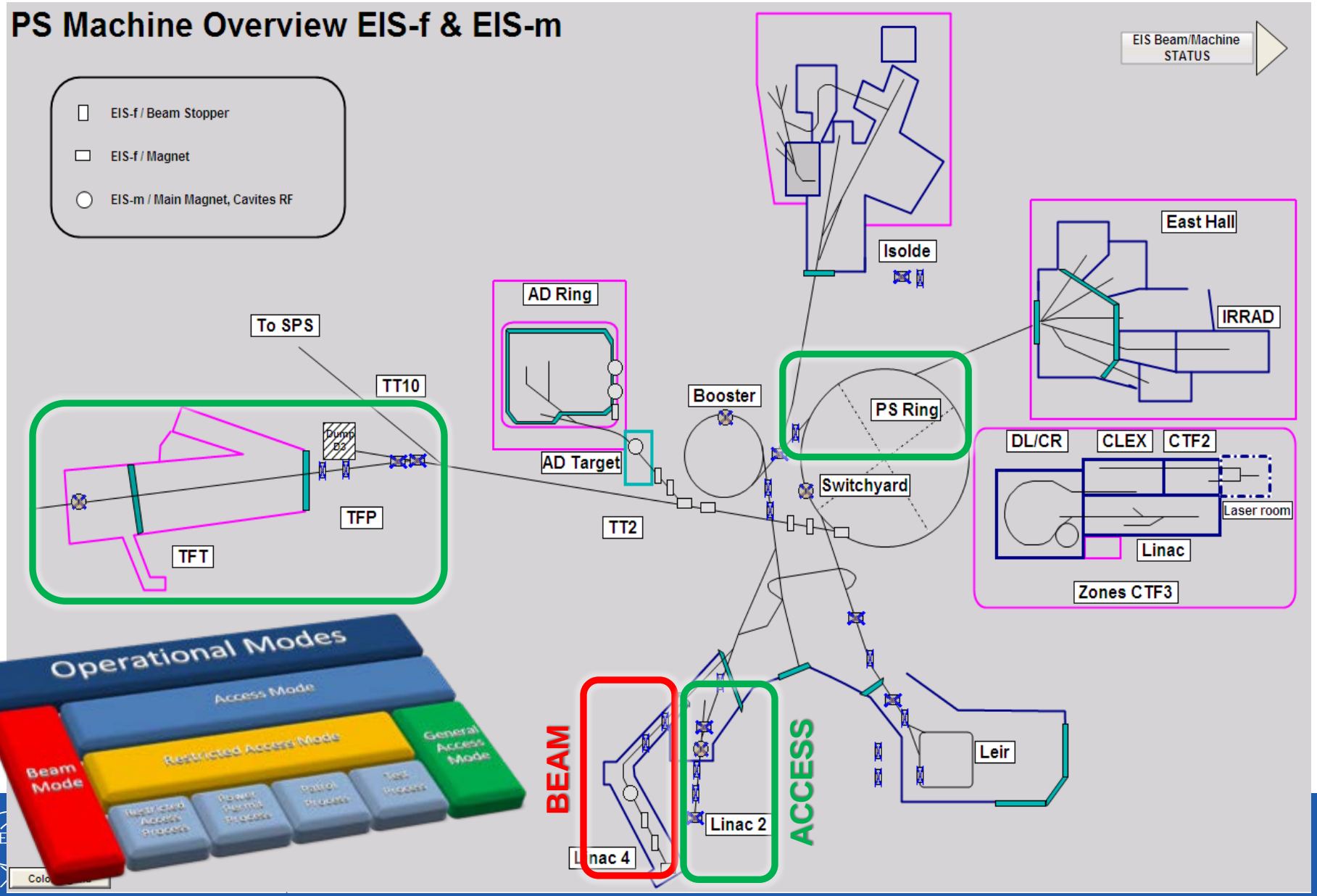
PS-PPS Project Scope



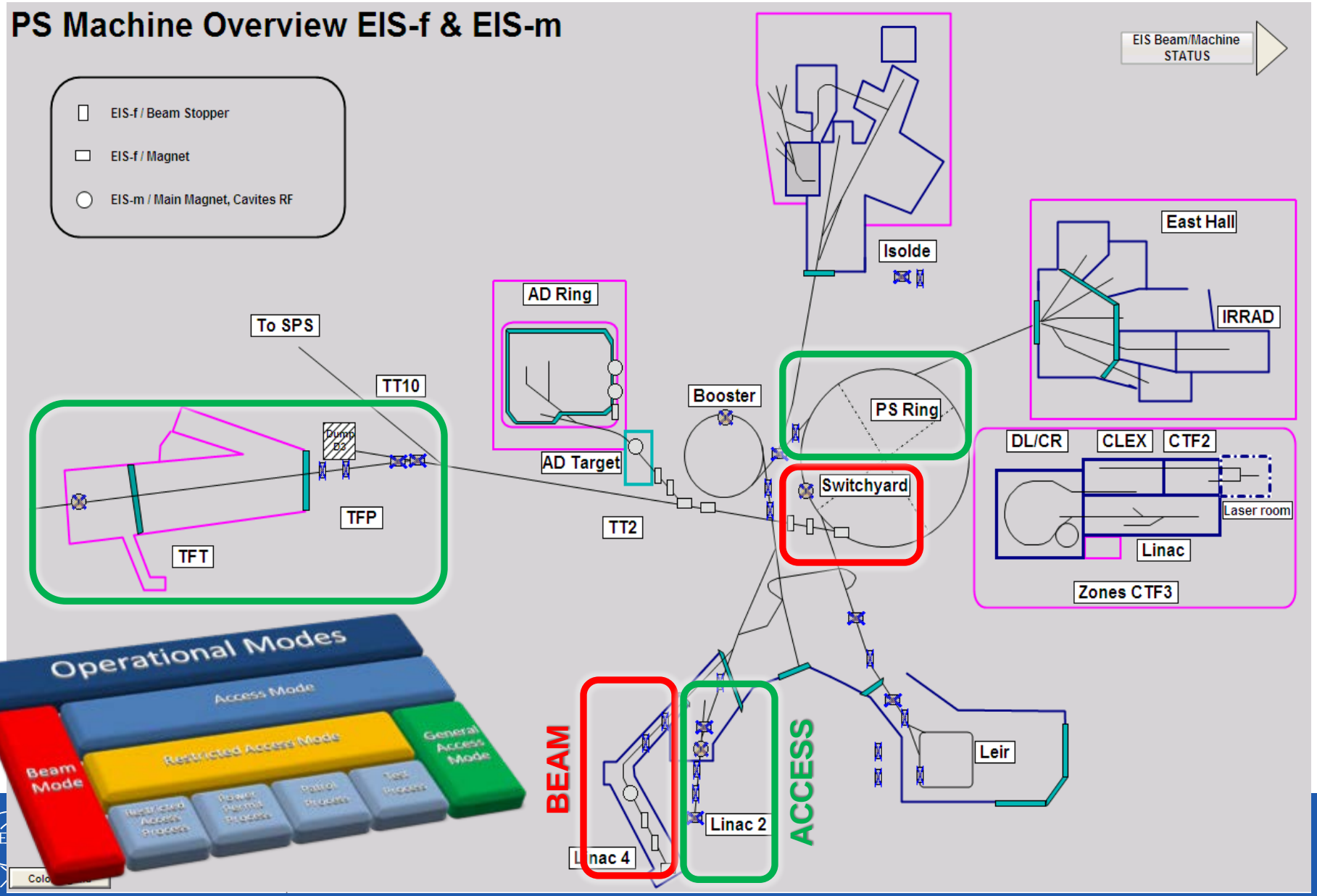
PS-PPS Project Scope



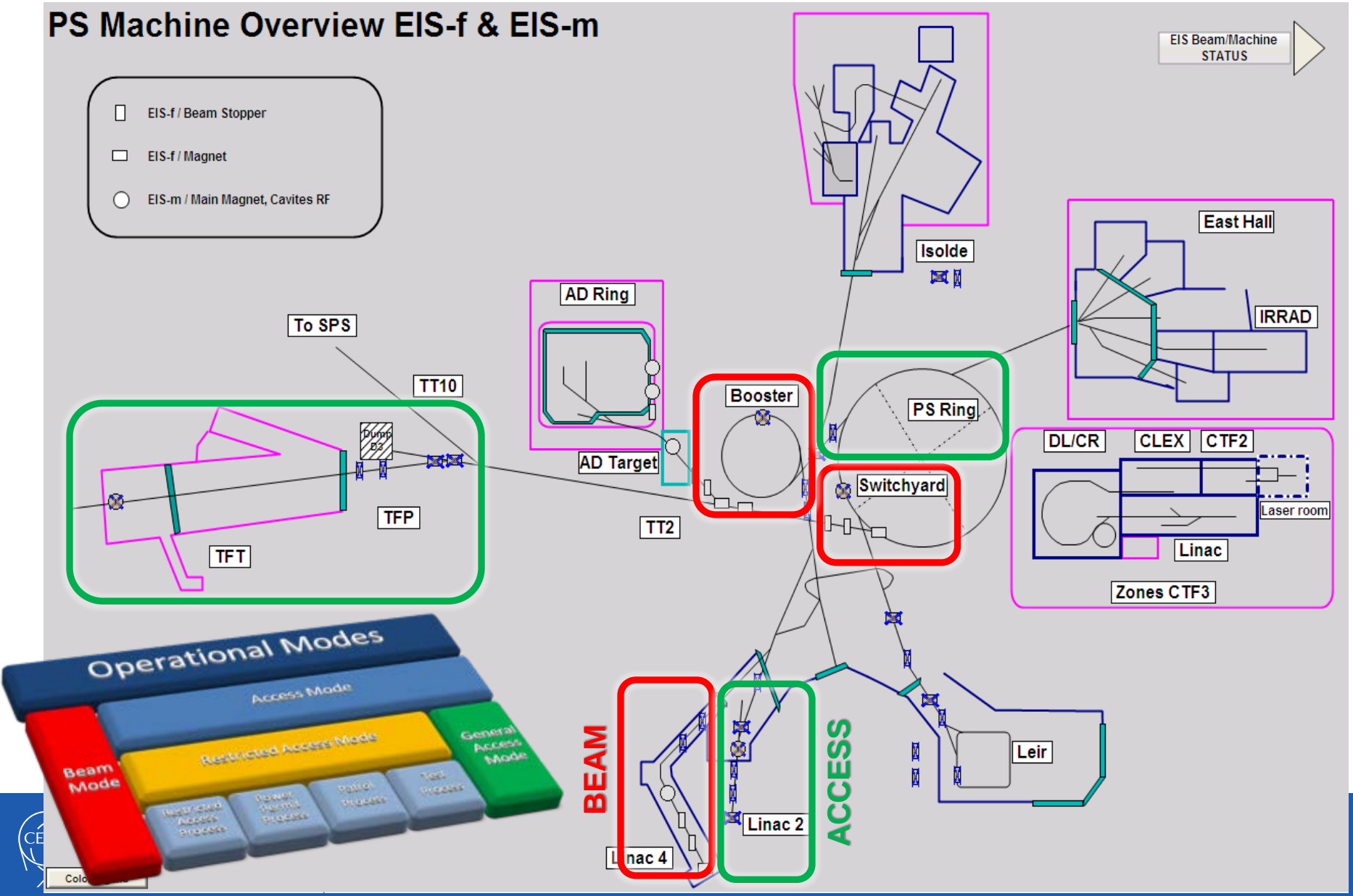
PS-PPS Project Scope



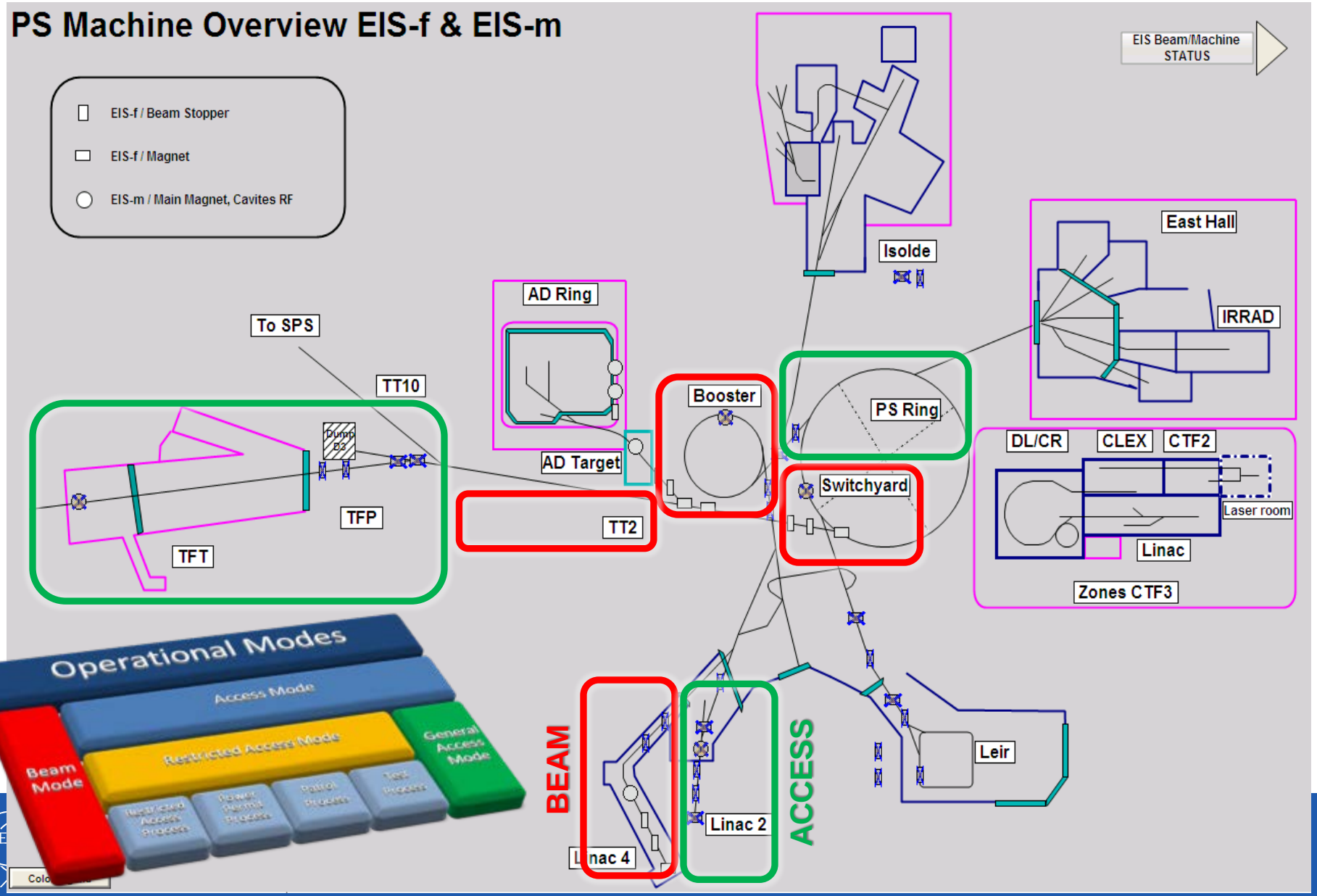
PS-PPS Project Scope



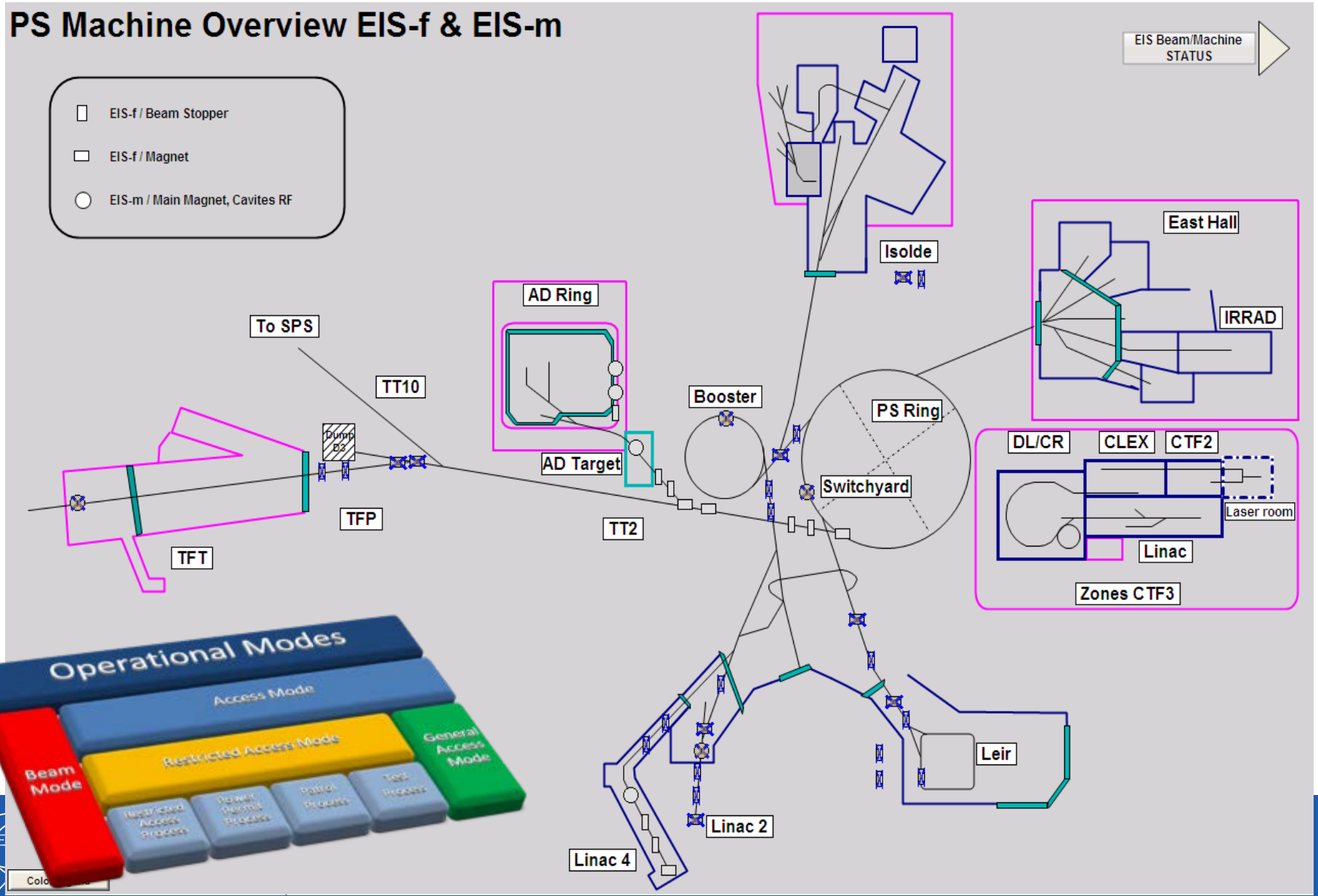
PS-PPS Project Scope



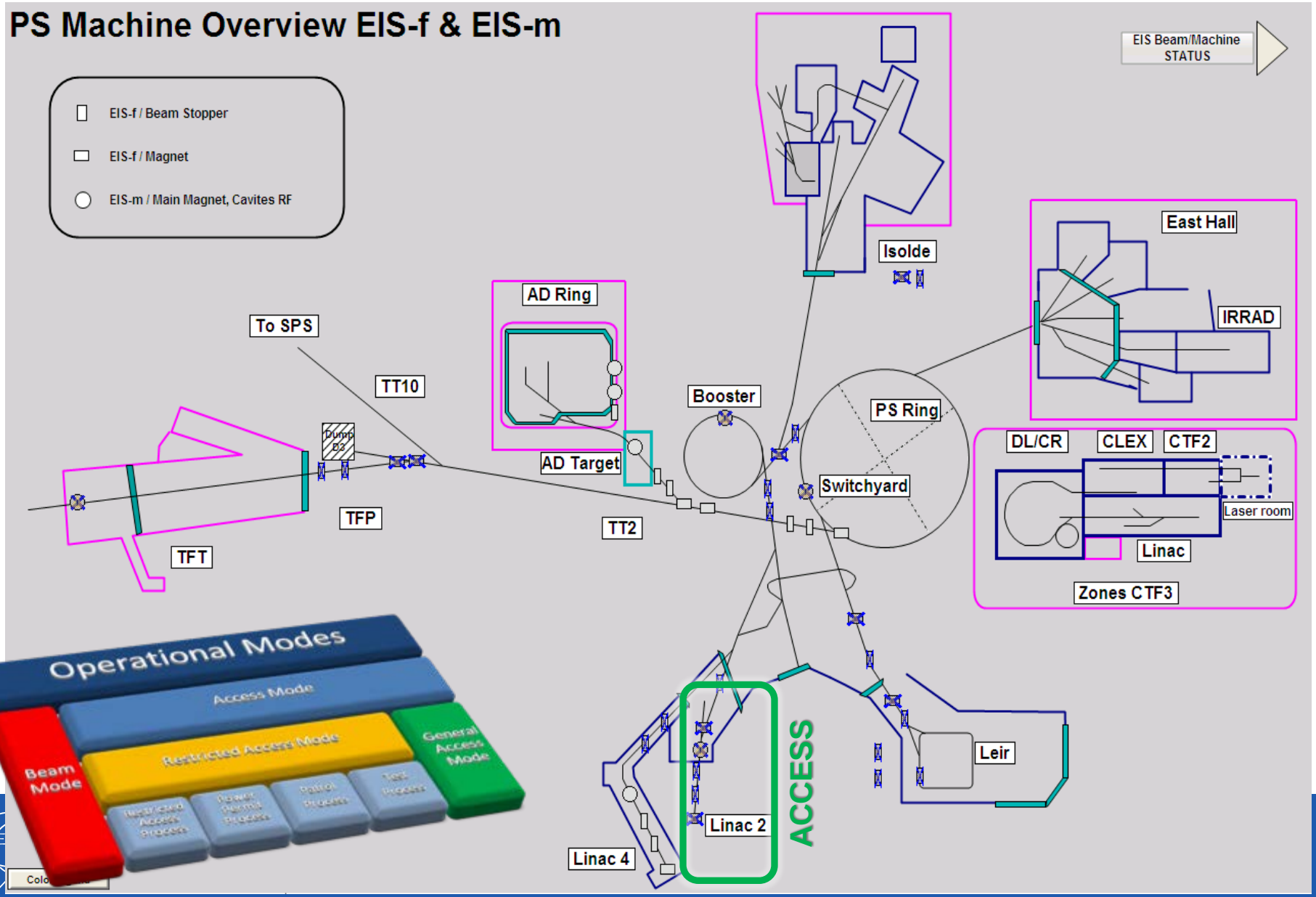
PS-PPS Project Scope



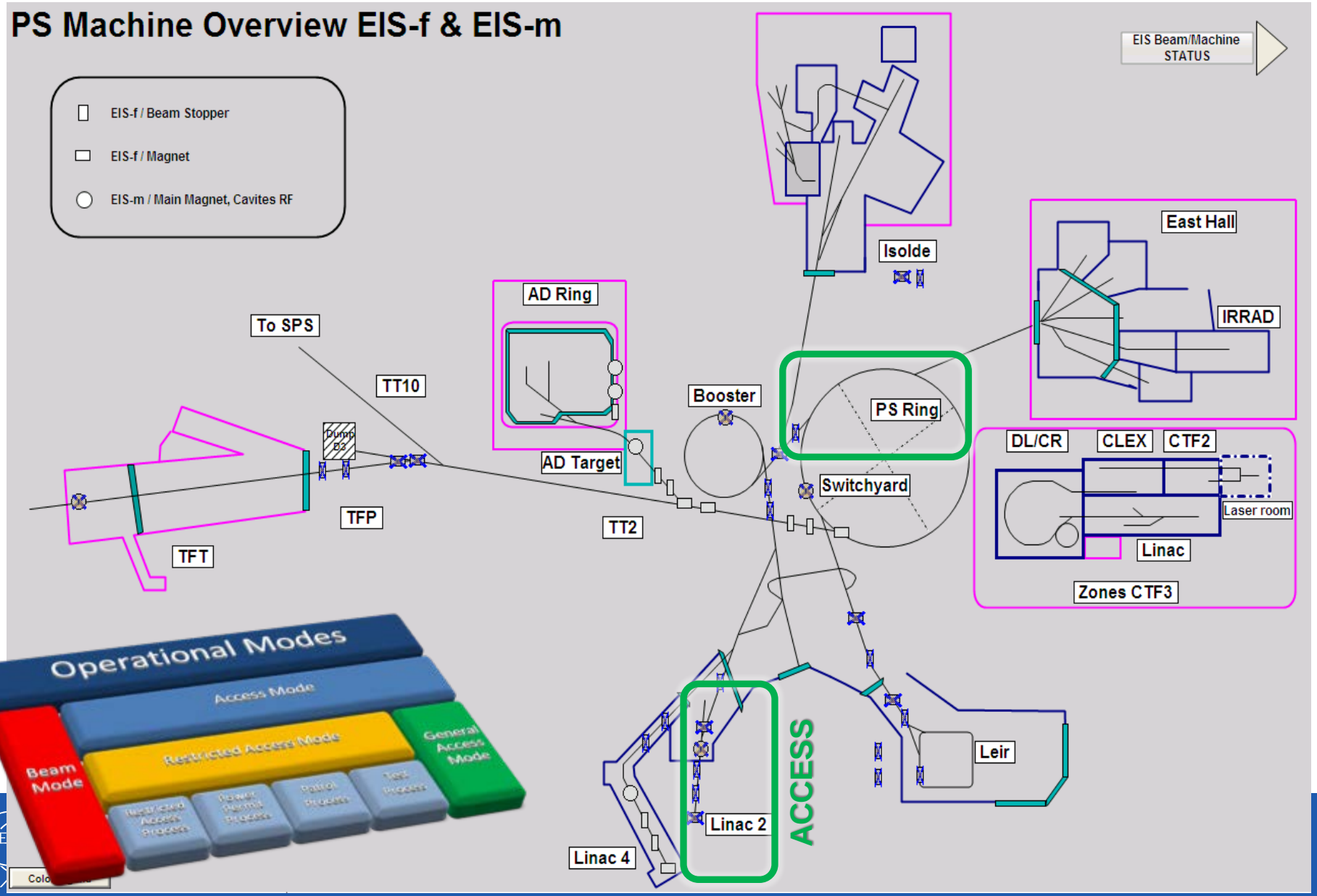
PS-PPS Project Scope



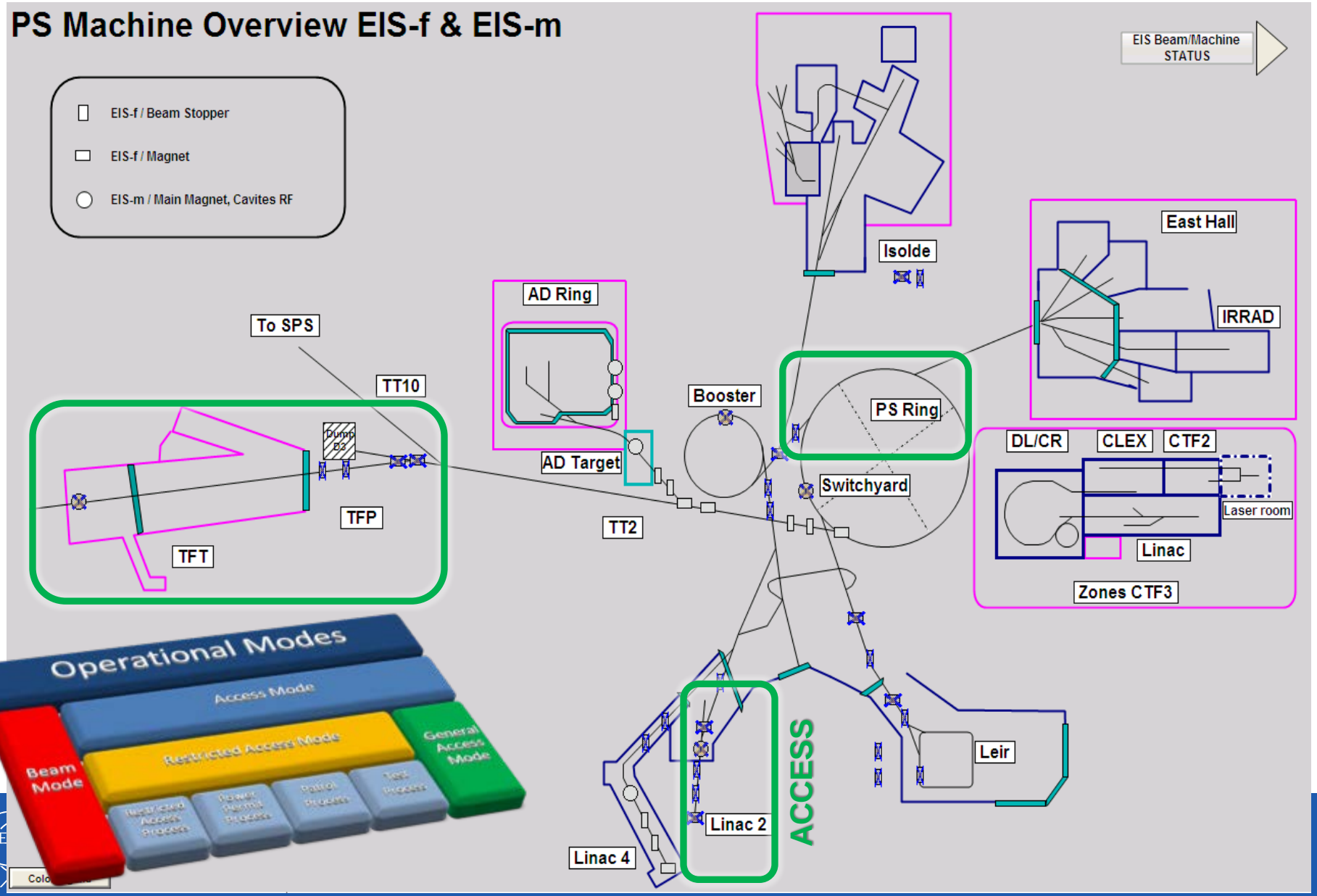
PS-PPS Project Scope



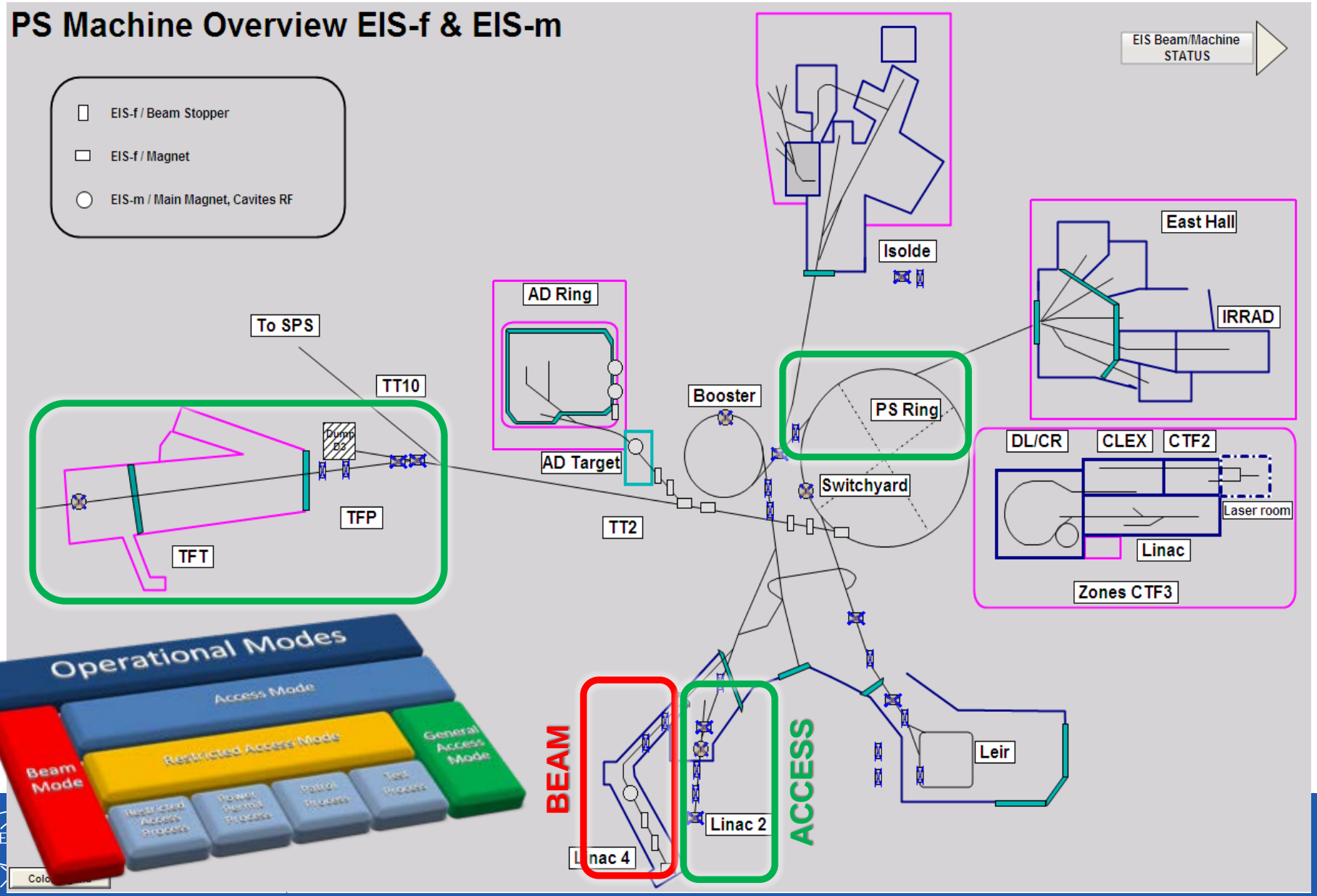
PS-PPS Project Scope



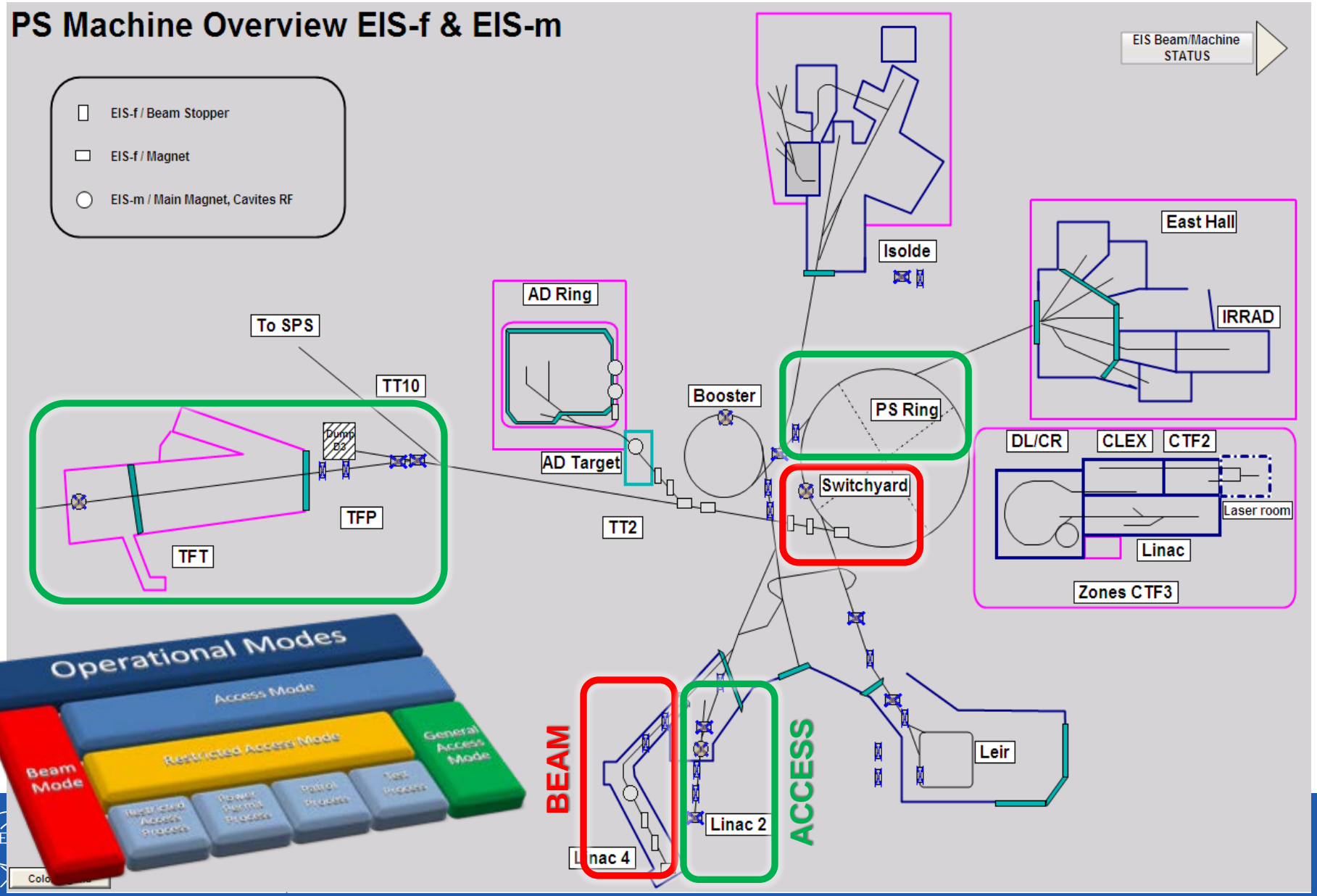
PS-PPS Project Scope



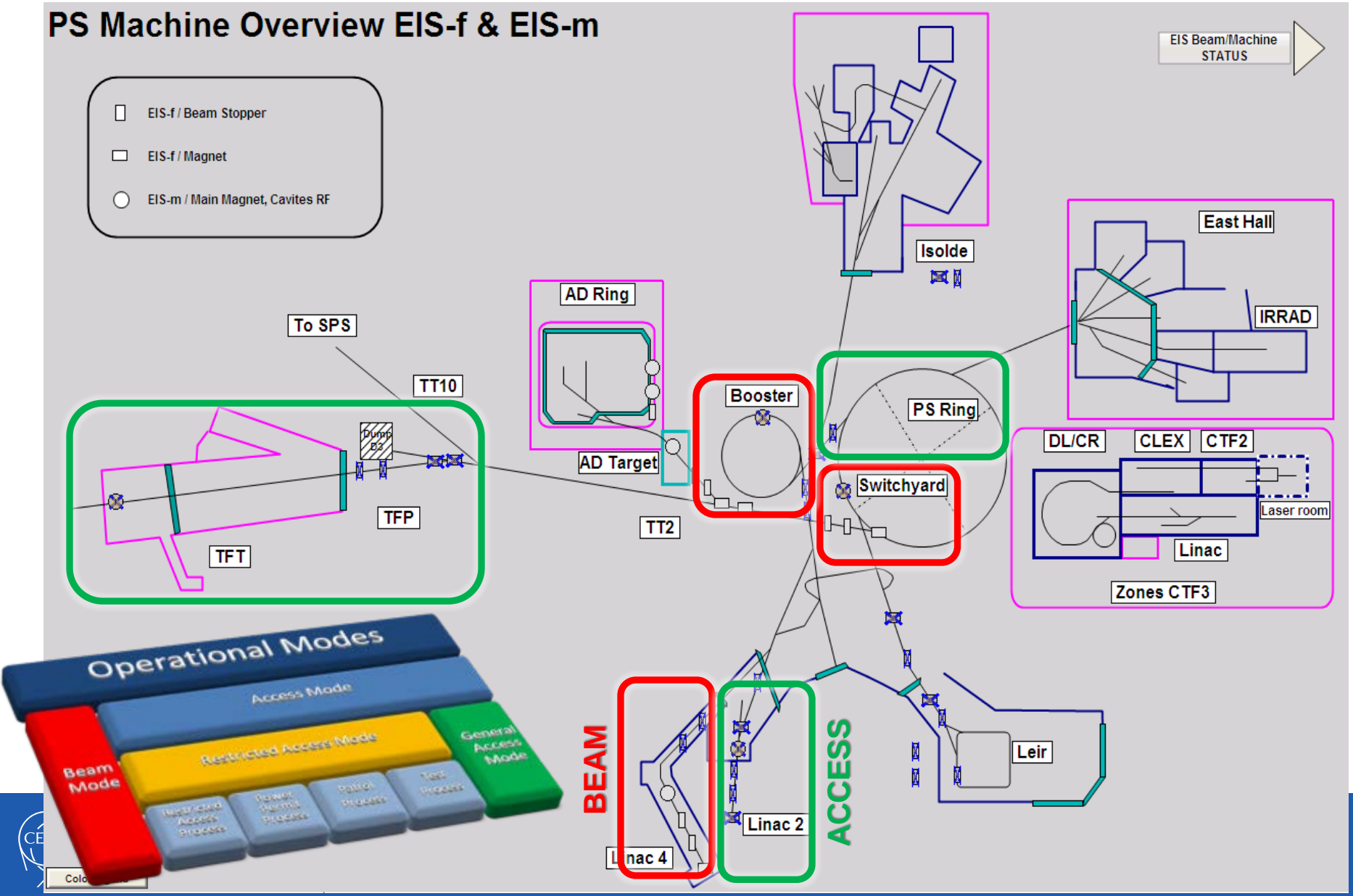
PS-PPS Project Scope



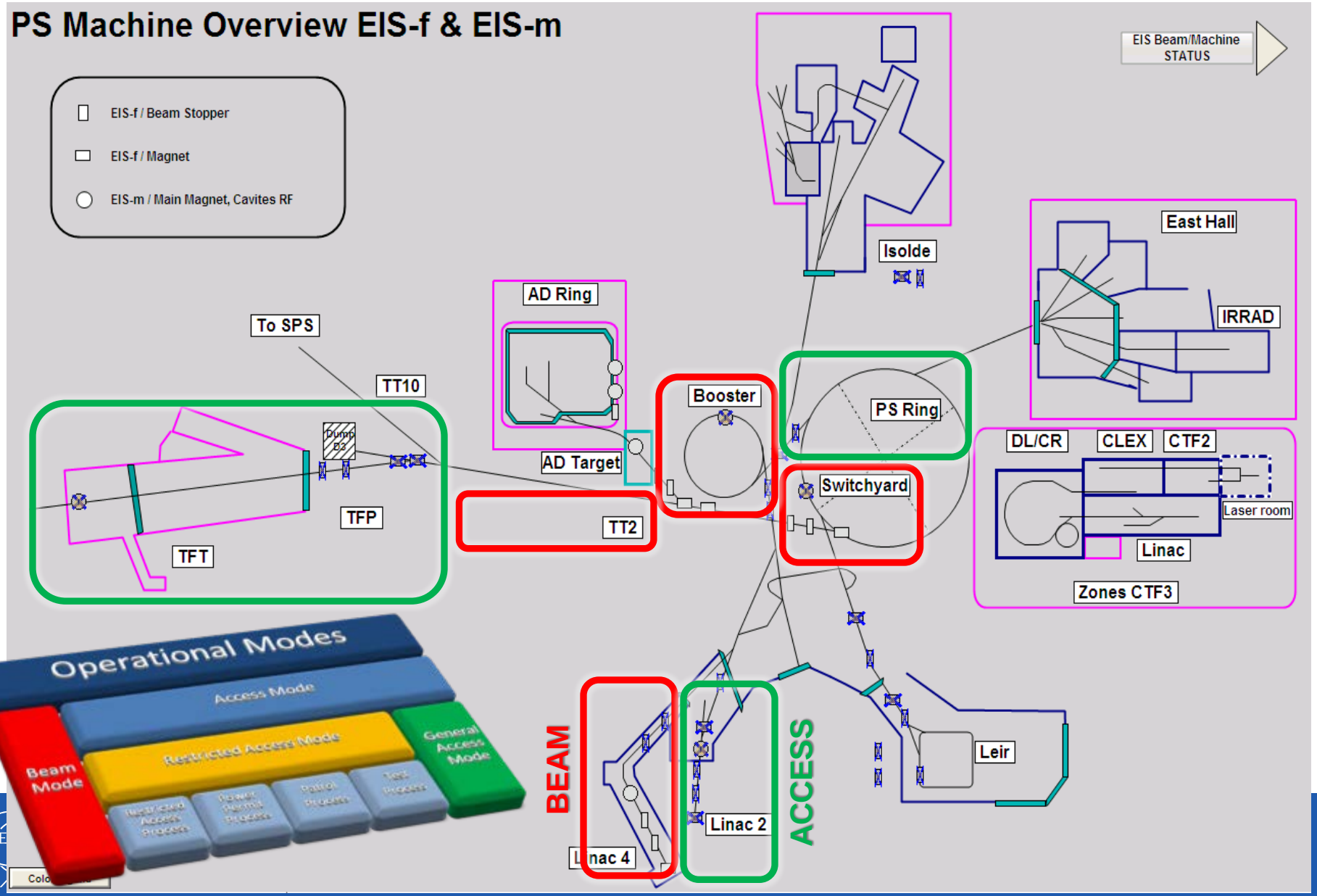
PS-PPS Project Scope



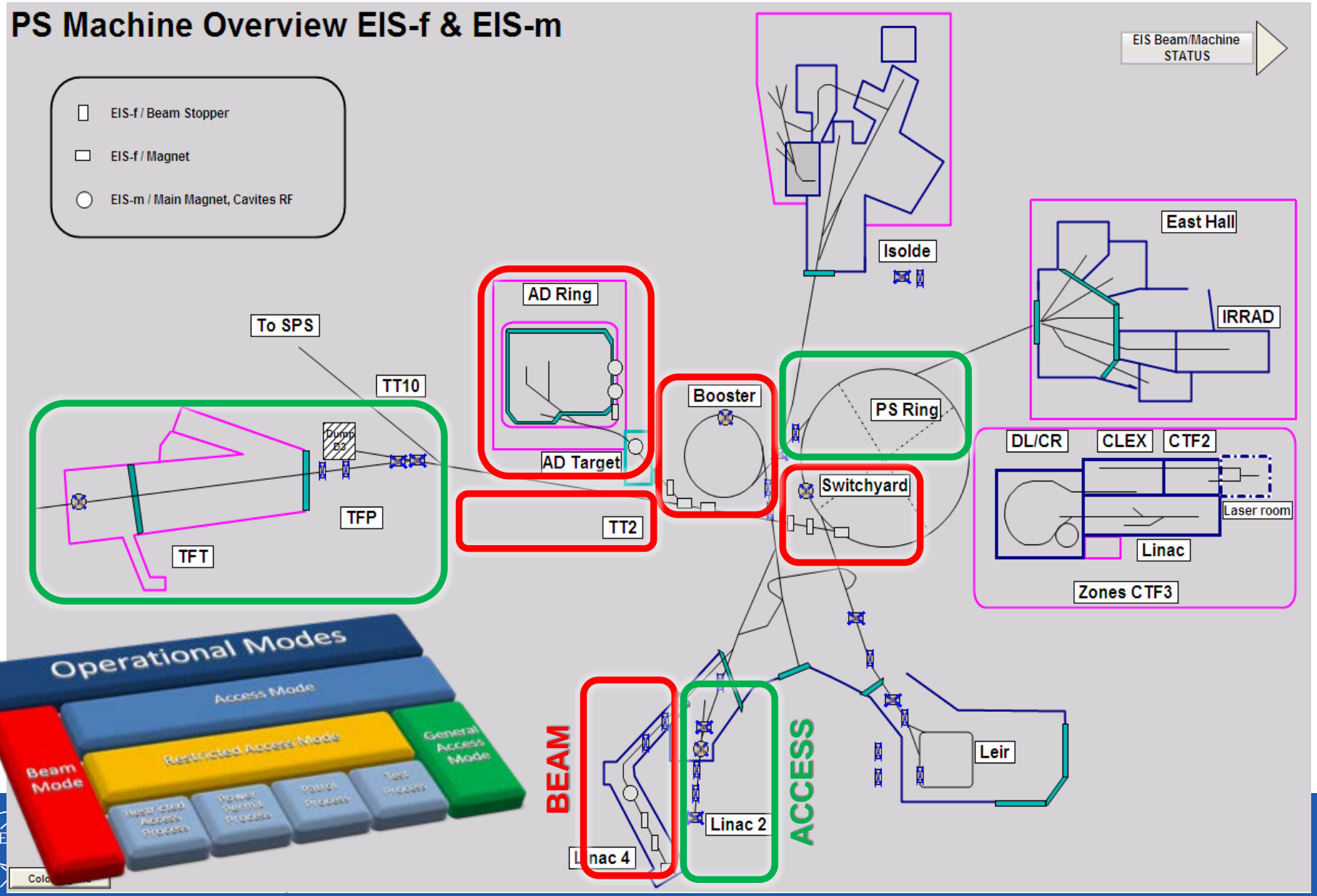
PS-PPS Project Scope



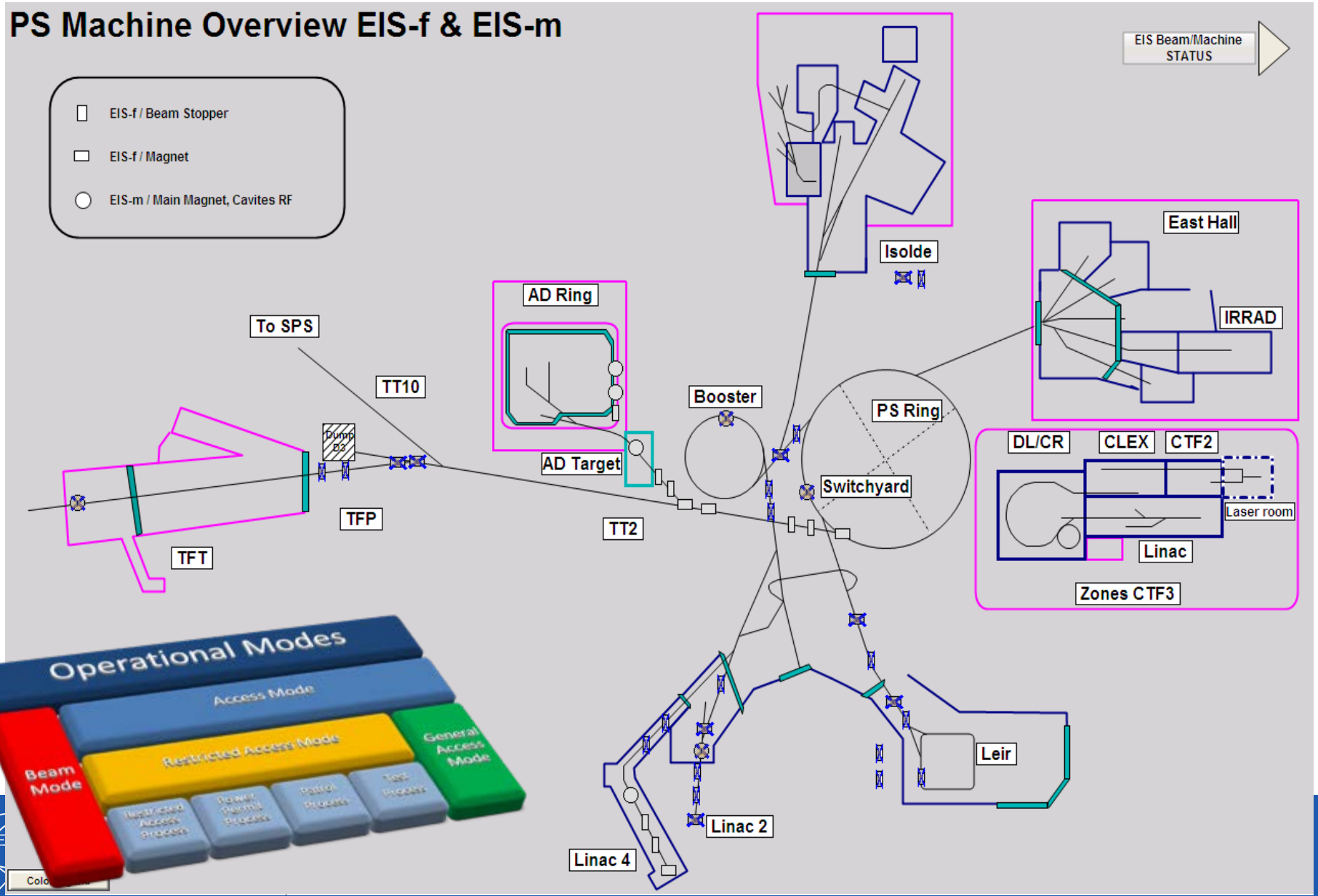
PS-PPS Project Scope



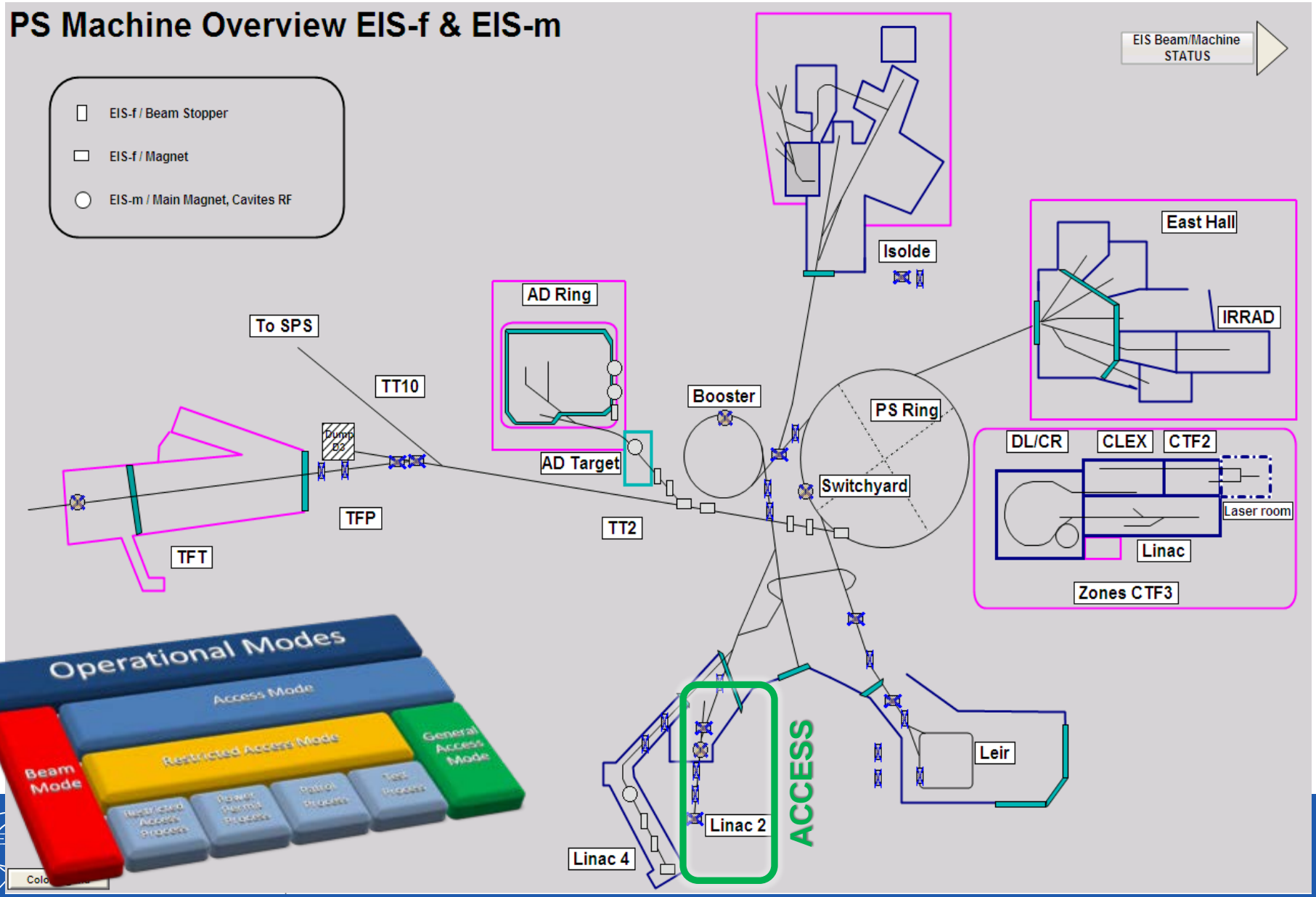
PS-PPS Project Scope



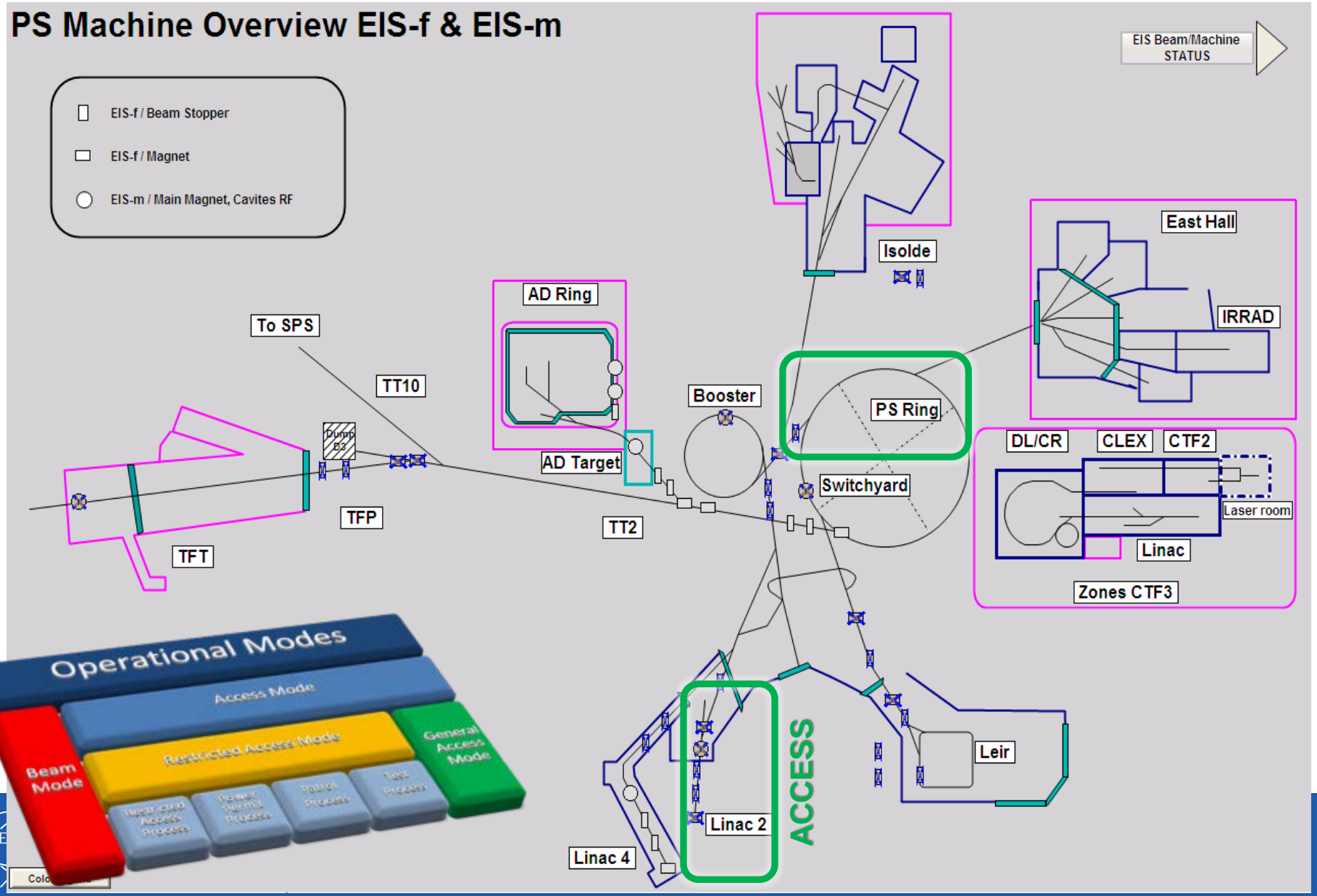
PS-PPS Project Scope



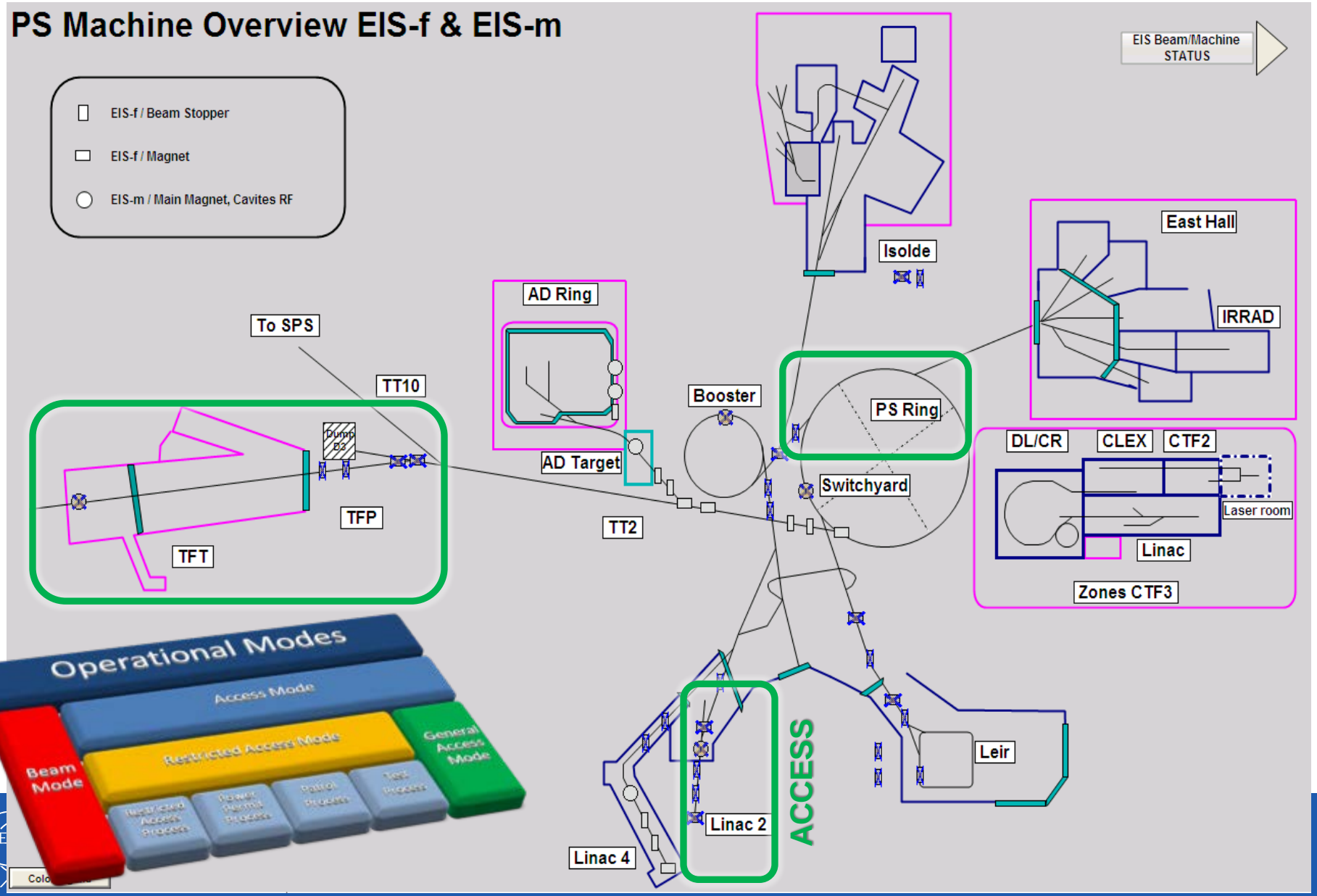
PS-PPS Project Scope



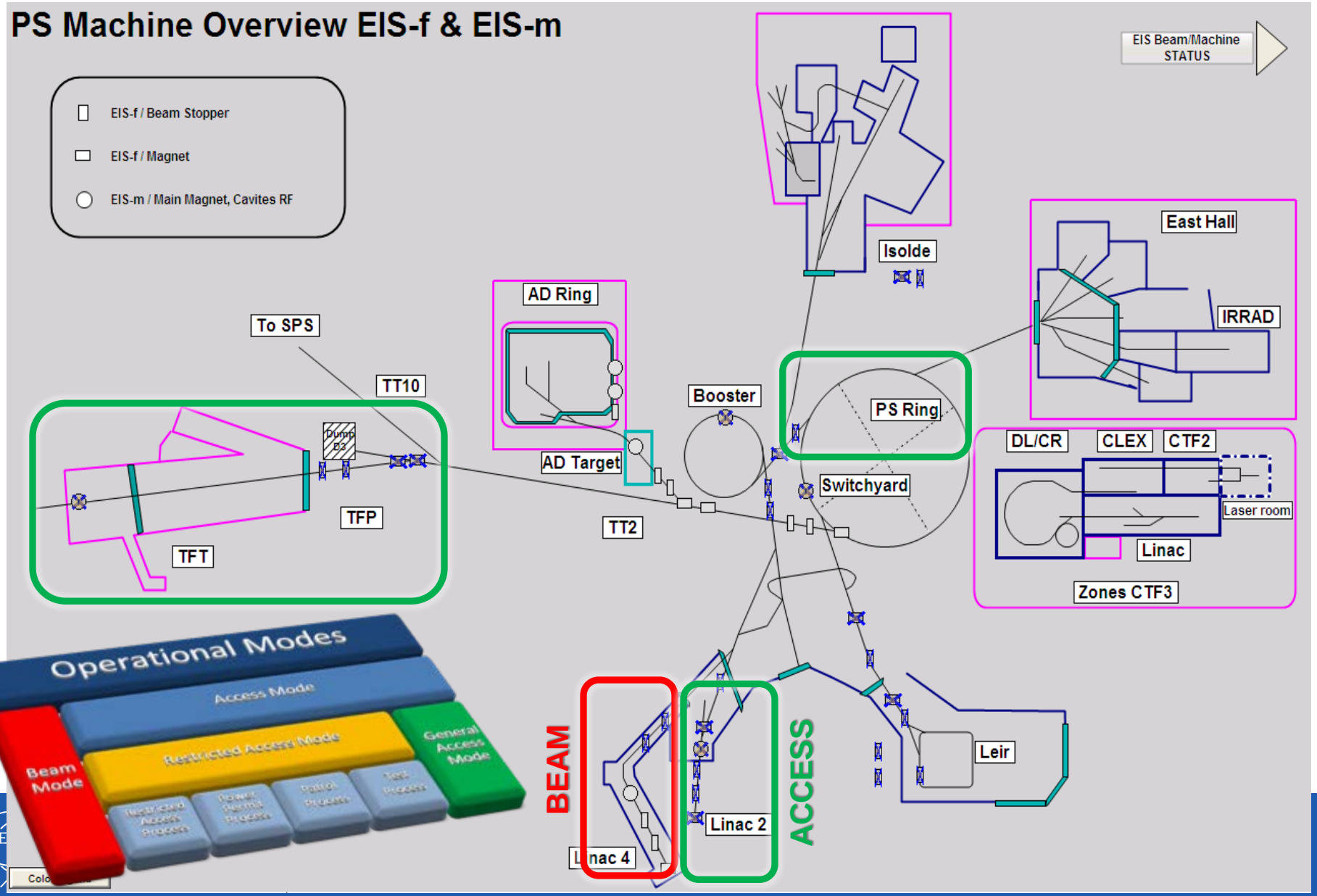
PS-PPS Project Scope



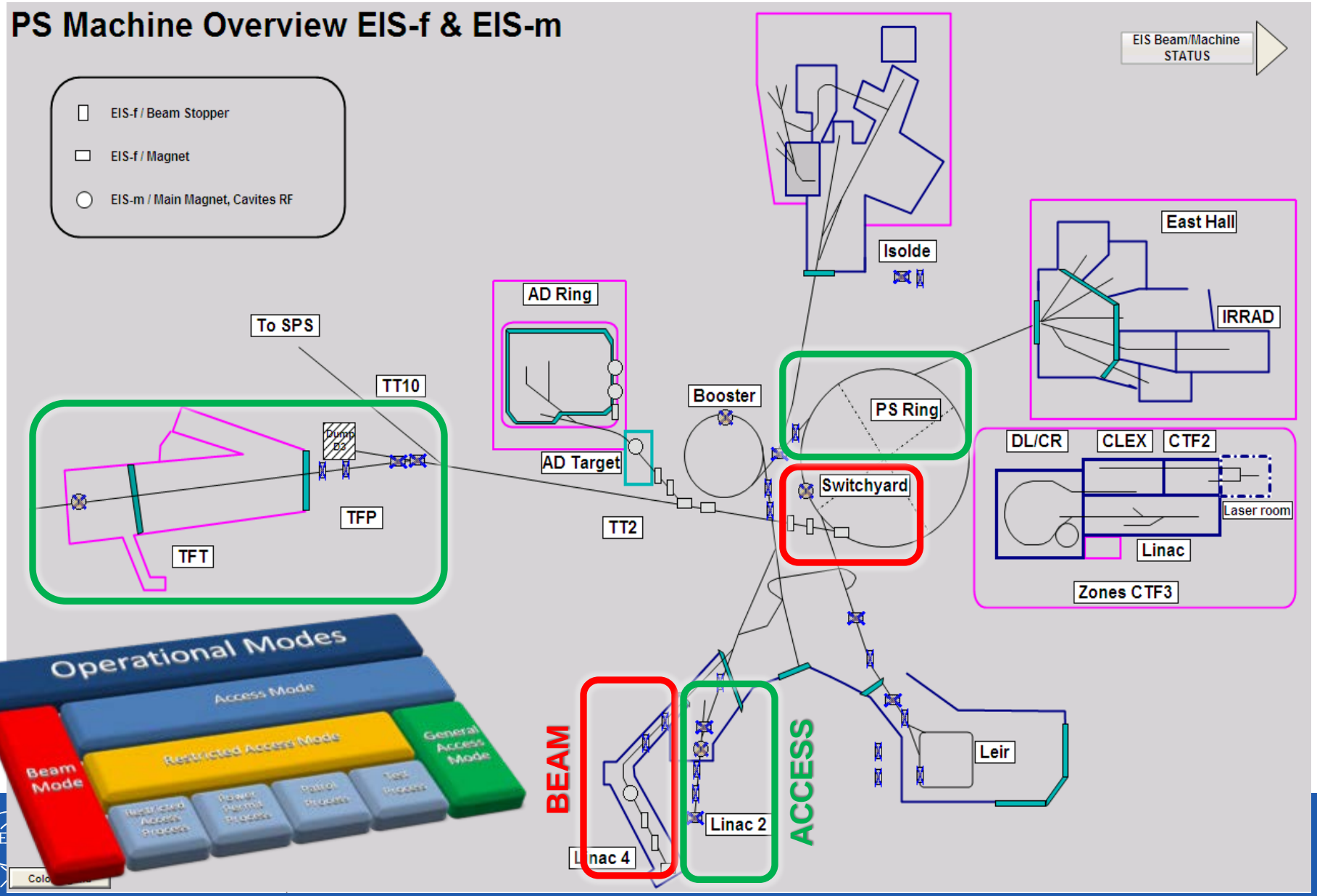
PS-PPS Project Scope



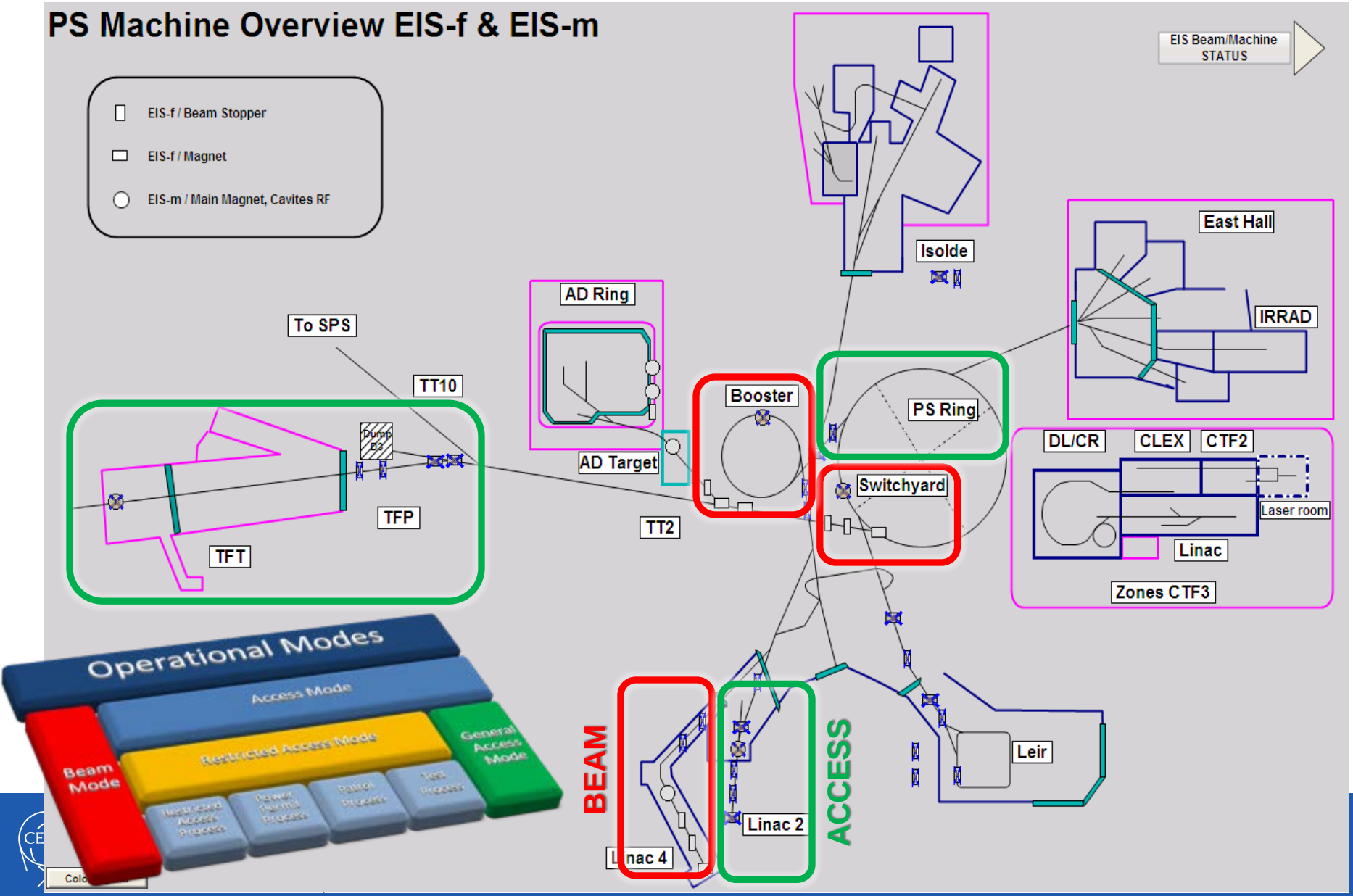
PS-PPS Project Scope



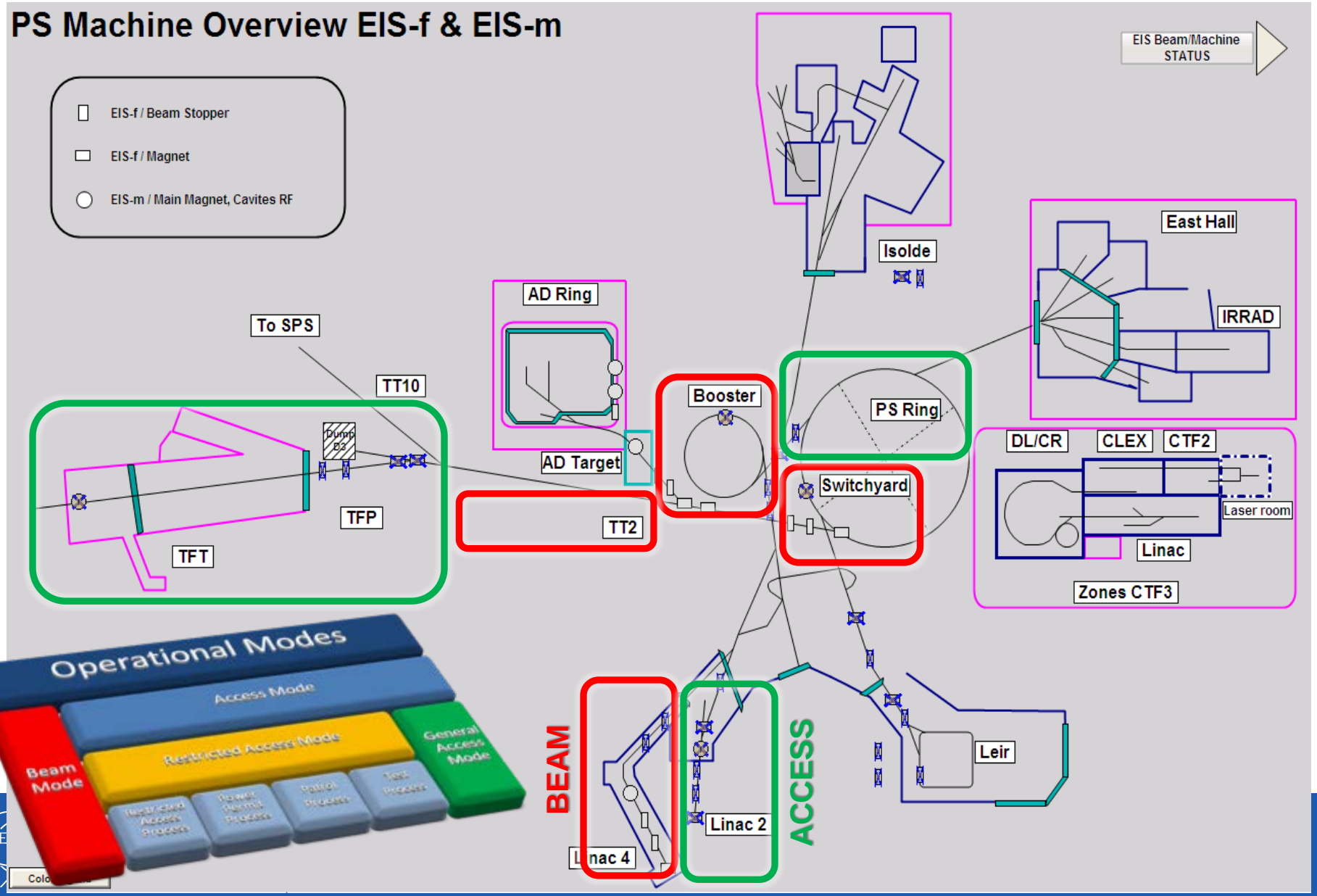
PS-PPS Project Scope



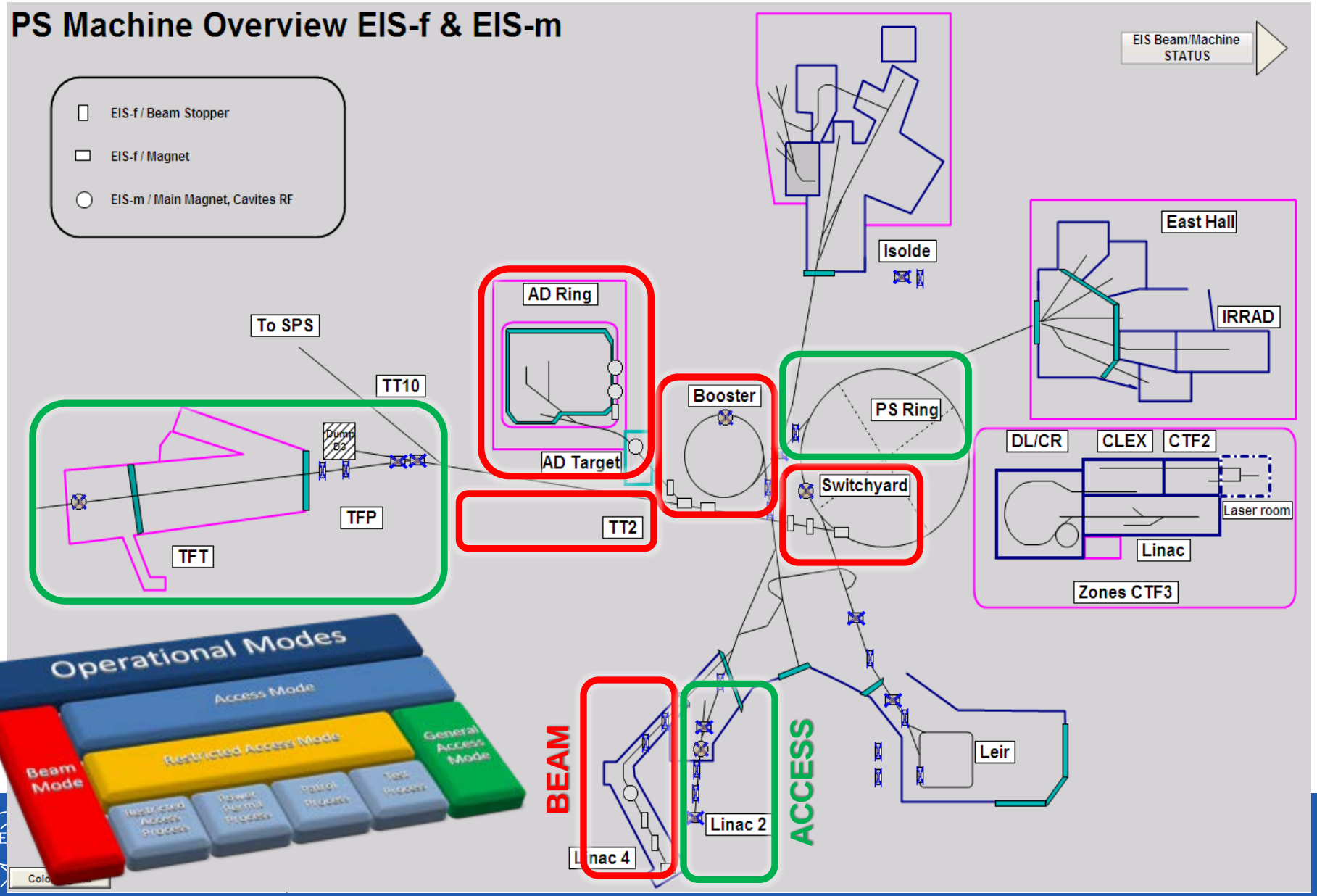
PS-PPS Project Scope



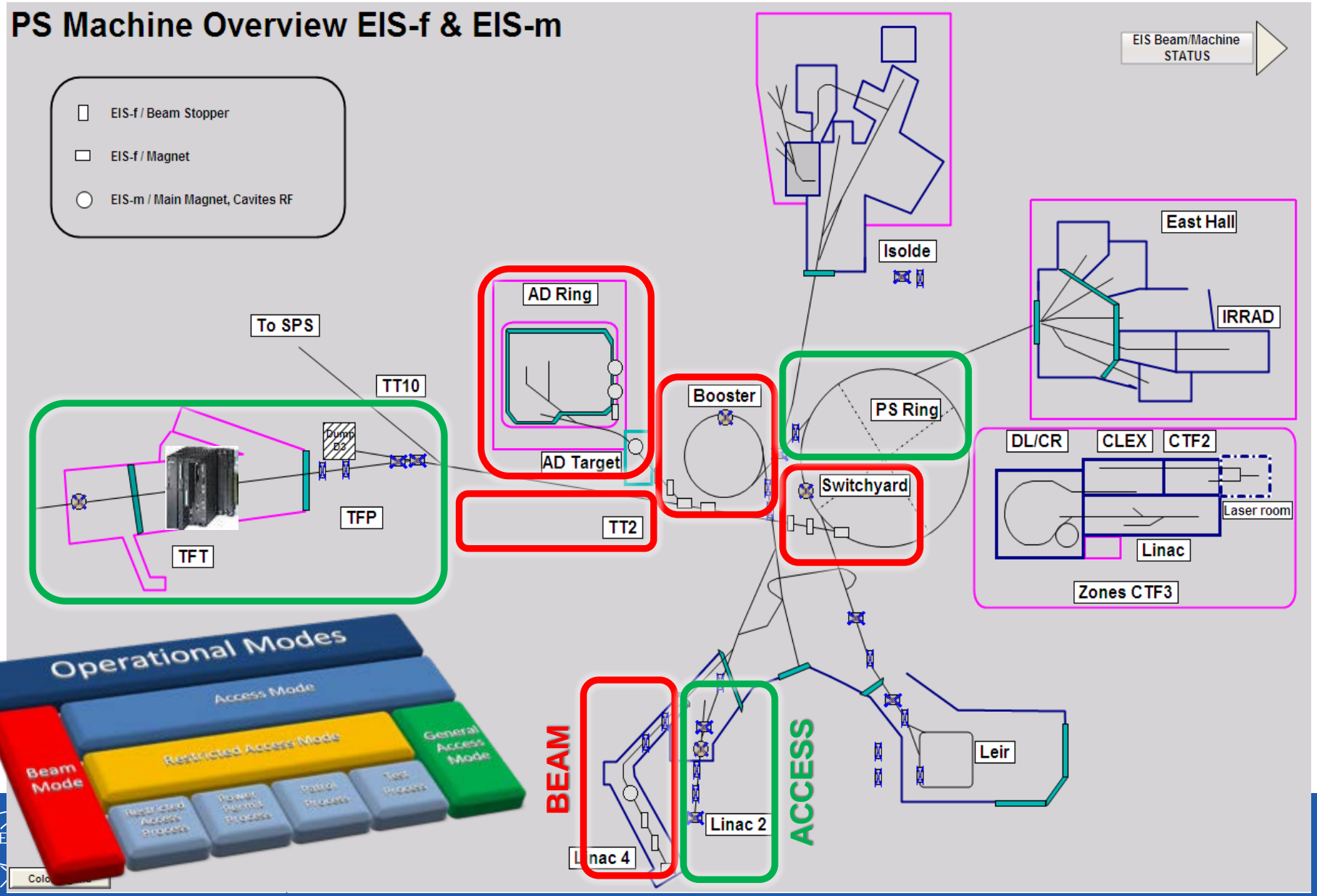
PS-PPS Project Scope



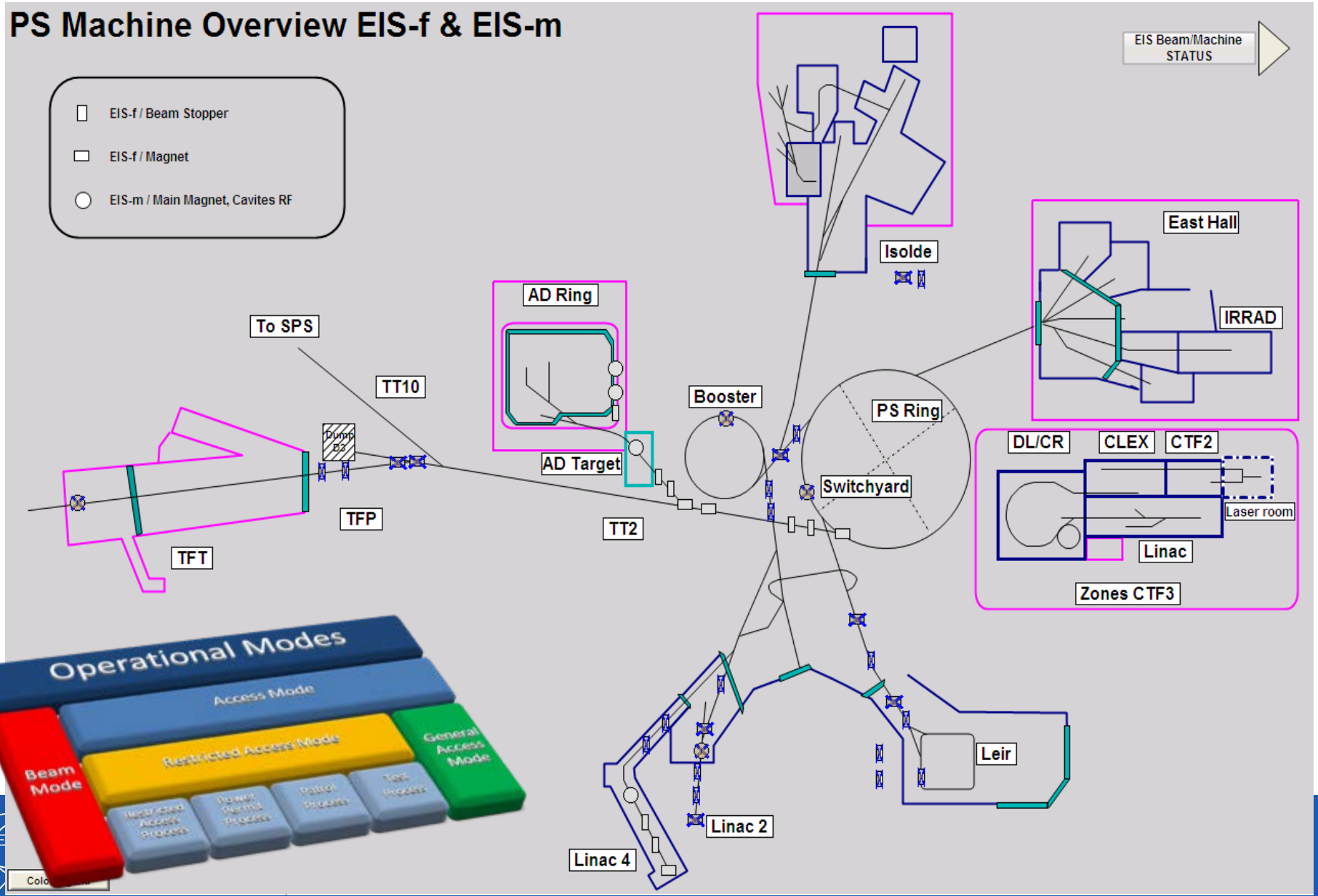
PS-PPS Project Scope



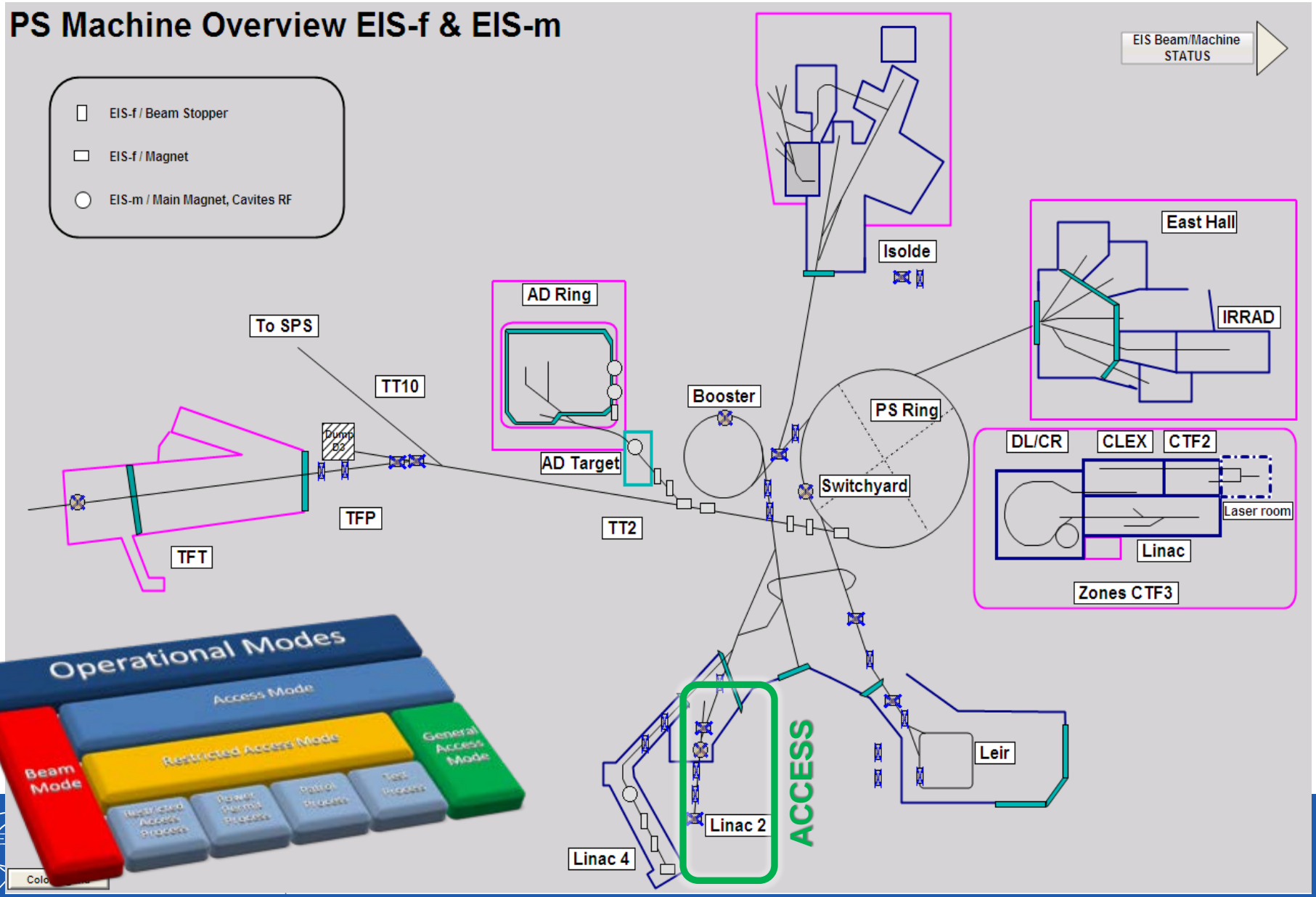
PS-PPS Project Scope



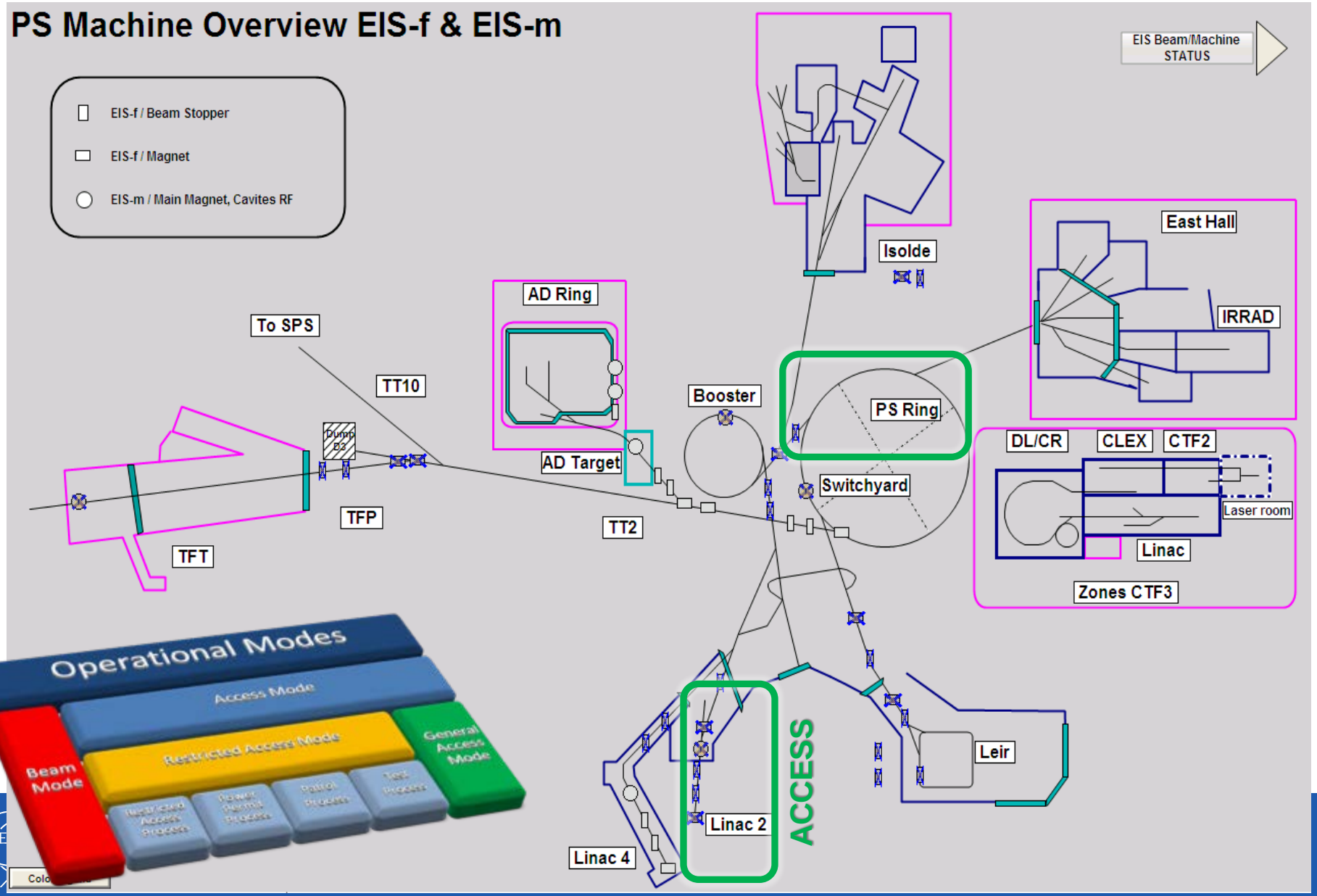
PS-PPS Project Scope



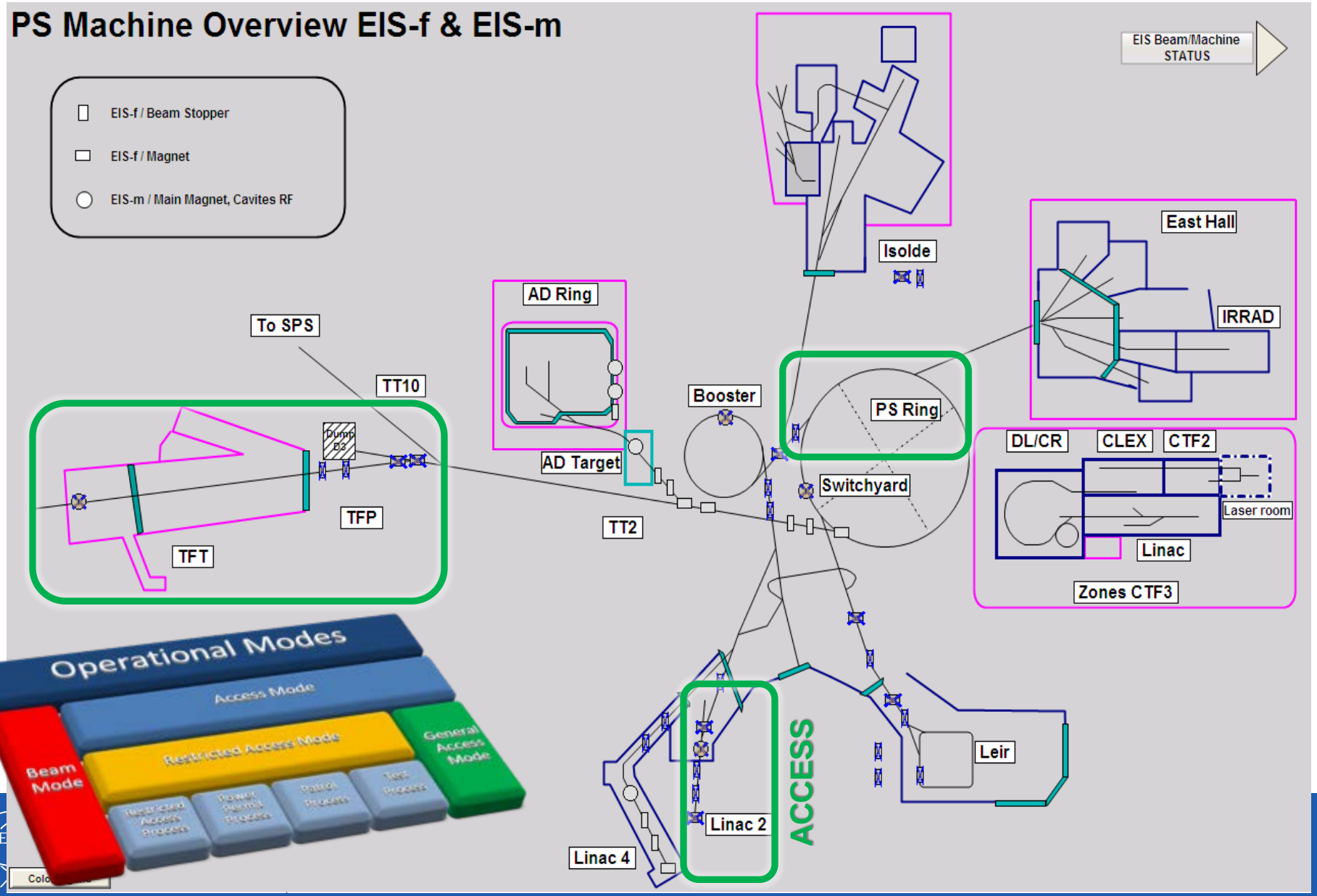
PS-PPS Project Scope



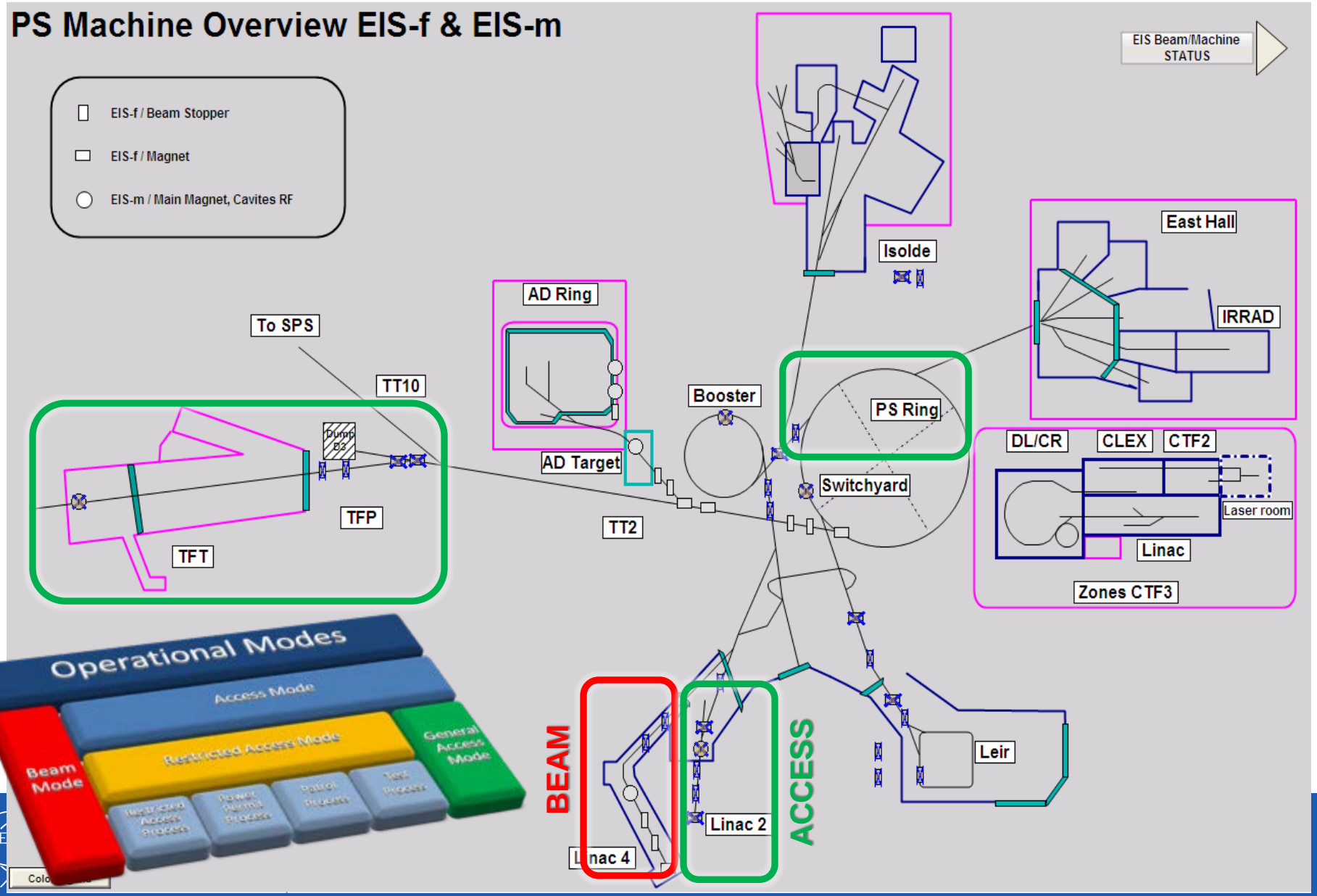
PS-PPS Project Scope



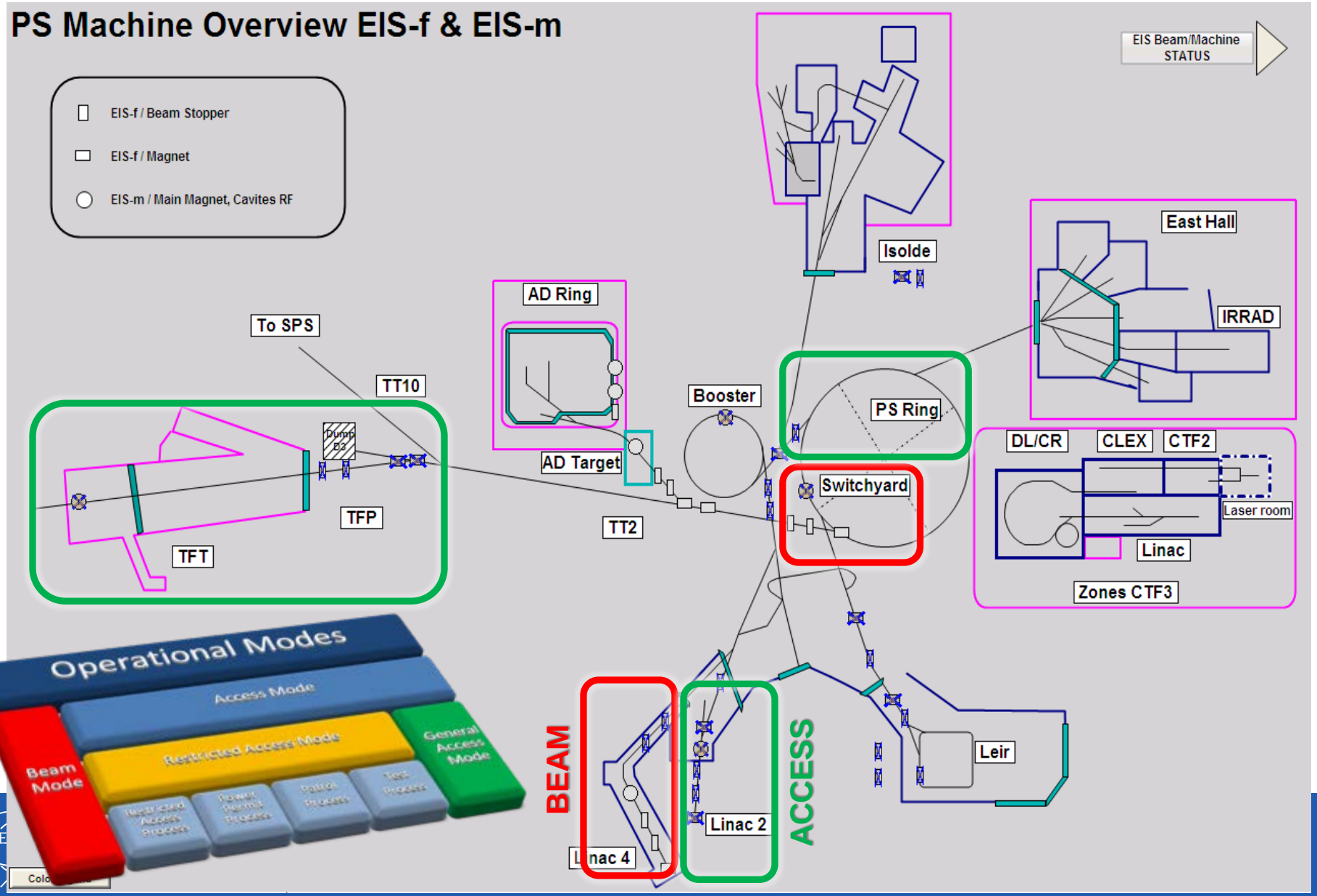
PS-PPS Project Scope



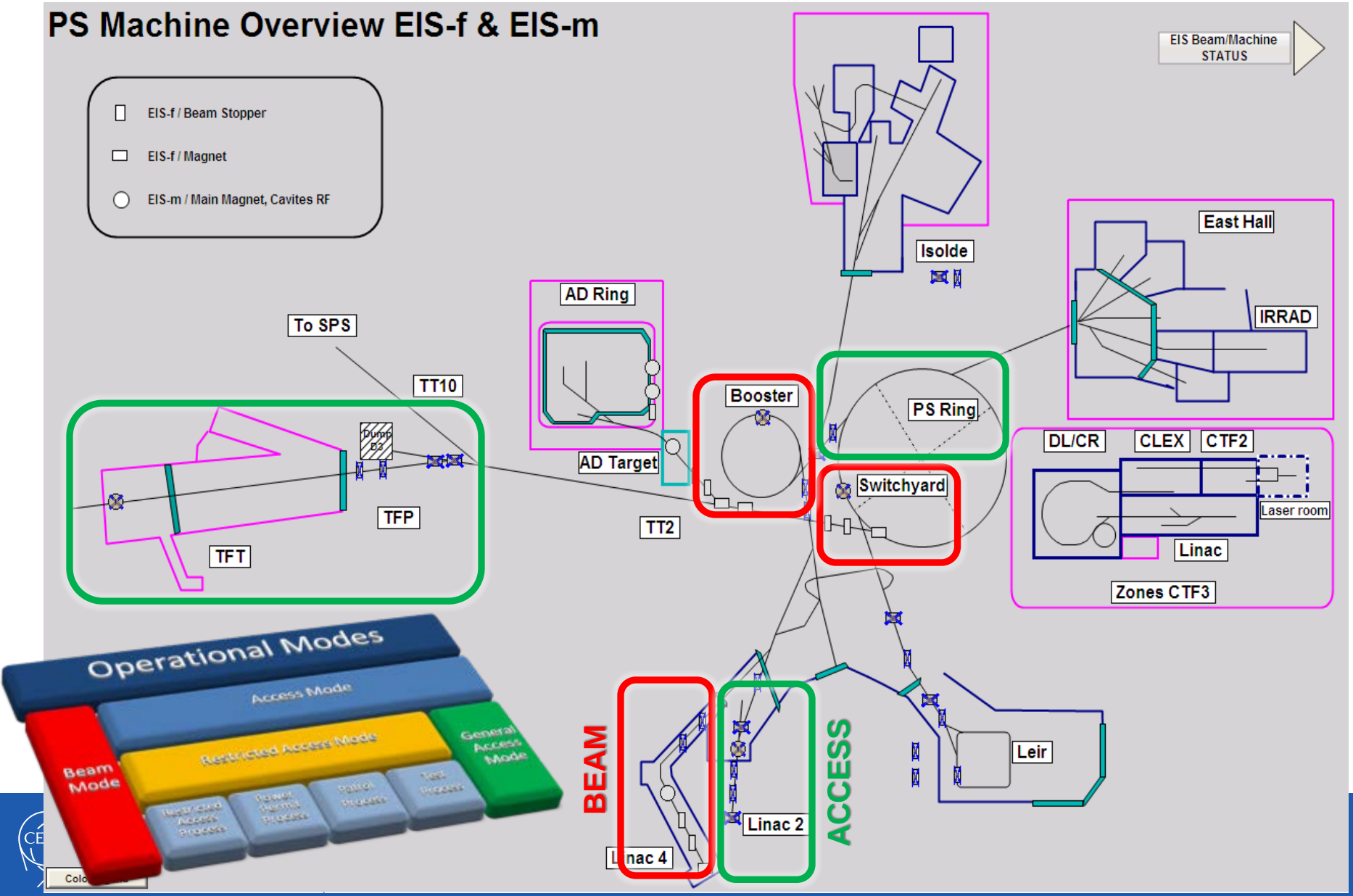
PS-PPS Project Scope



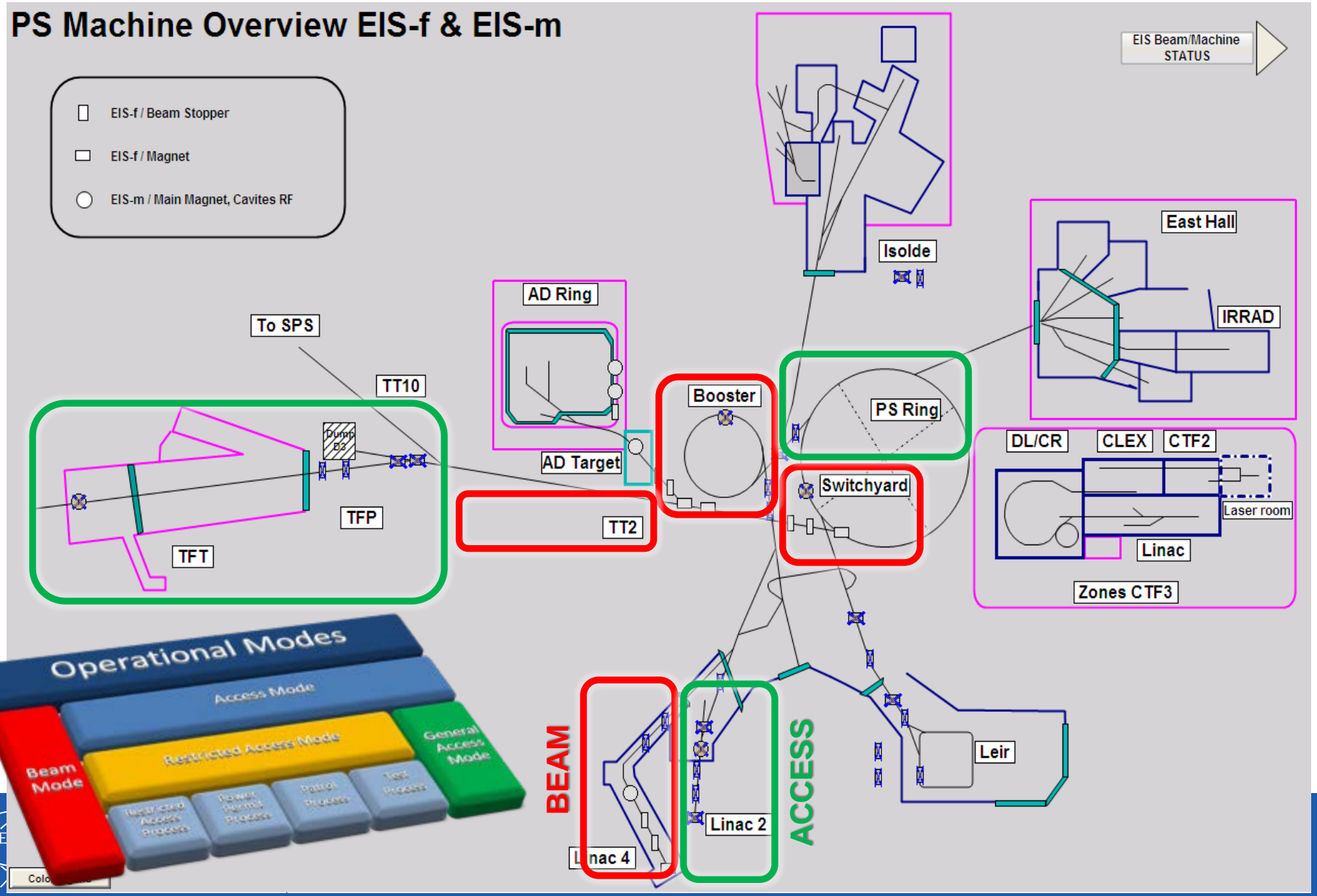
PS-PPS Project Scope



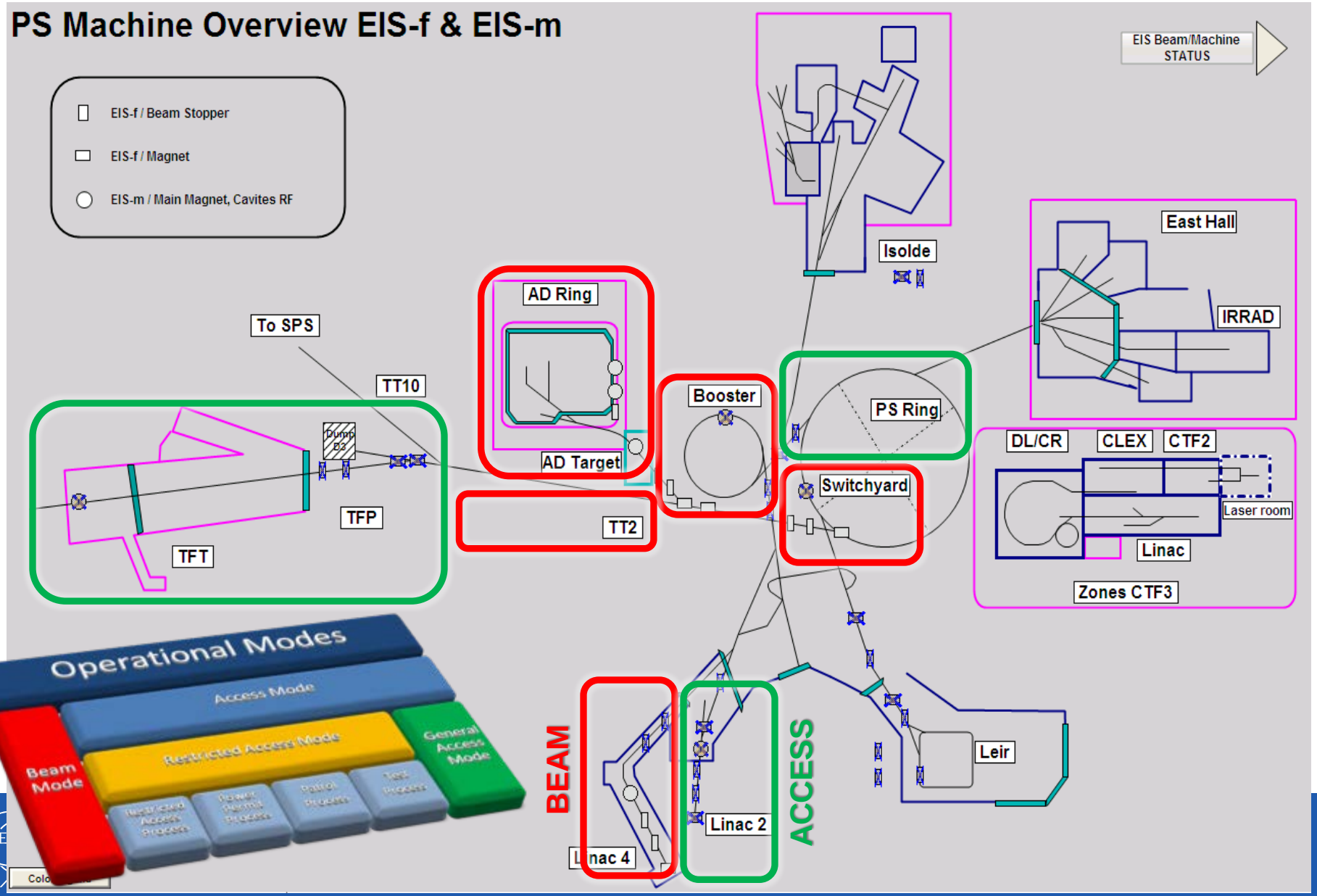
PS-PPS Project Scope



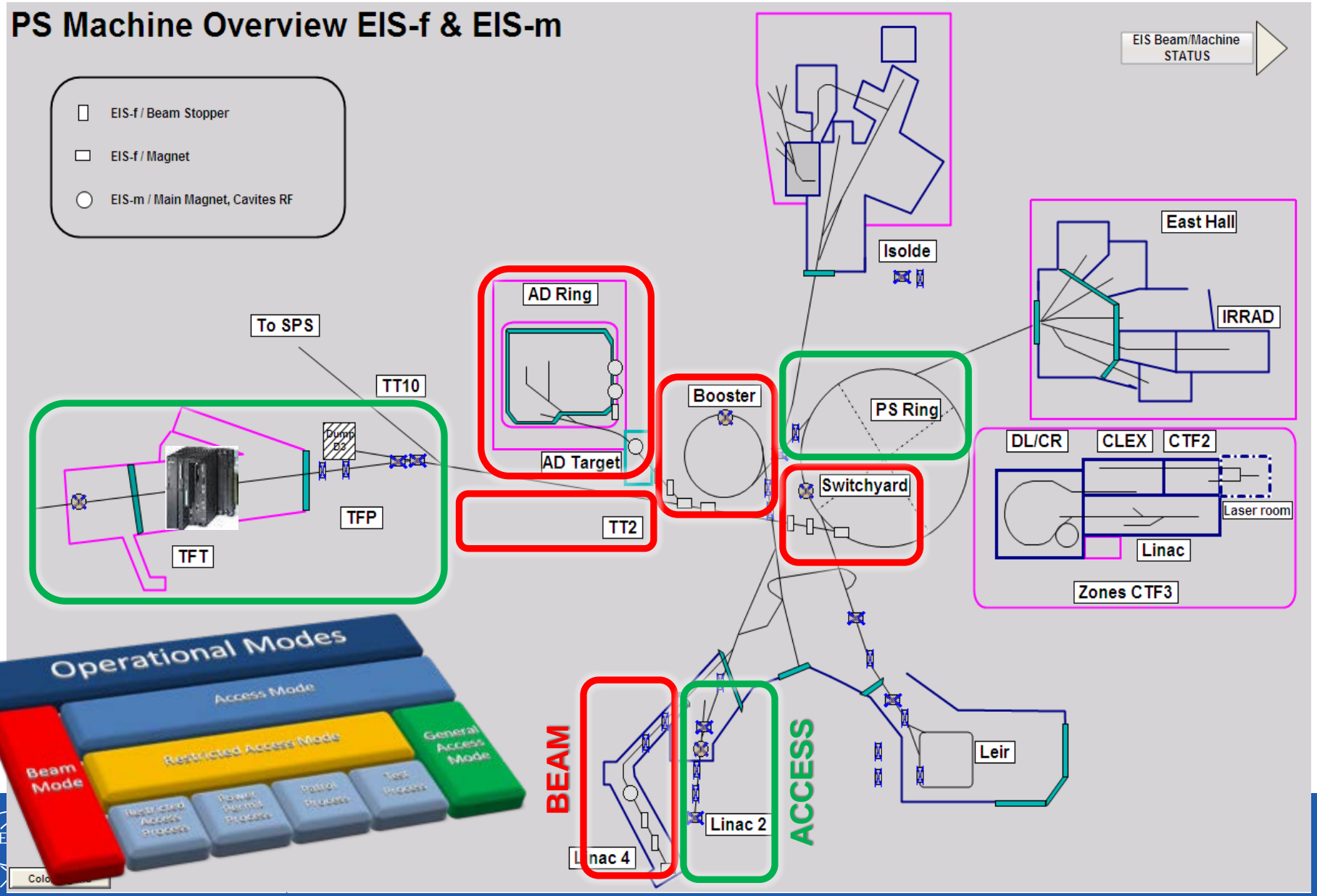
PS-PPS Project Scope



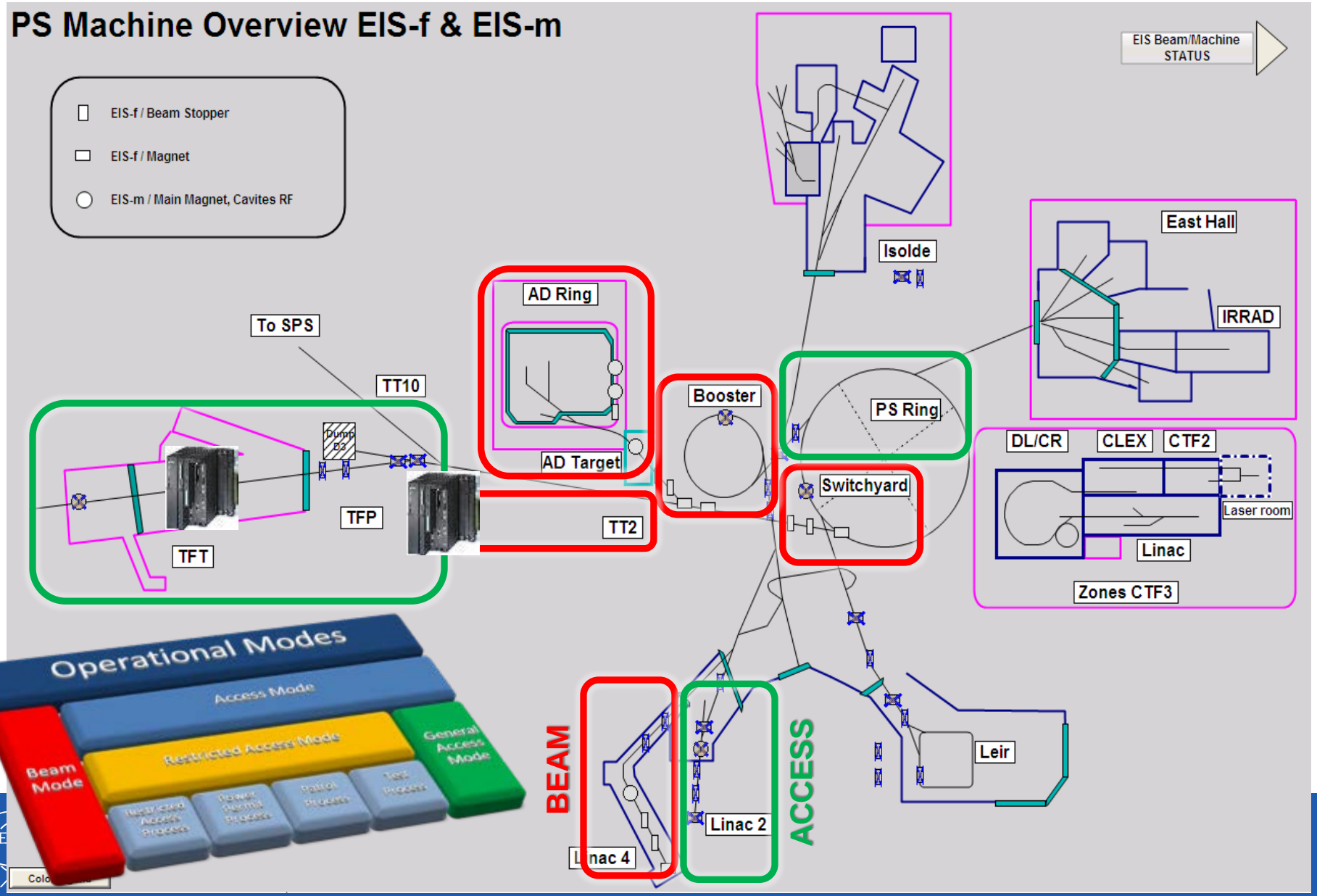
PS-PPS Project Scope



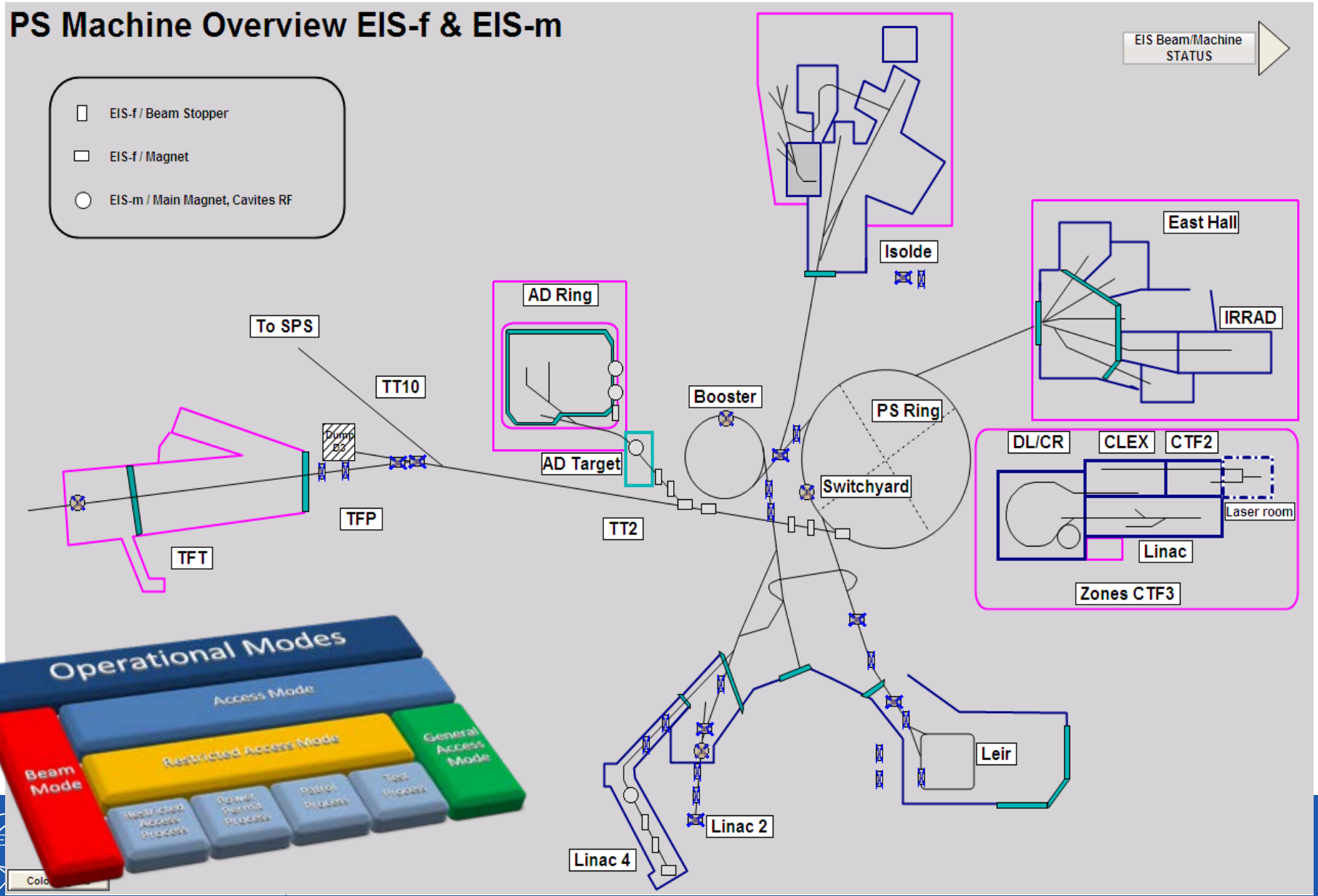
PS-PPS Project Scope



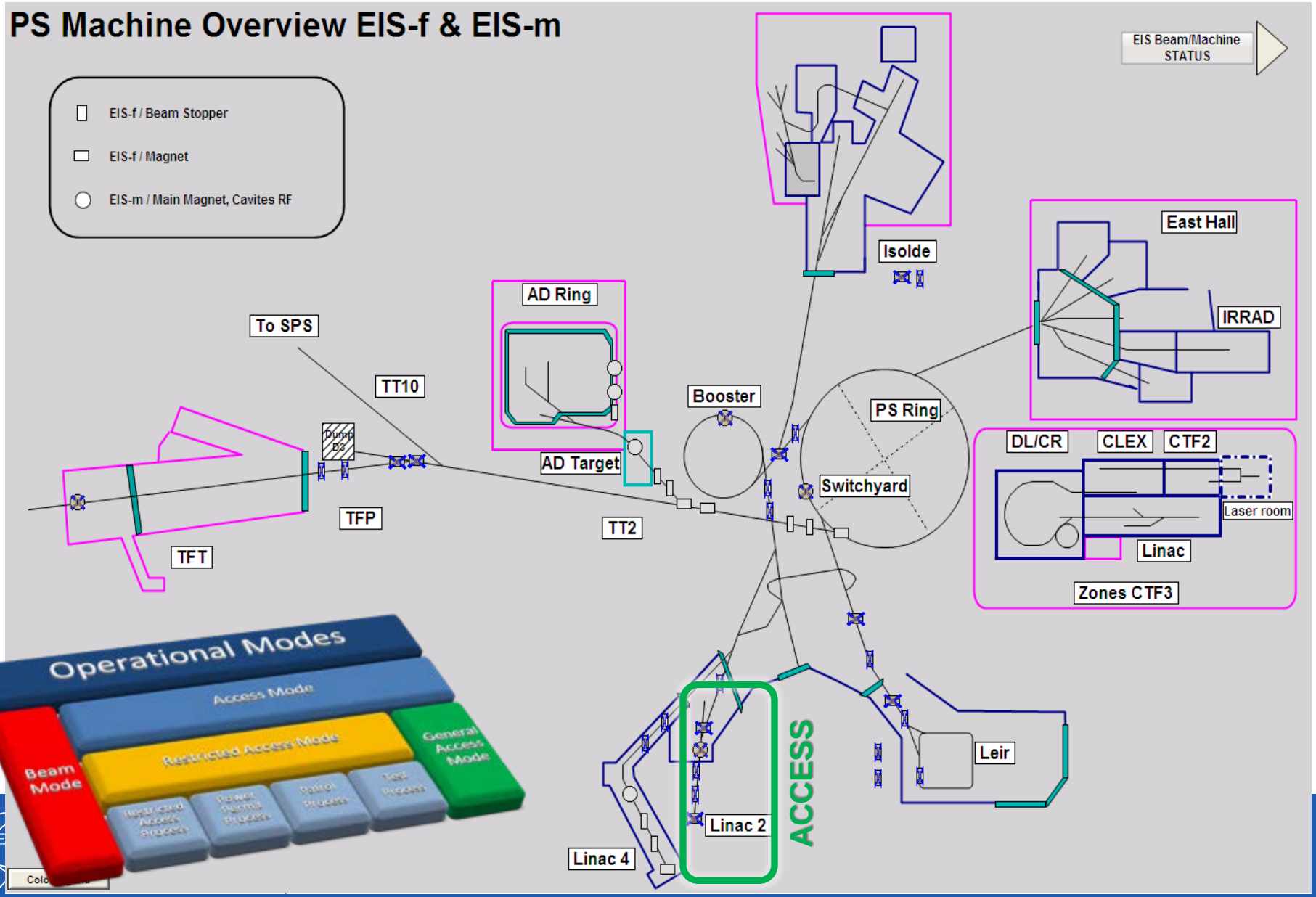
PS-PPS Project Scope



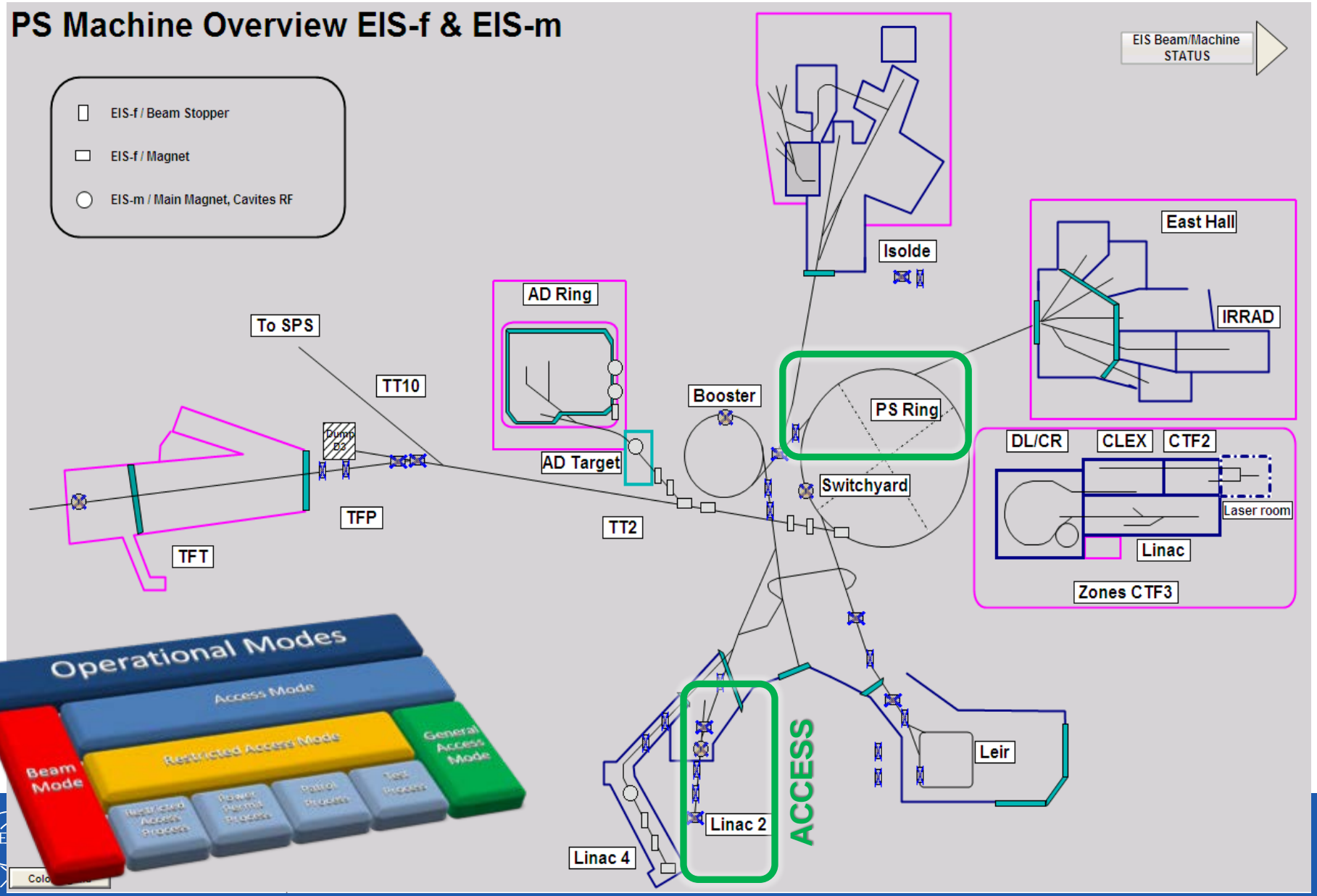
PS-PPS Project Scope



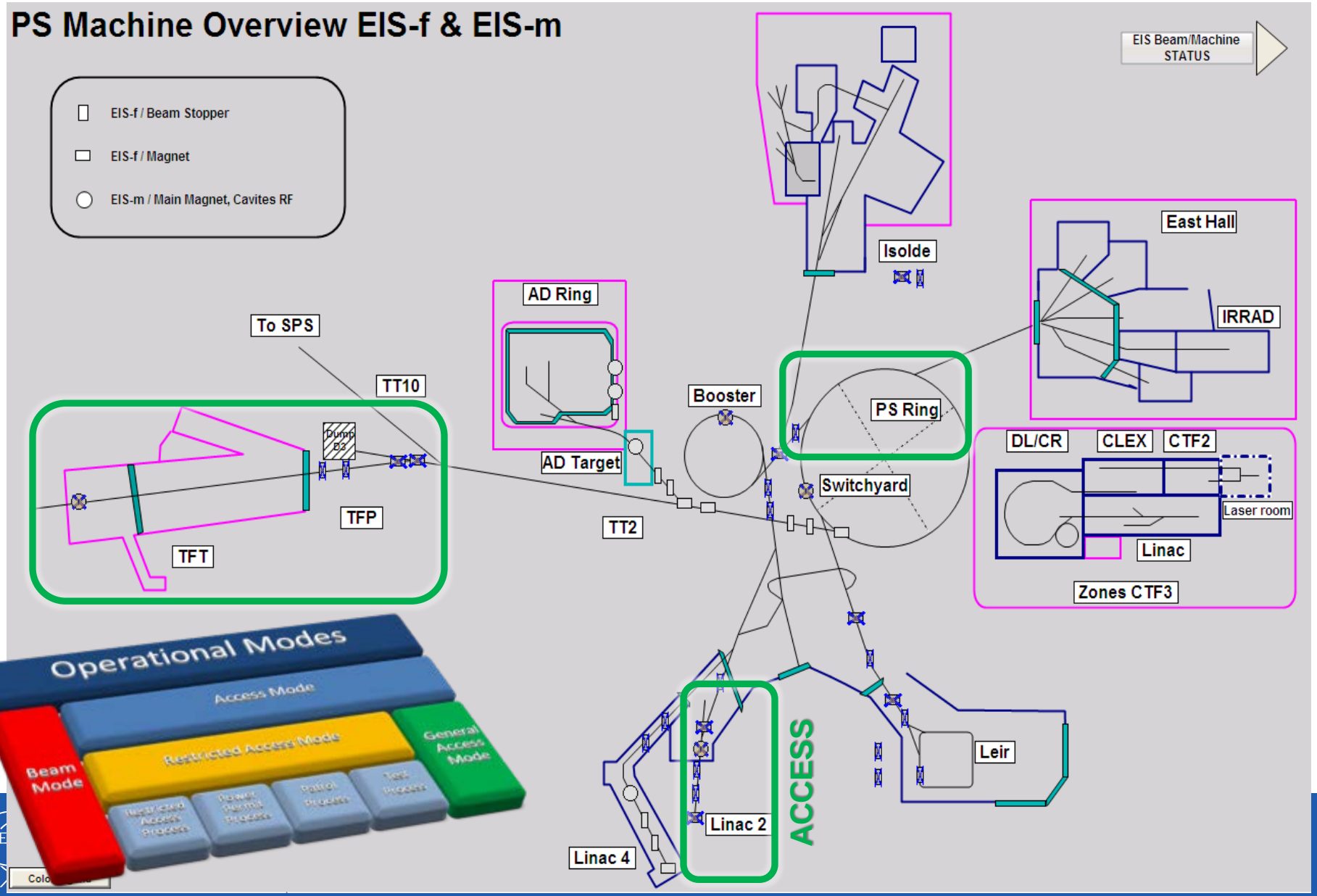
PS-PPS Project Scope



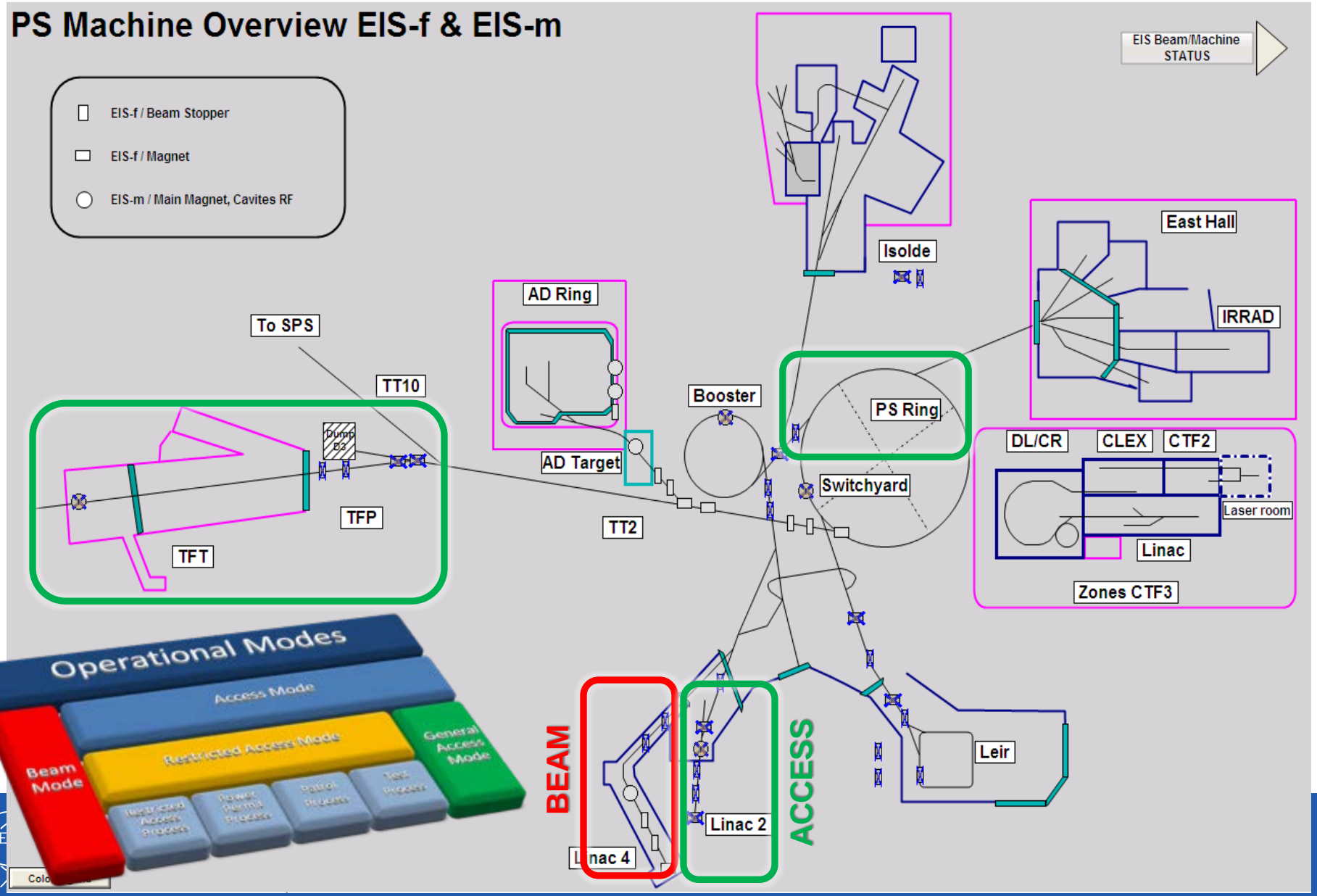
PS-PPS Project Scope



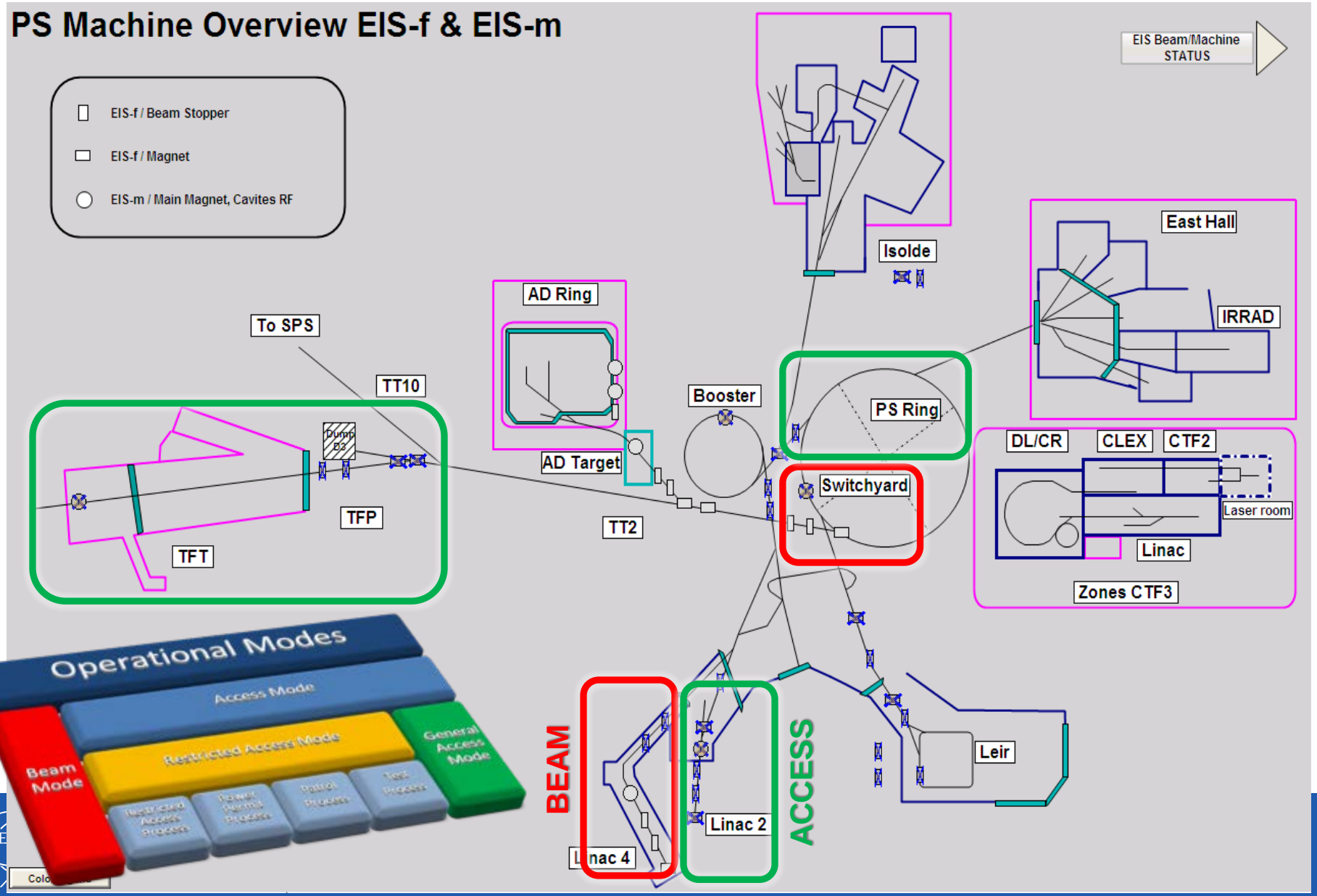
PS-PPS Project Scope



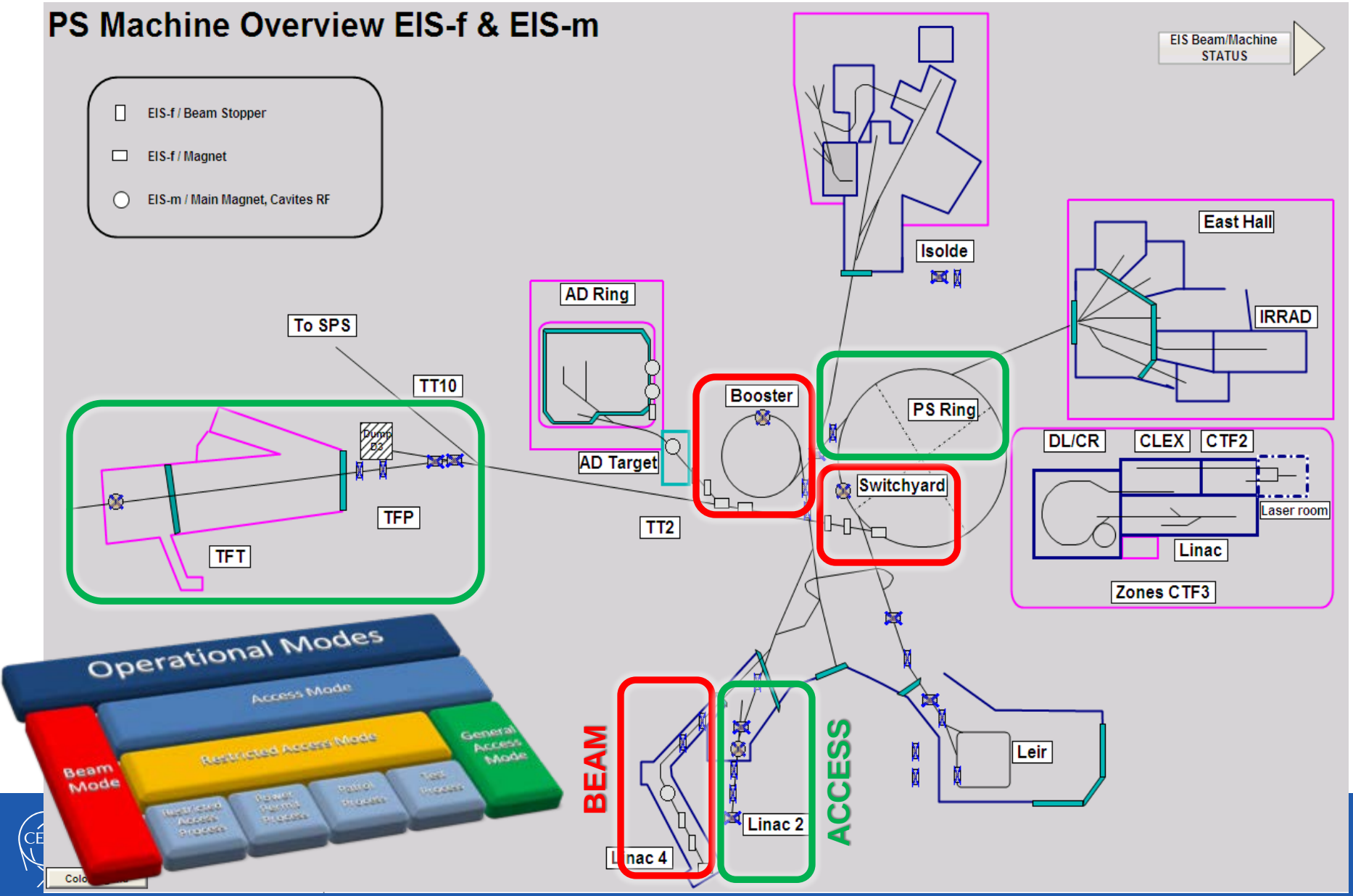
PS-PPS Project Scope



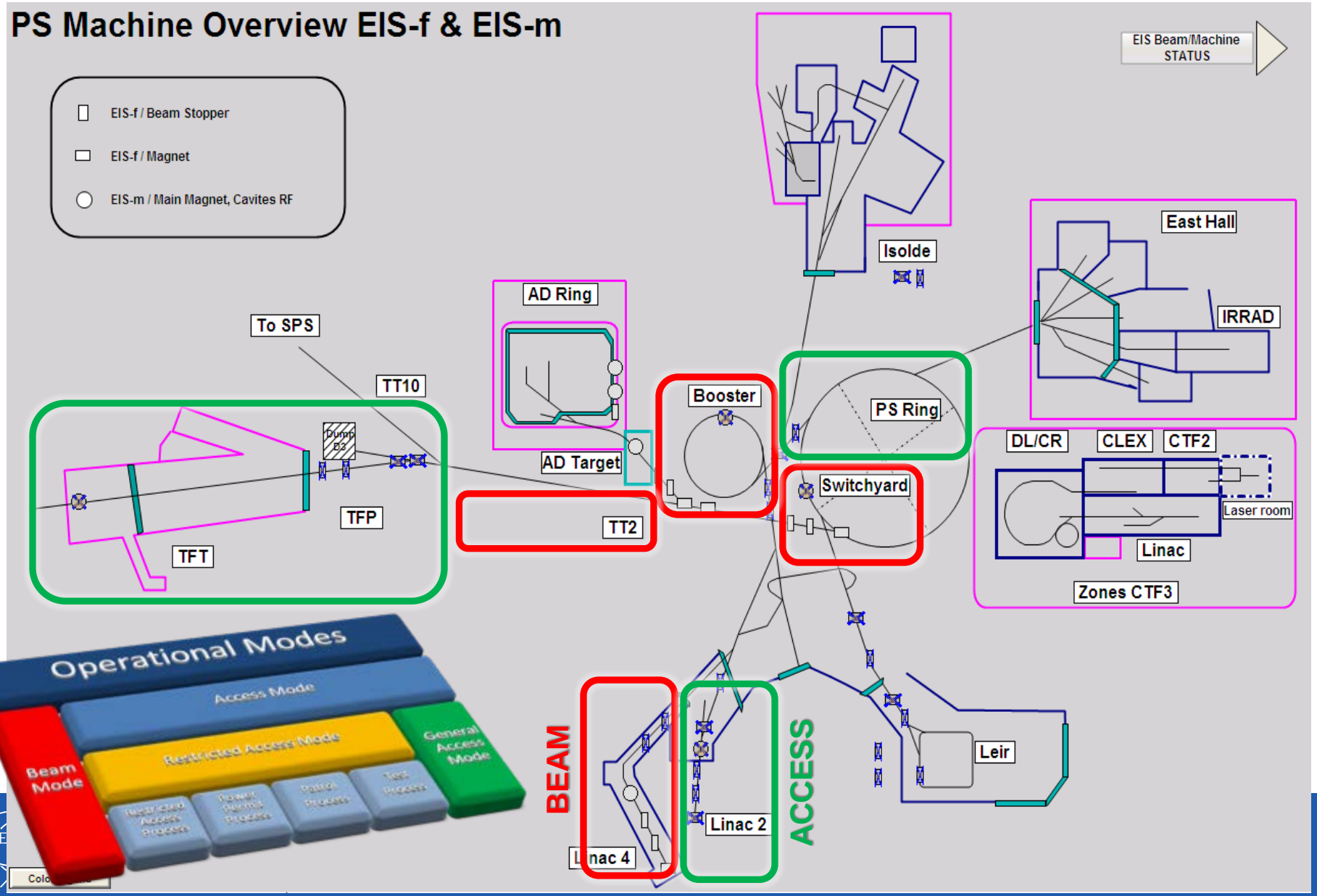
PS-PPS Project Scope



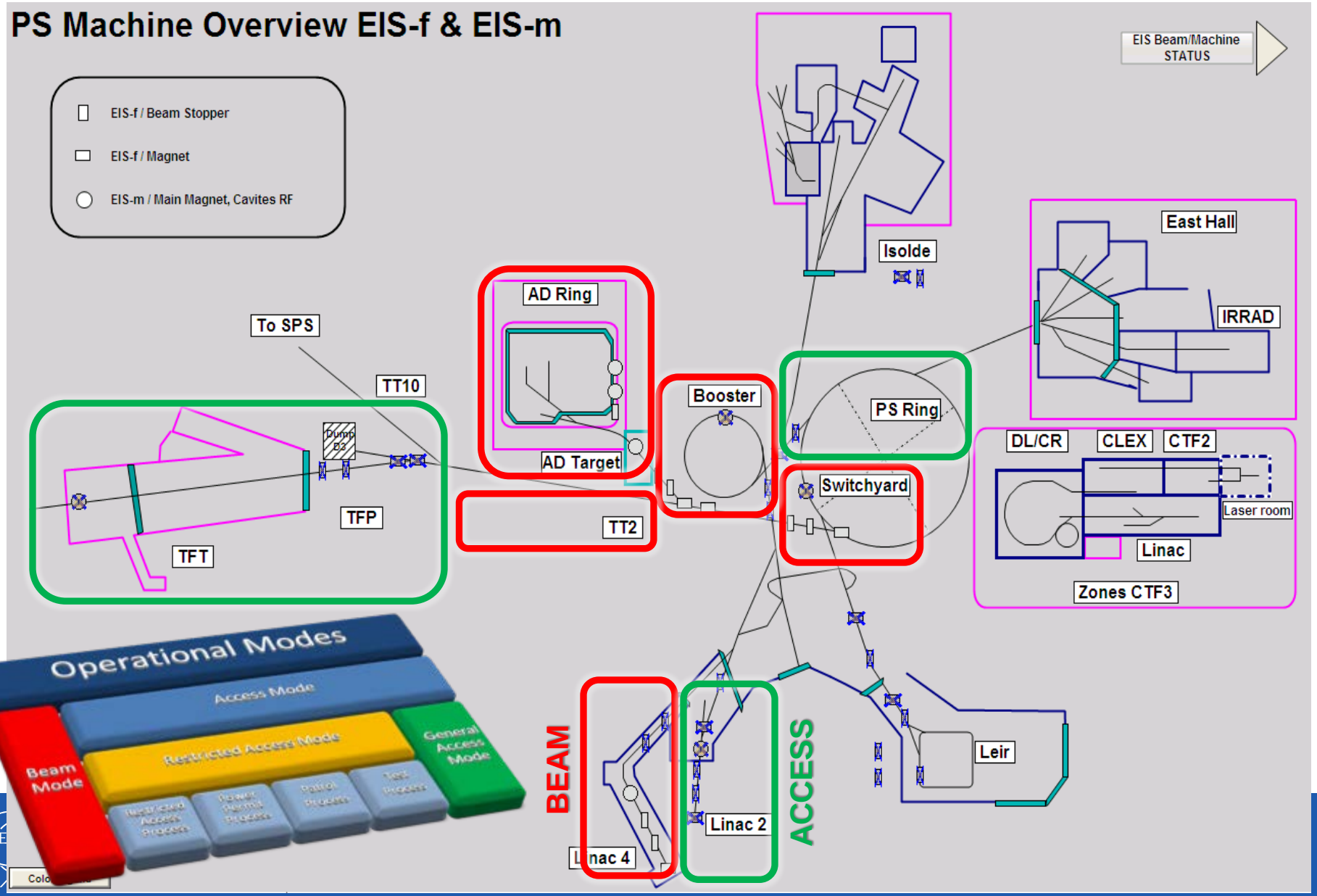
PS-PPS Project Scope



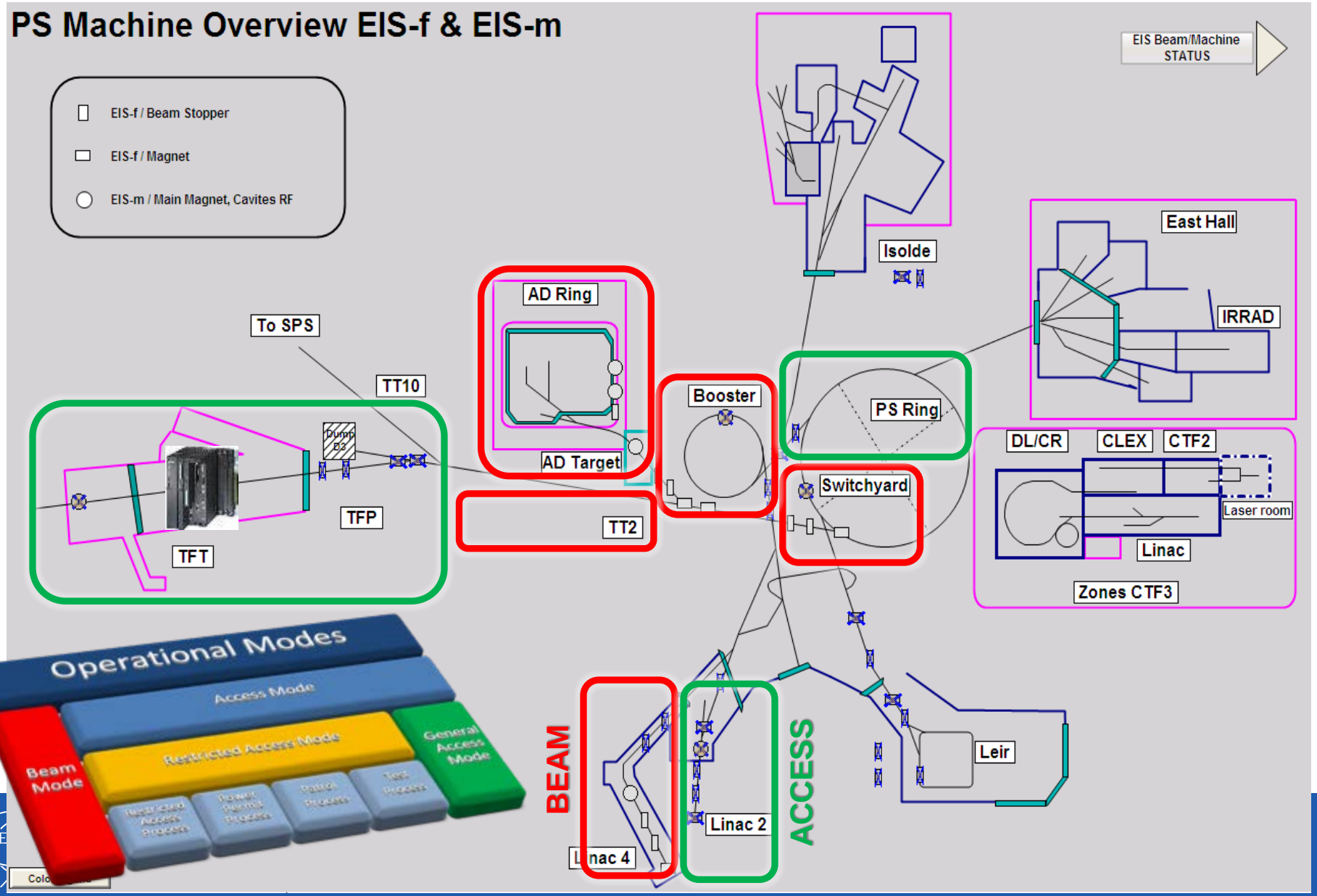
PS-PPS Project Scope



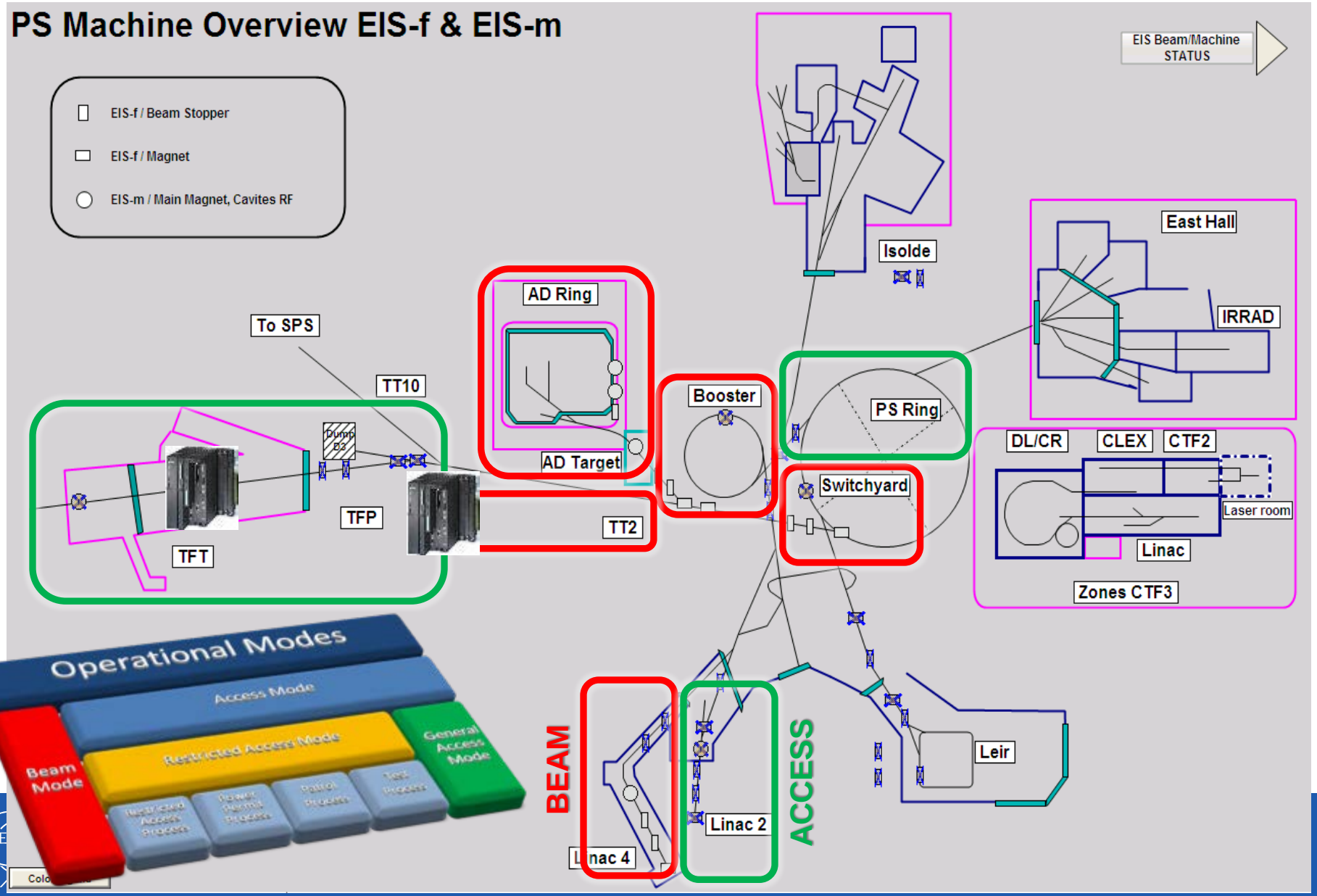
PS-PPS Project Scope



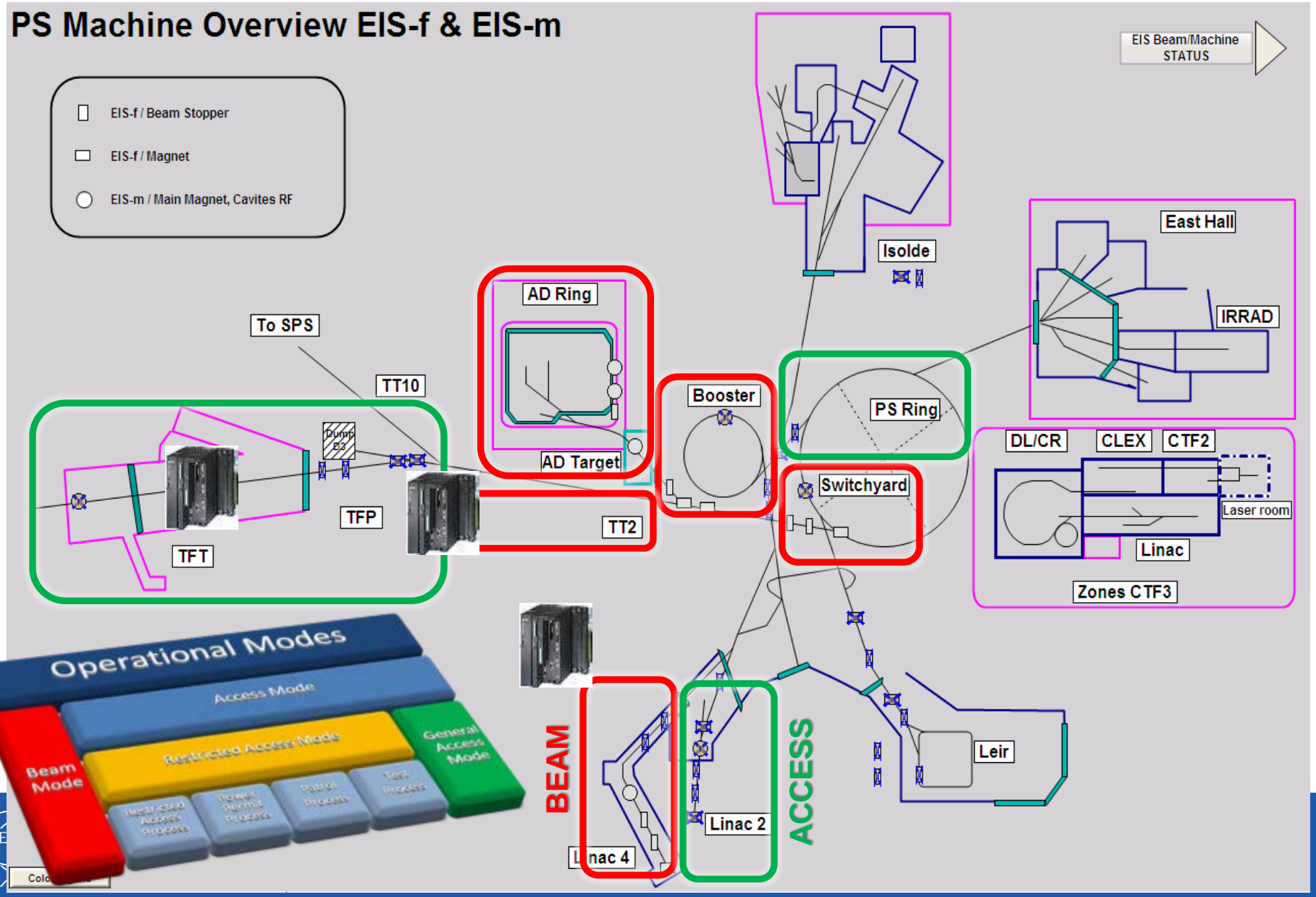
PS-PPS Project Scope



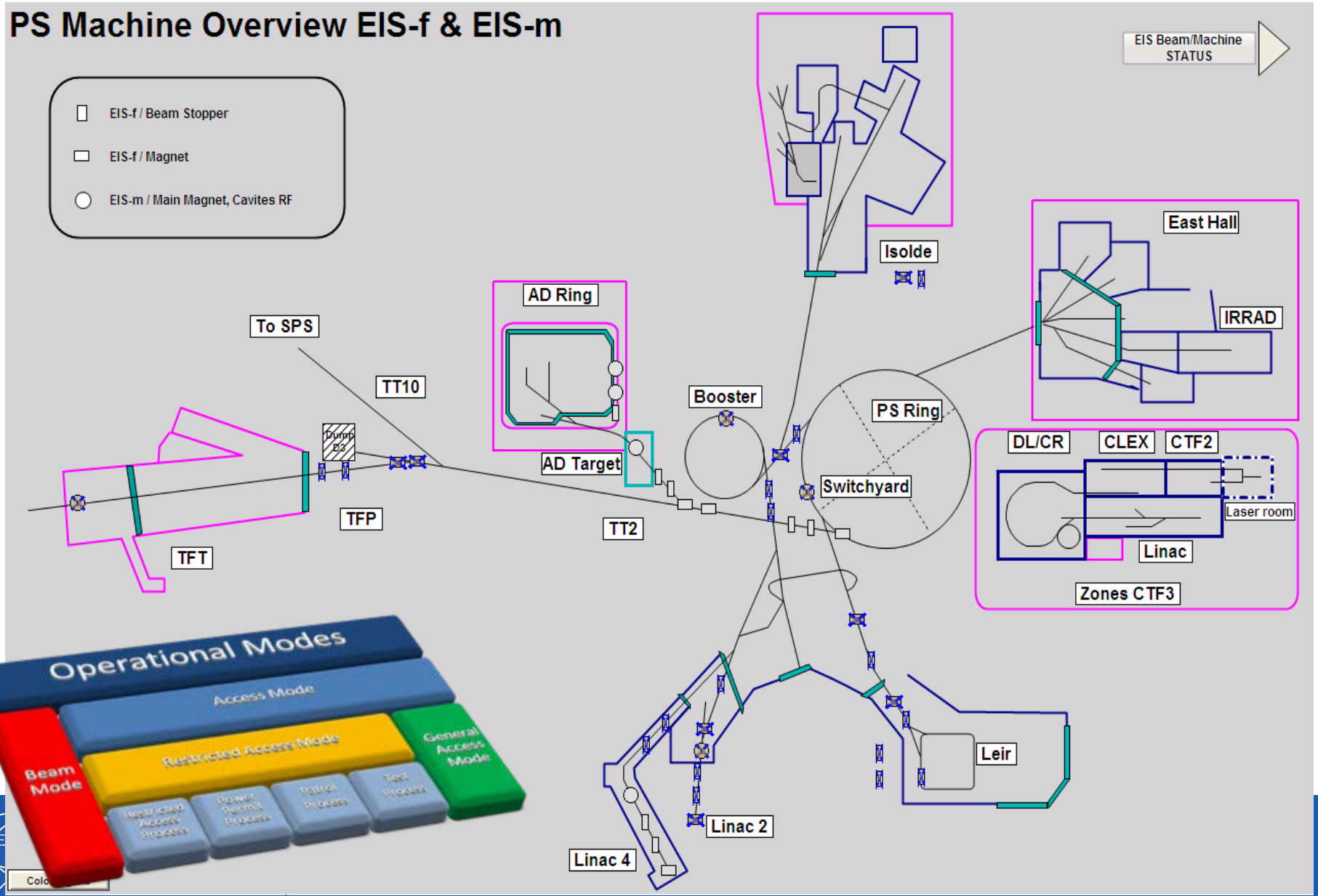
PS-PPS Project Scope



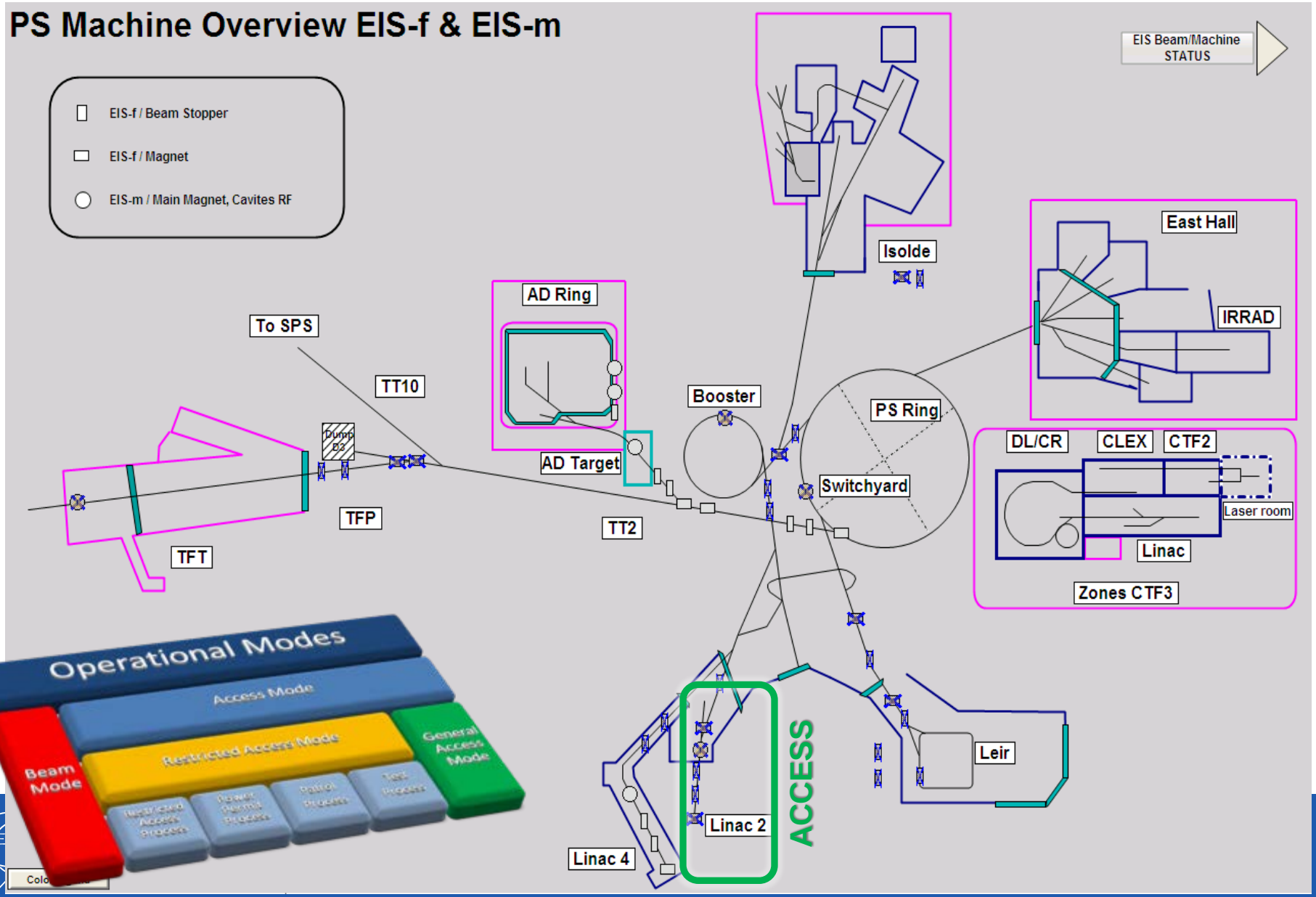
PS-PPS Project Scope



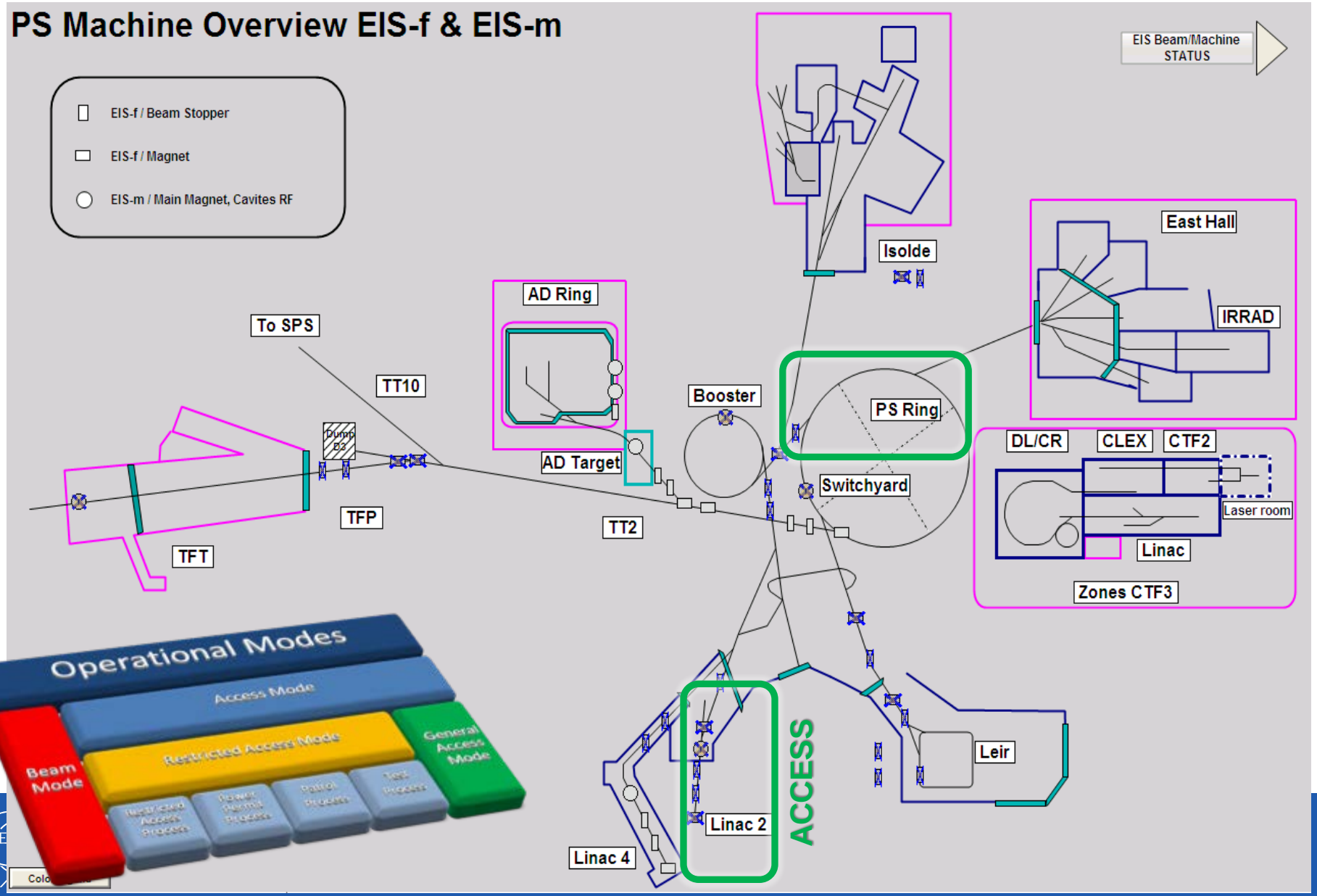
PS-PPS Project Scope



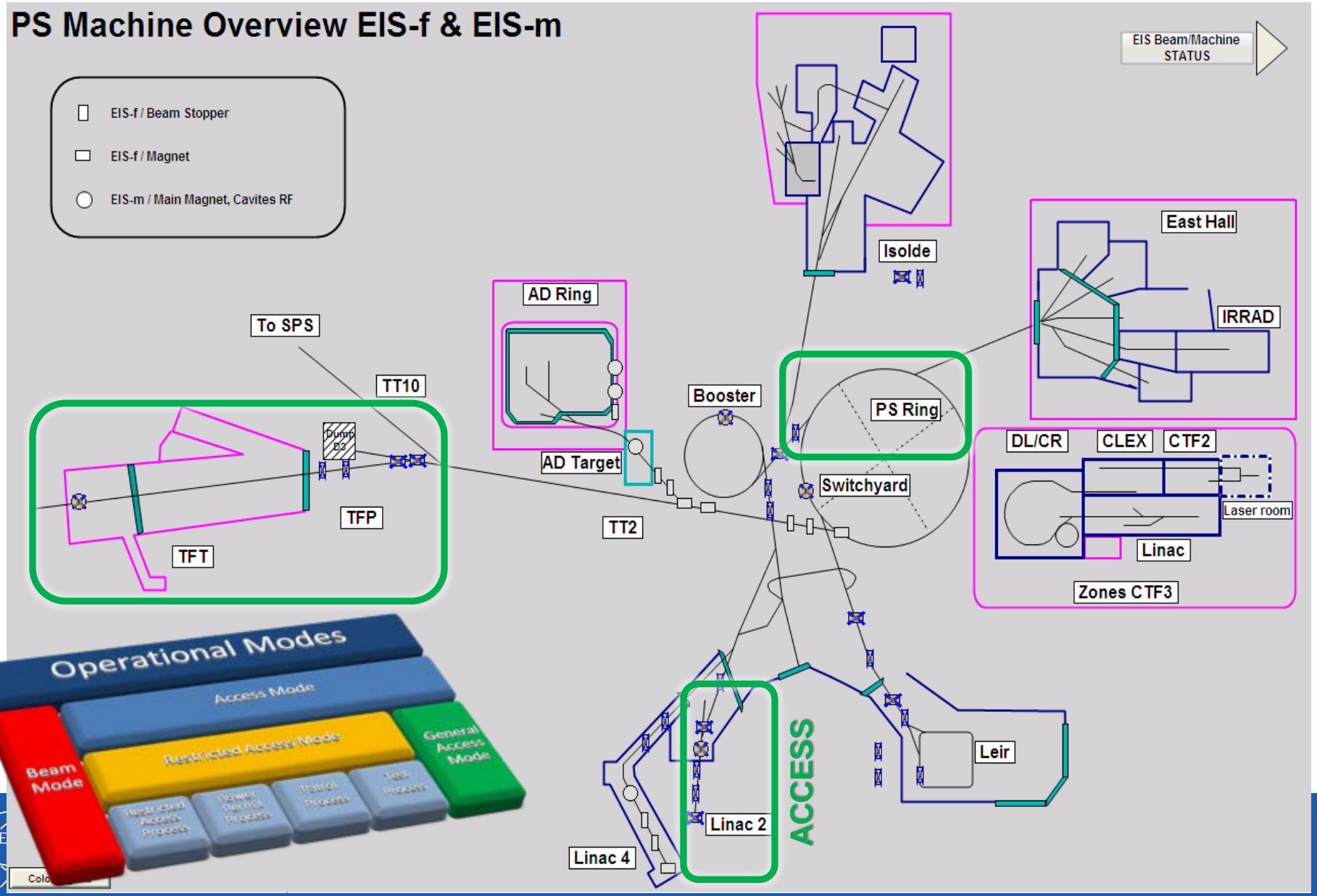
PS-PPS Project Scope



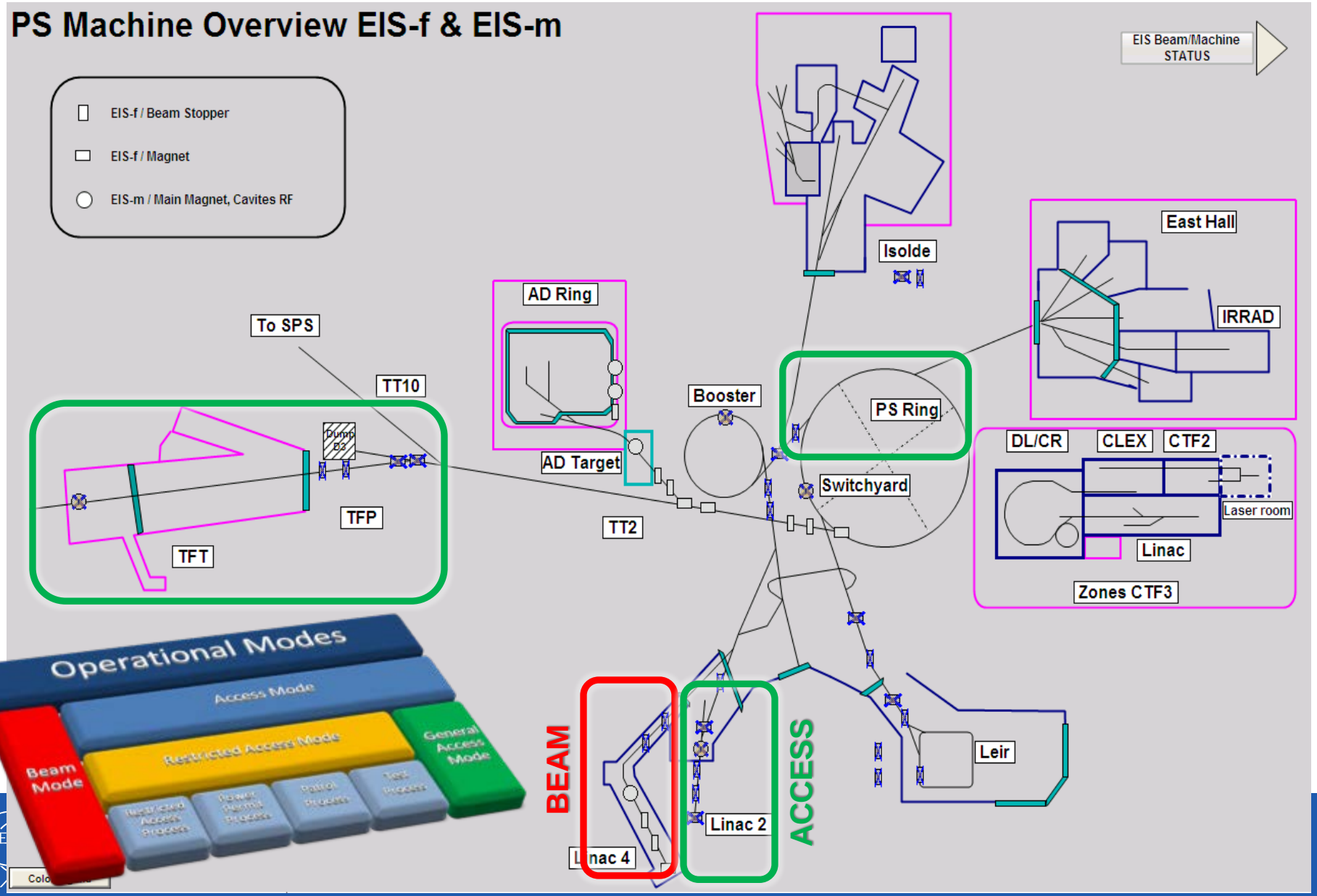
PS-PPS Project Scope



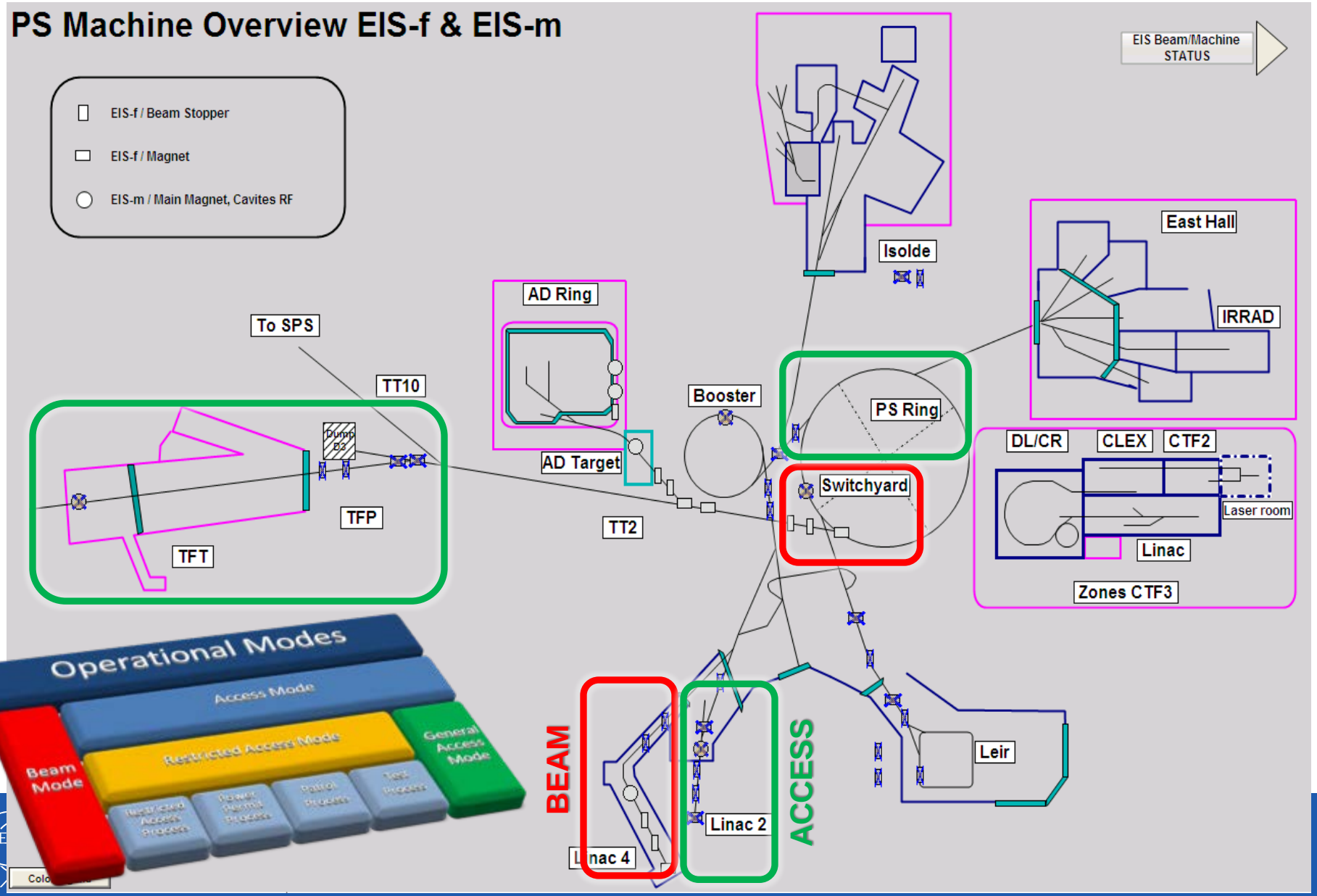
PS-PPS Project Scope



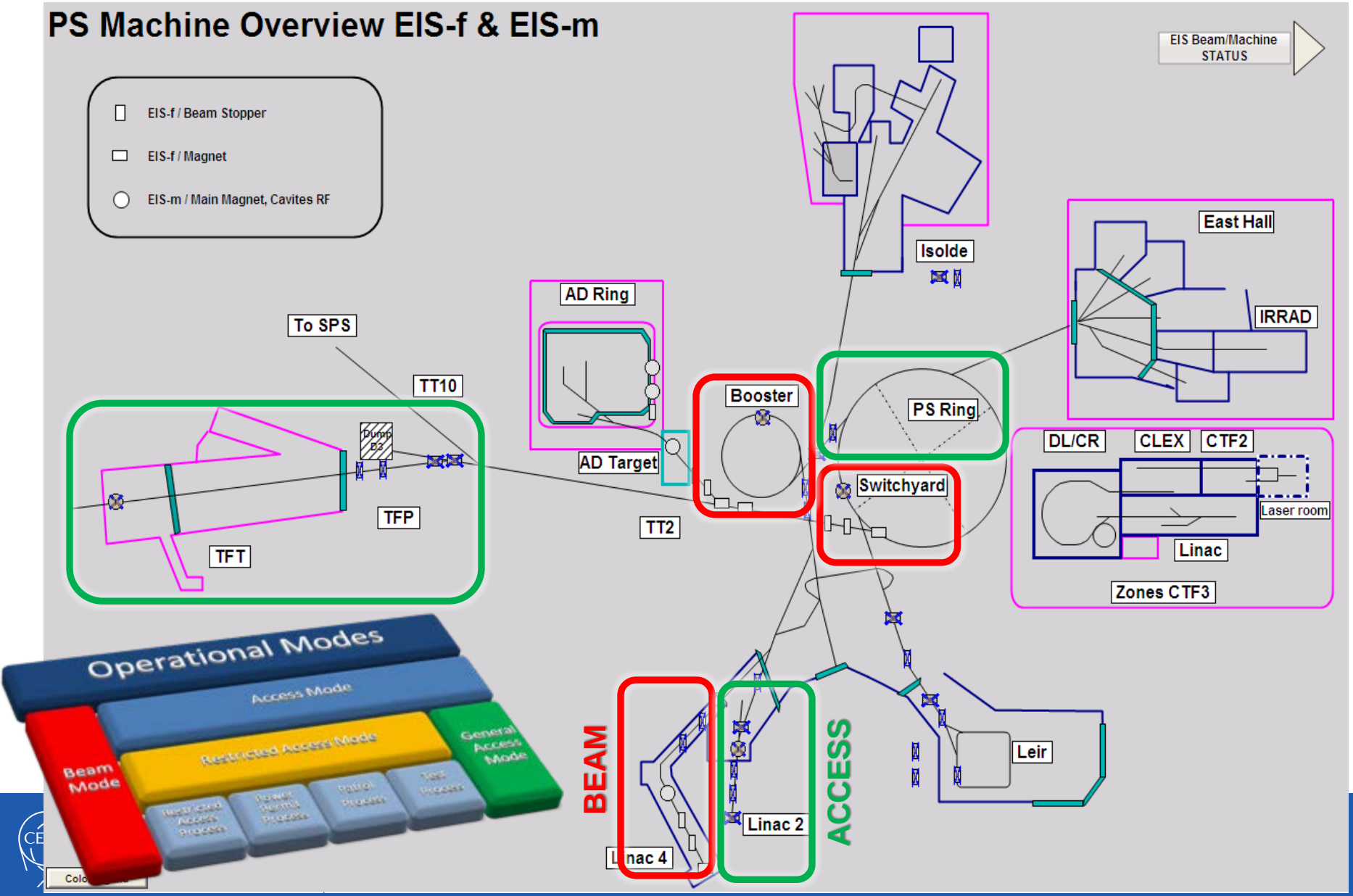
PS-PPS Project Scope



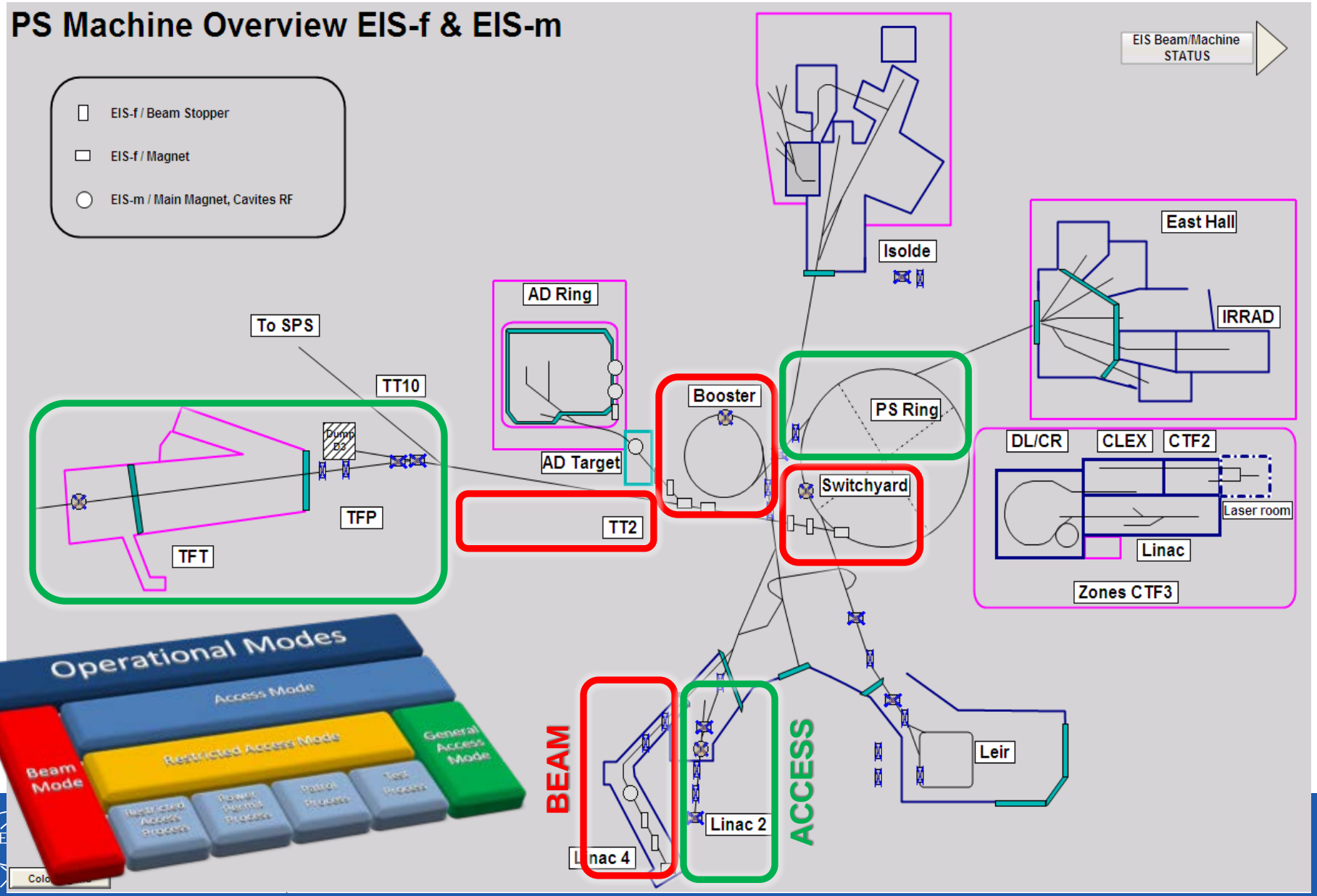
PS-PPS Project Scope



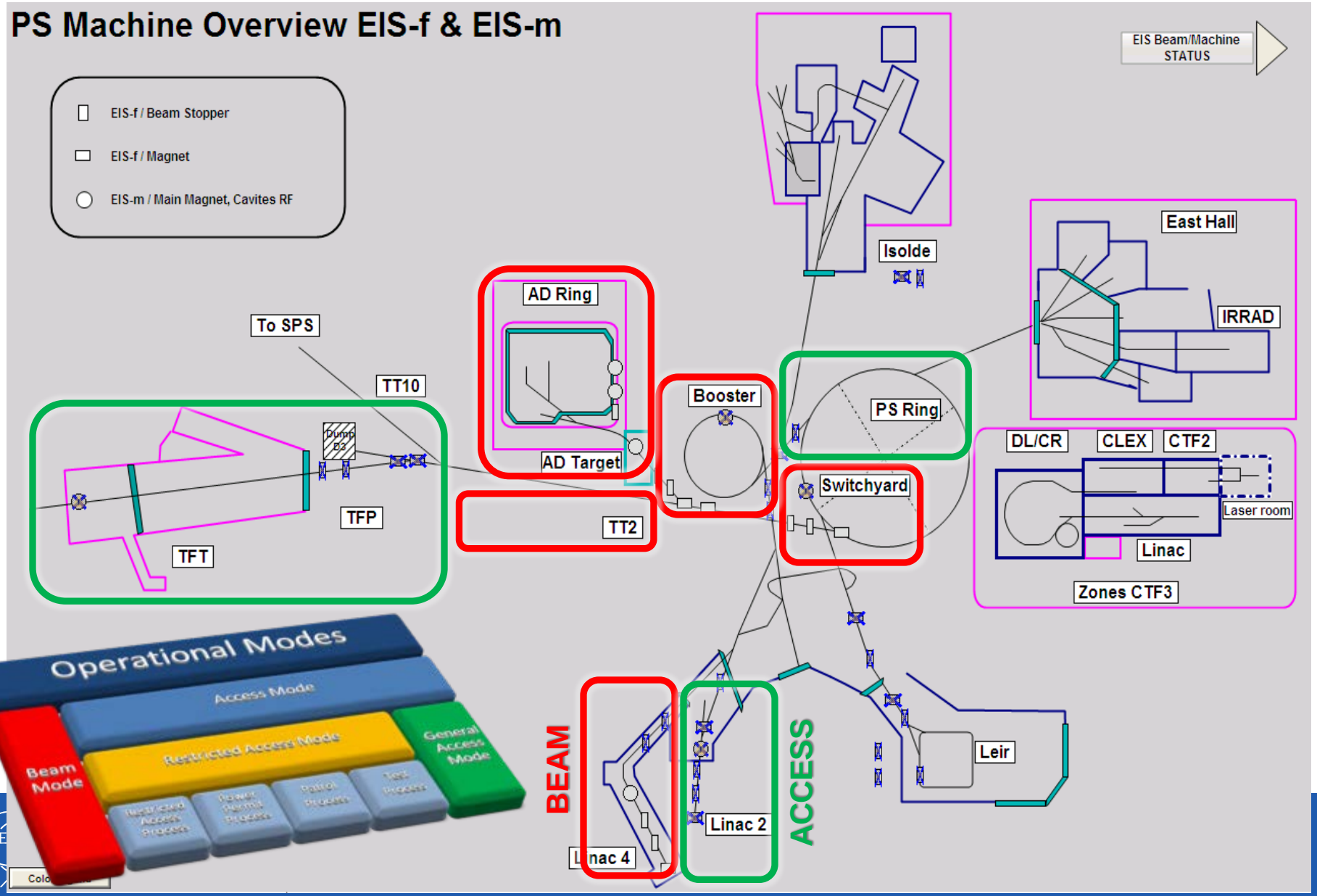
PS-PPS Project Scope



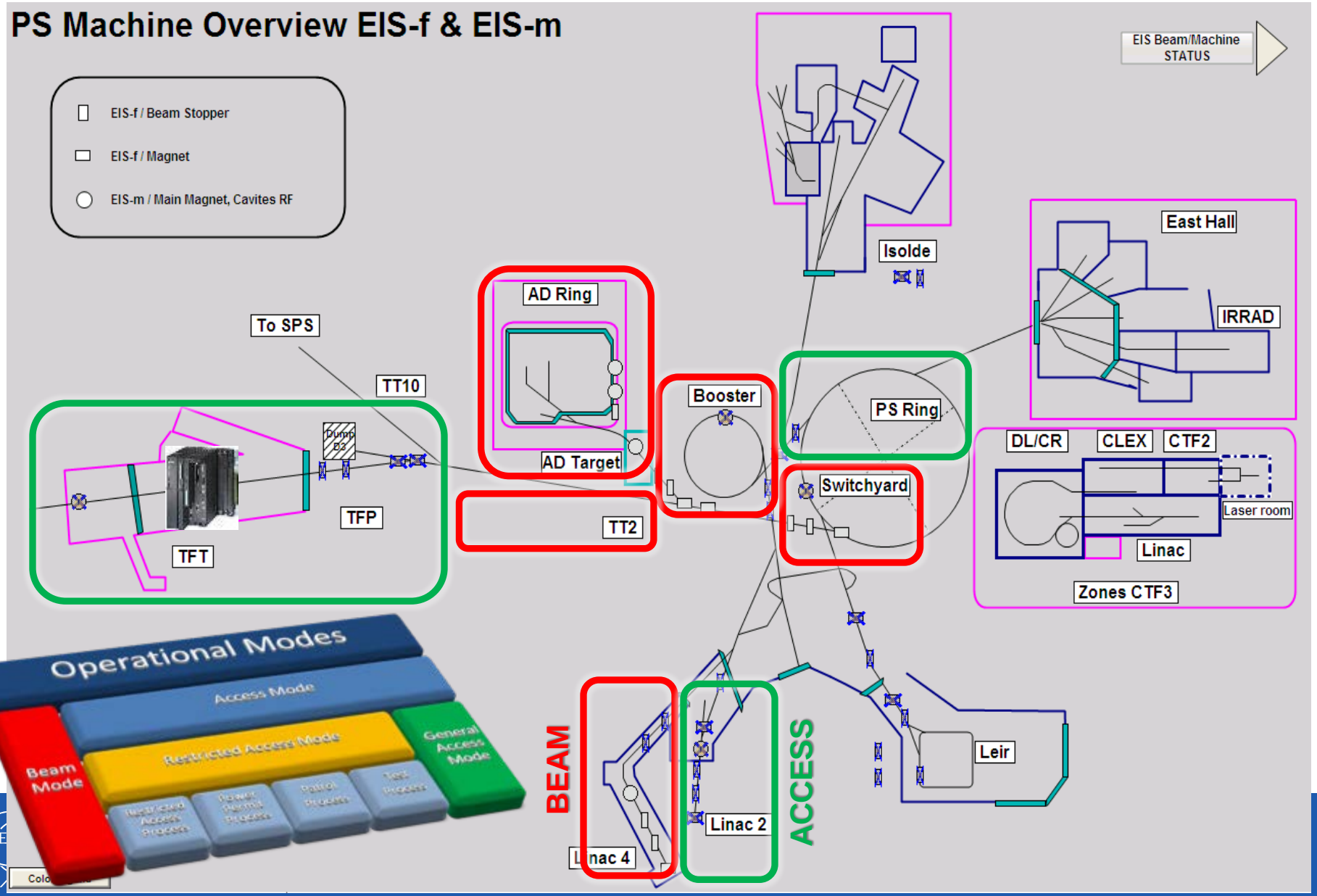
PS-PPS Project Scope



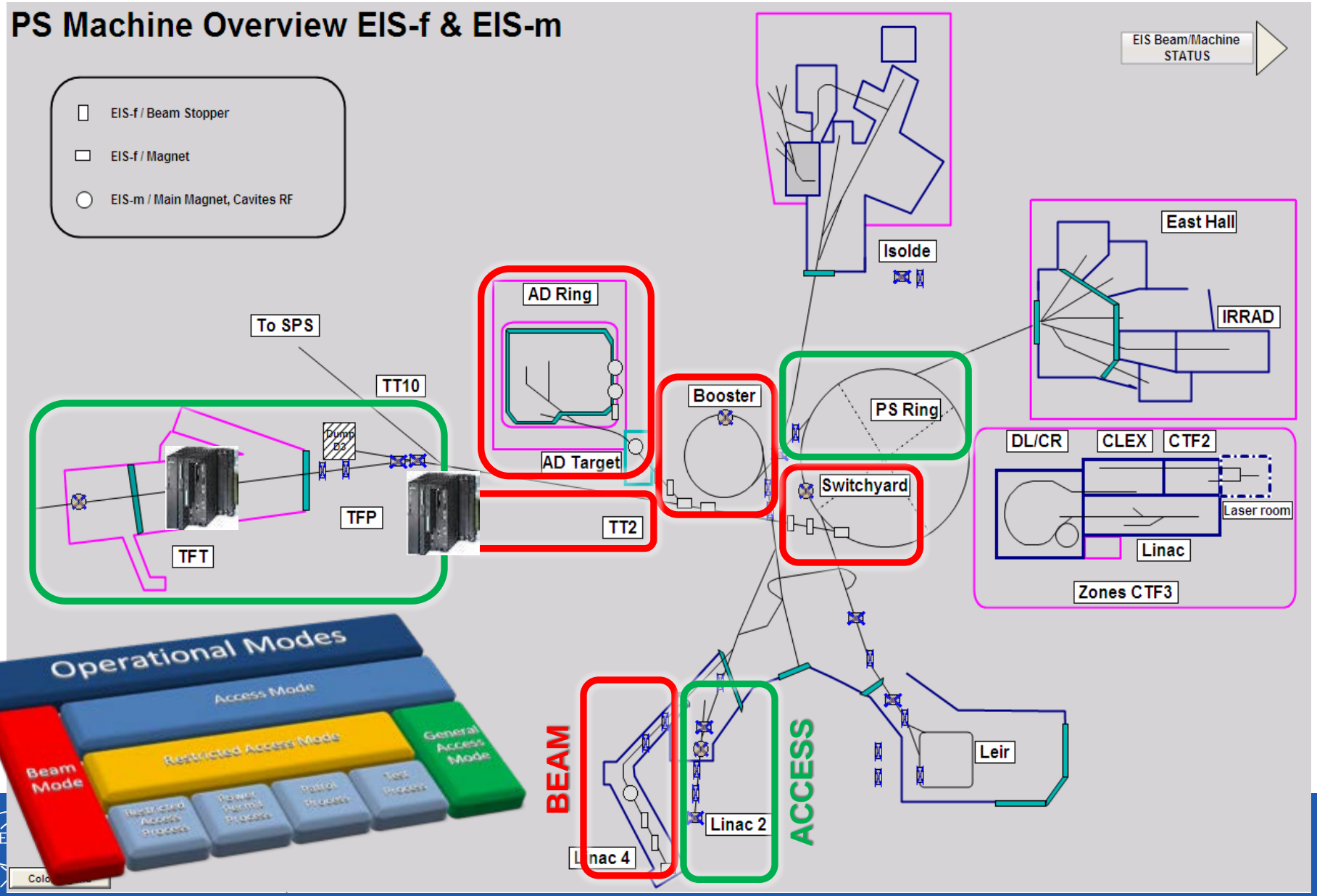
PS-PPS Project Scope



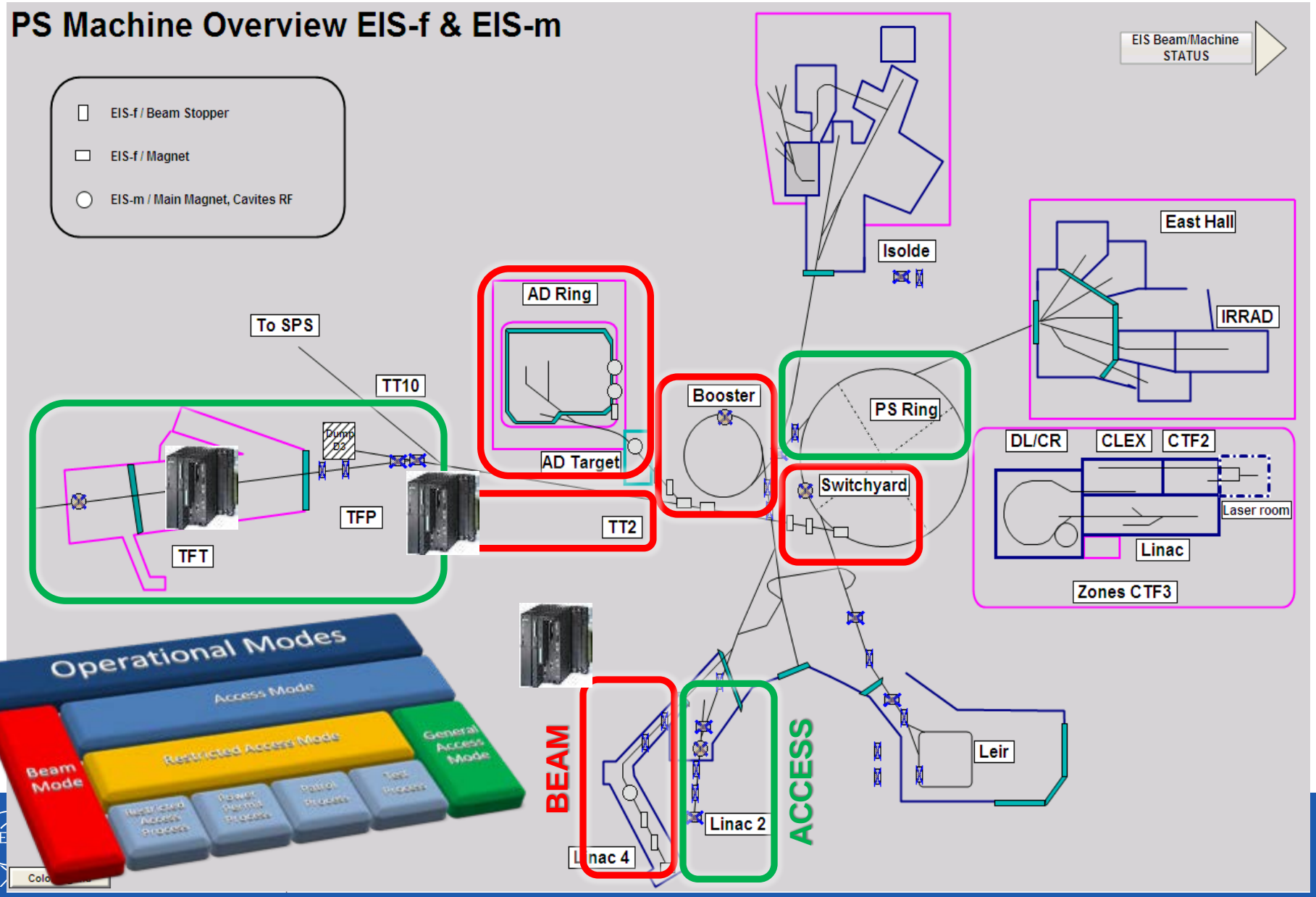
PS-PPS Project Scope



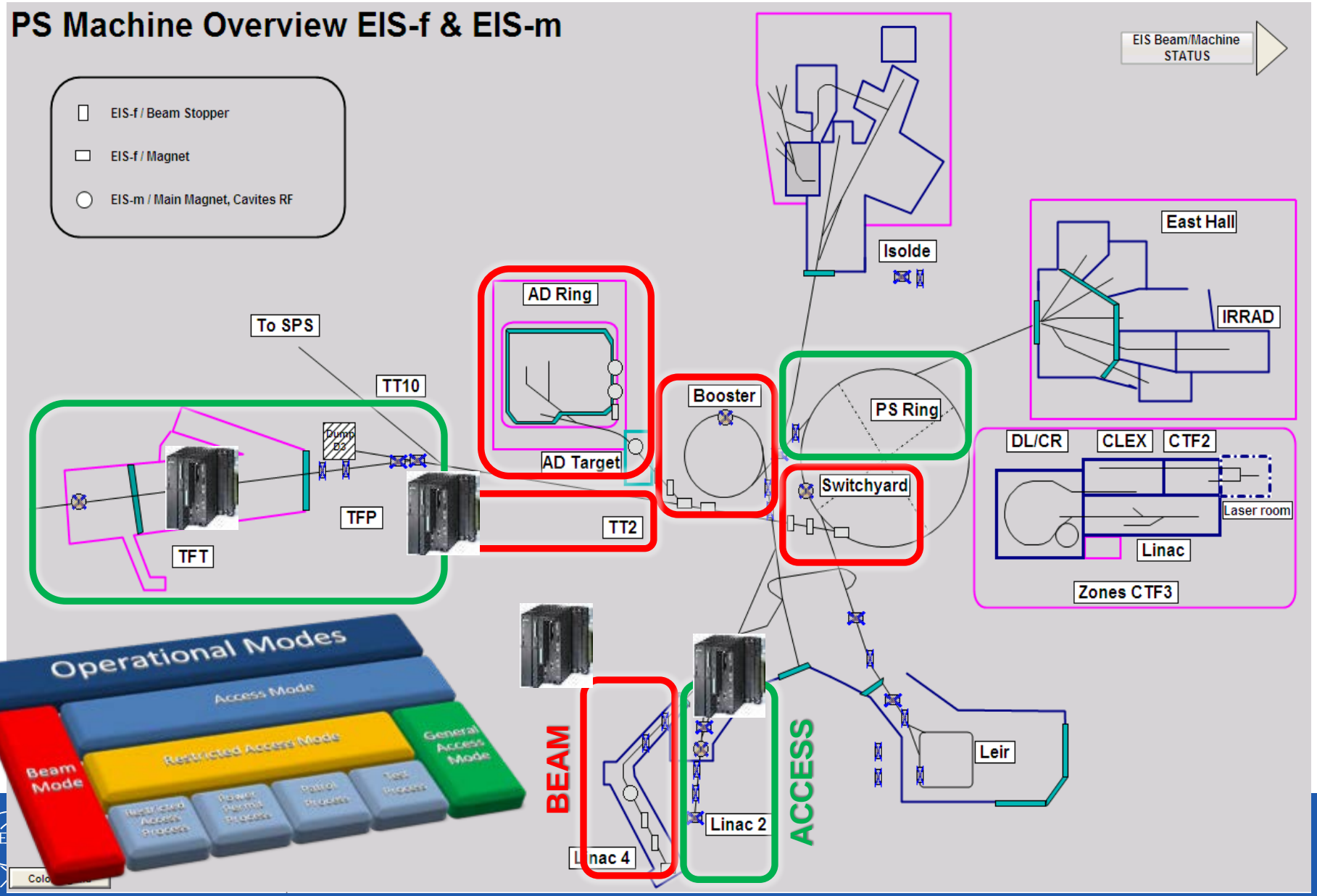
PS-PPS Project Scope



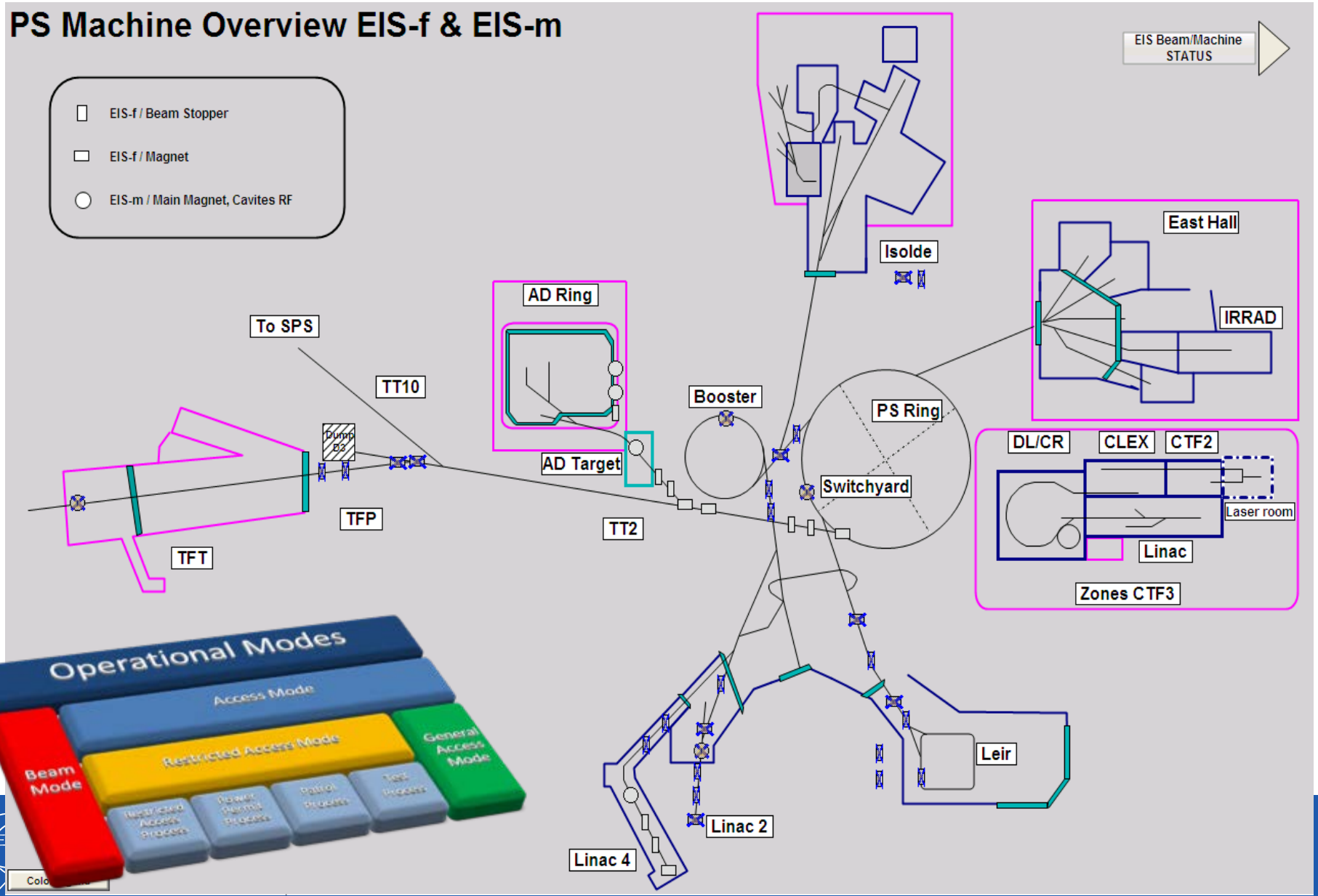
PS-PPS Project Scope



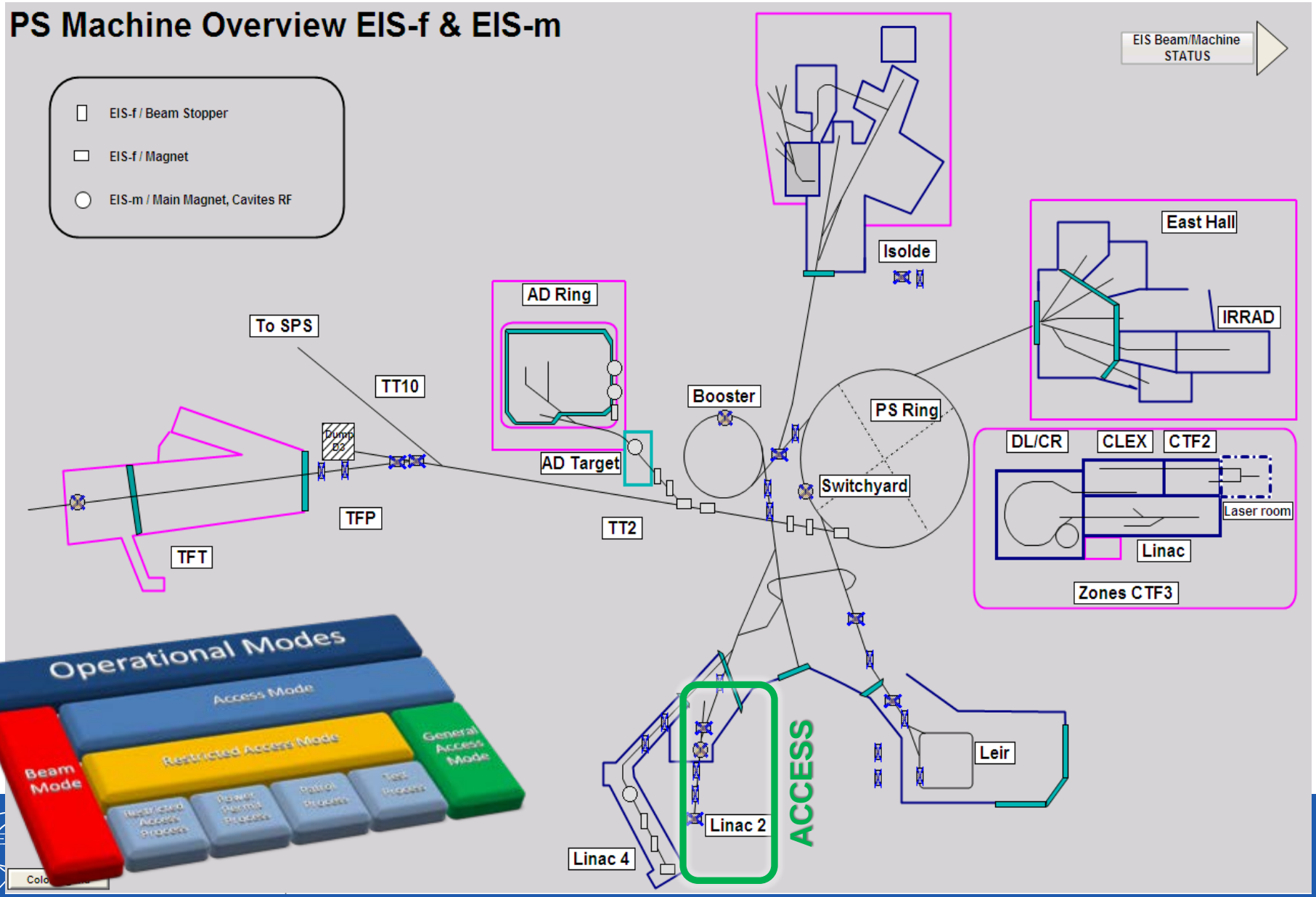
PS-PPS Project Scope



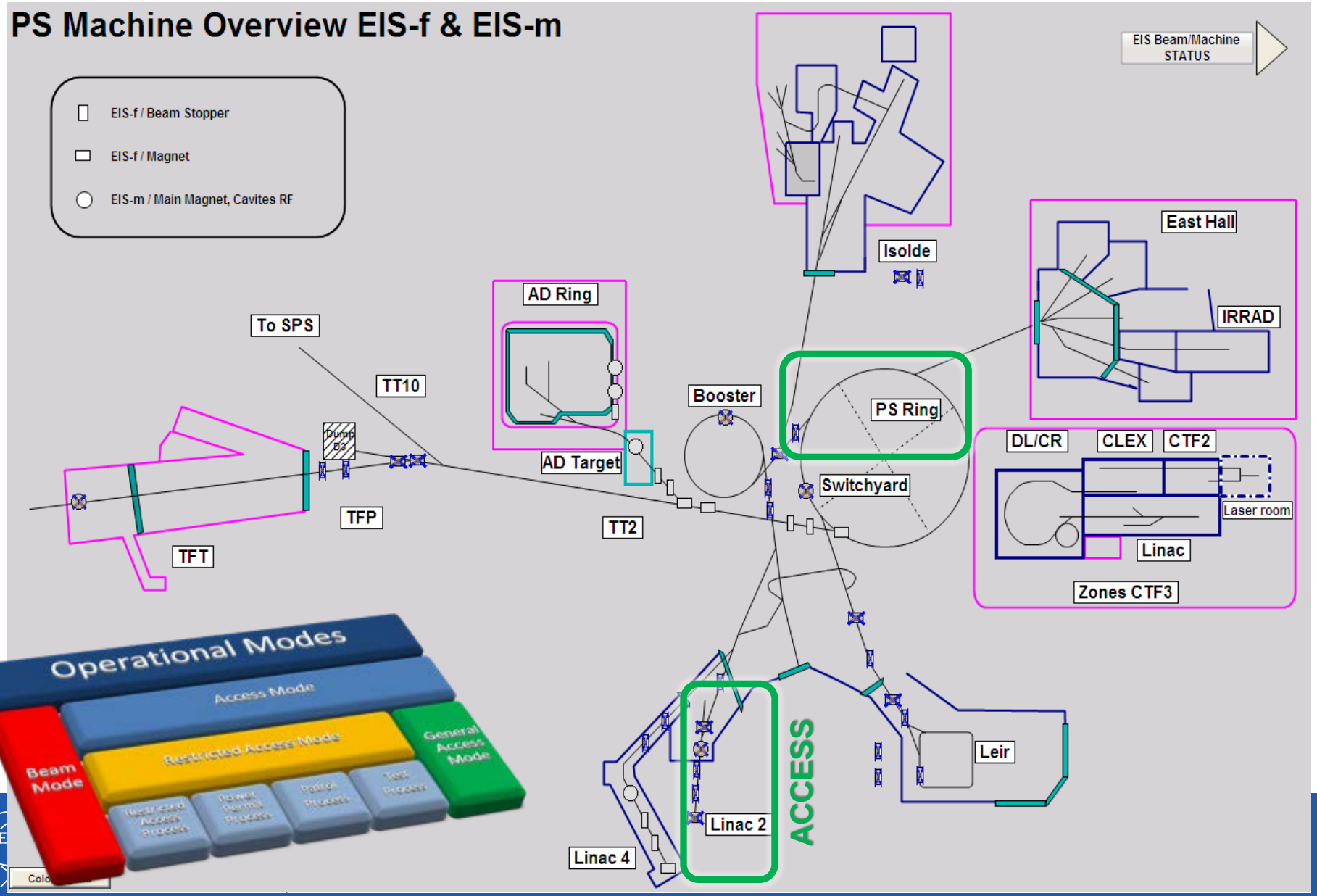
PS-PPS Project Scope



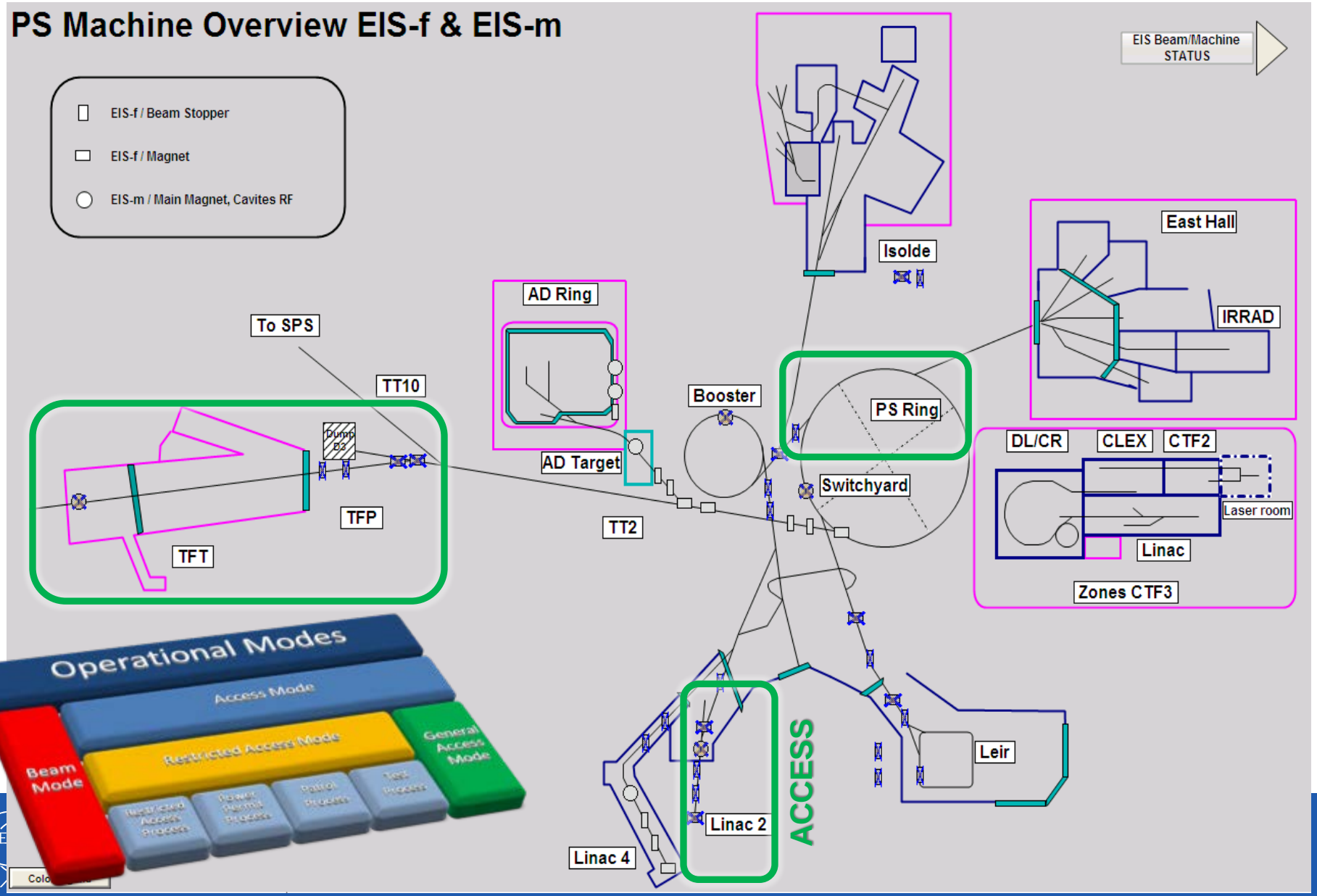
PS-PPS Project Scope



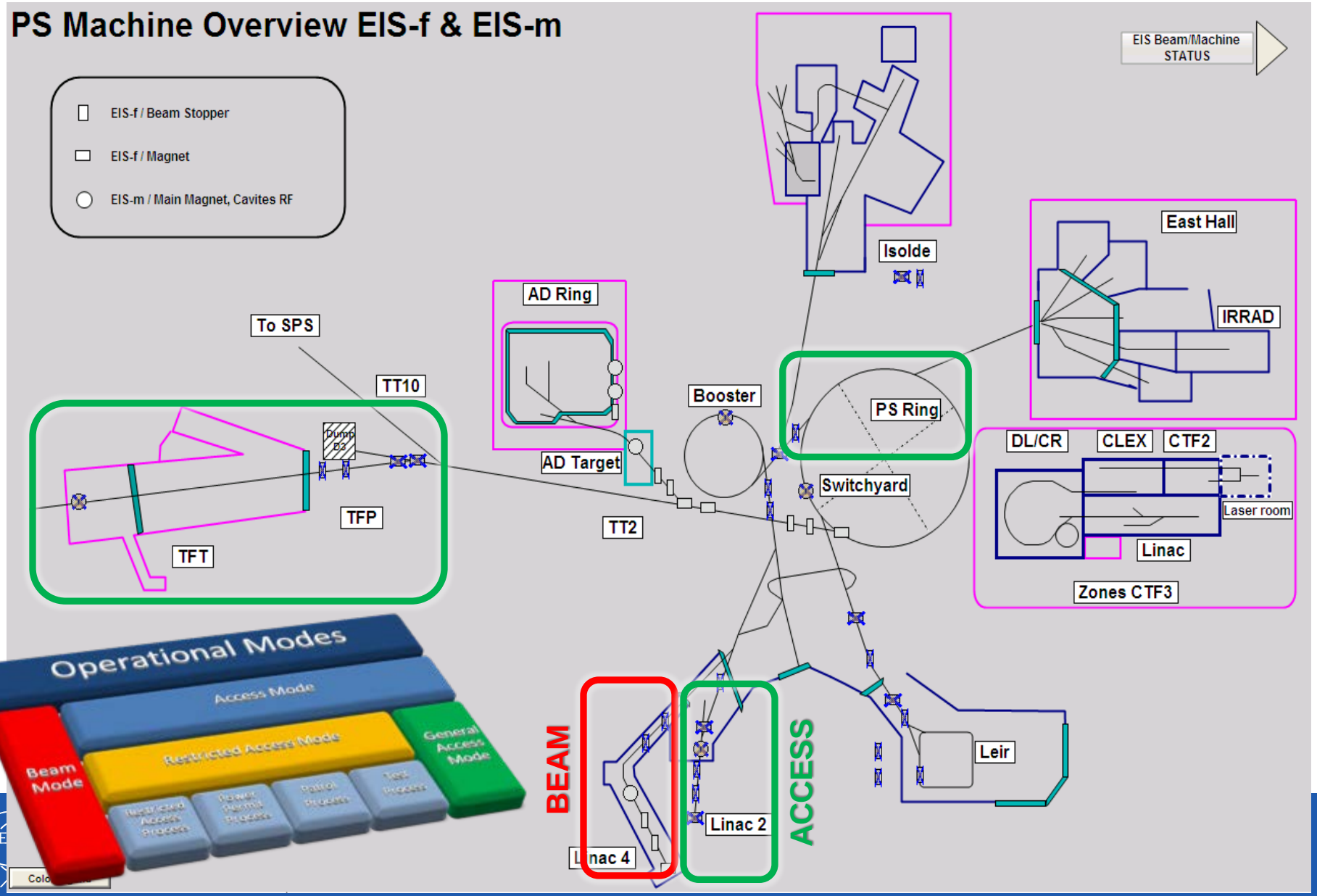
PS-PPS Project Scope



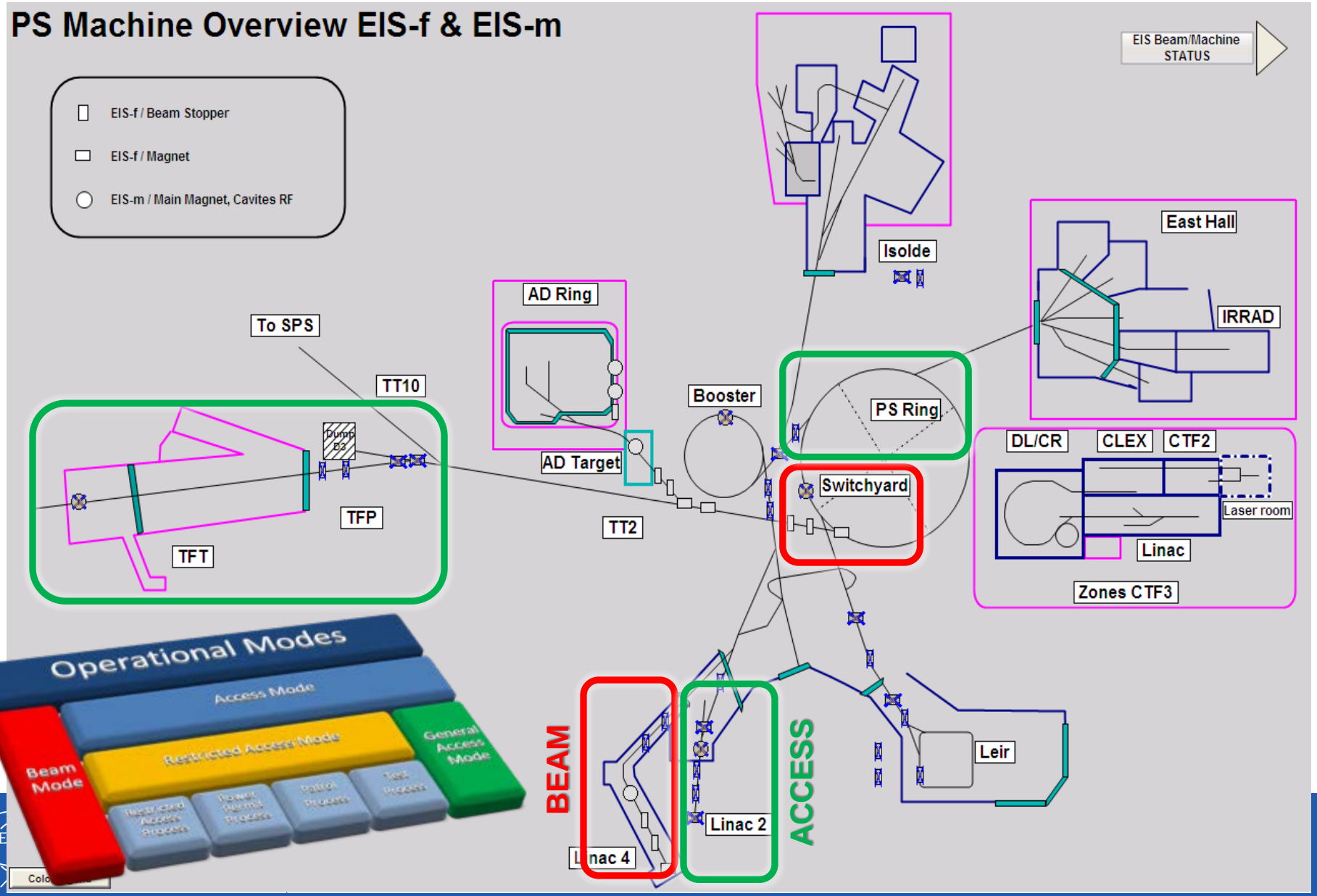
PS-PPS Project Scope



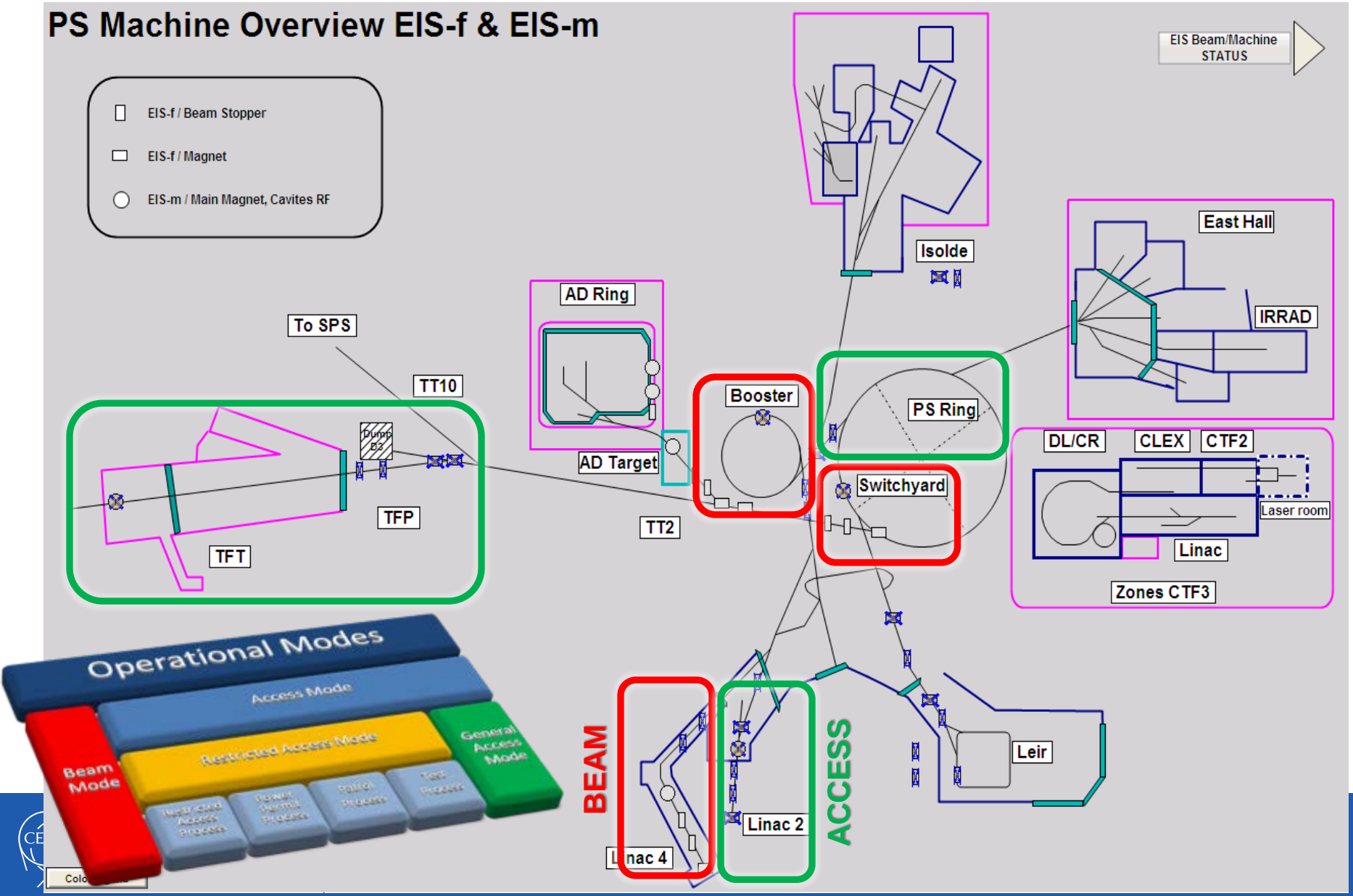
PS-PPS Project Scope



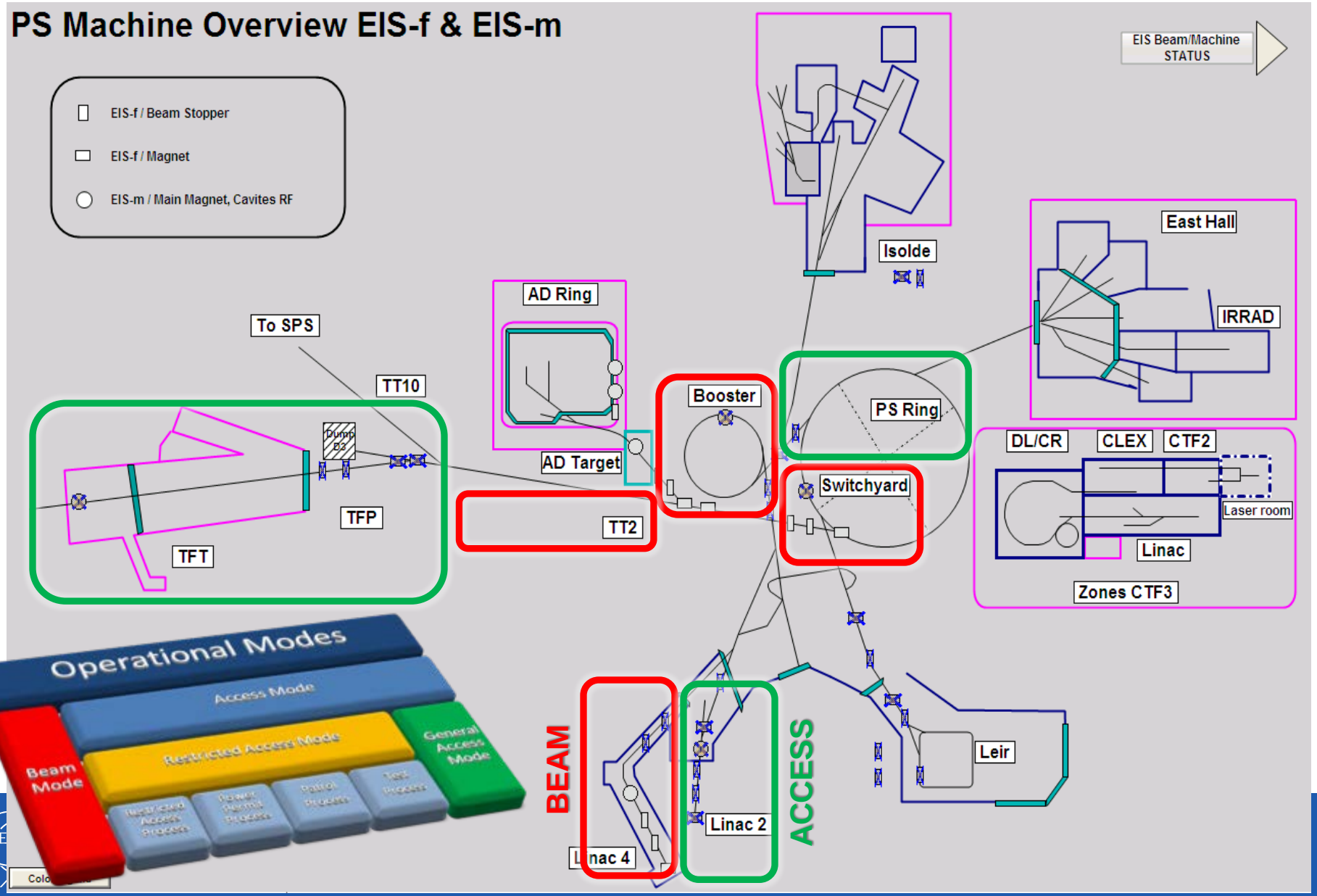
PS-PPS Project Scope



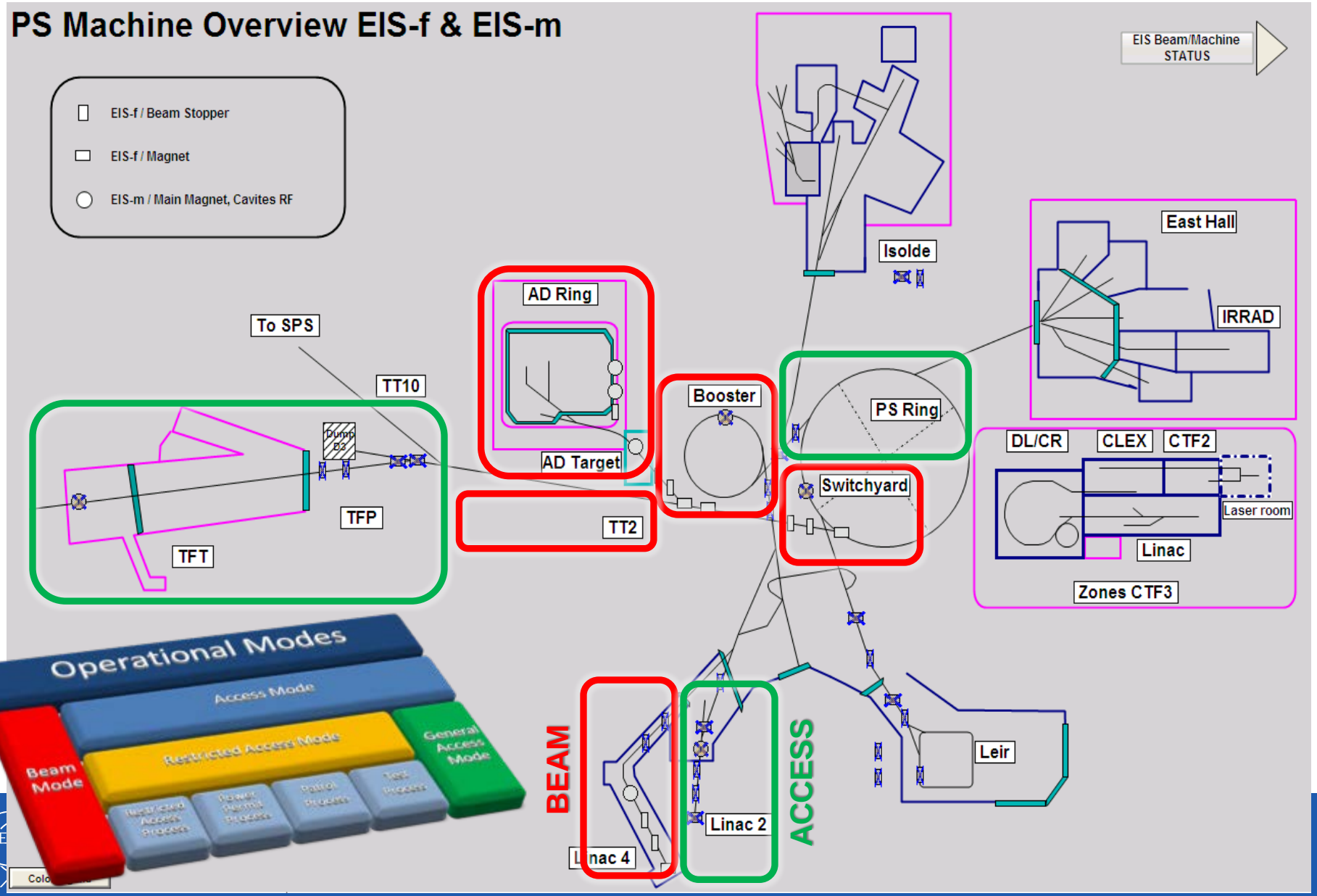
PS-PPS Project Scope



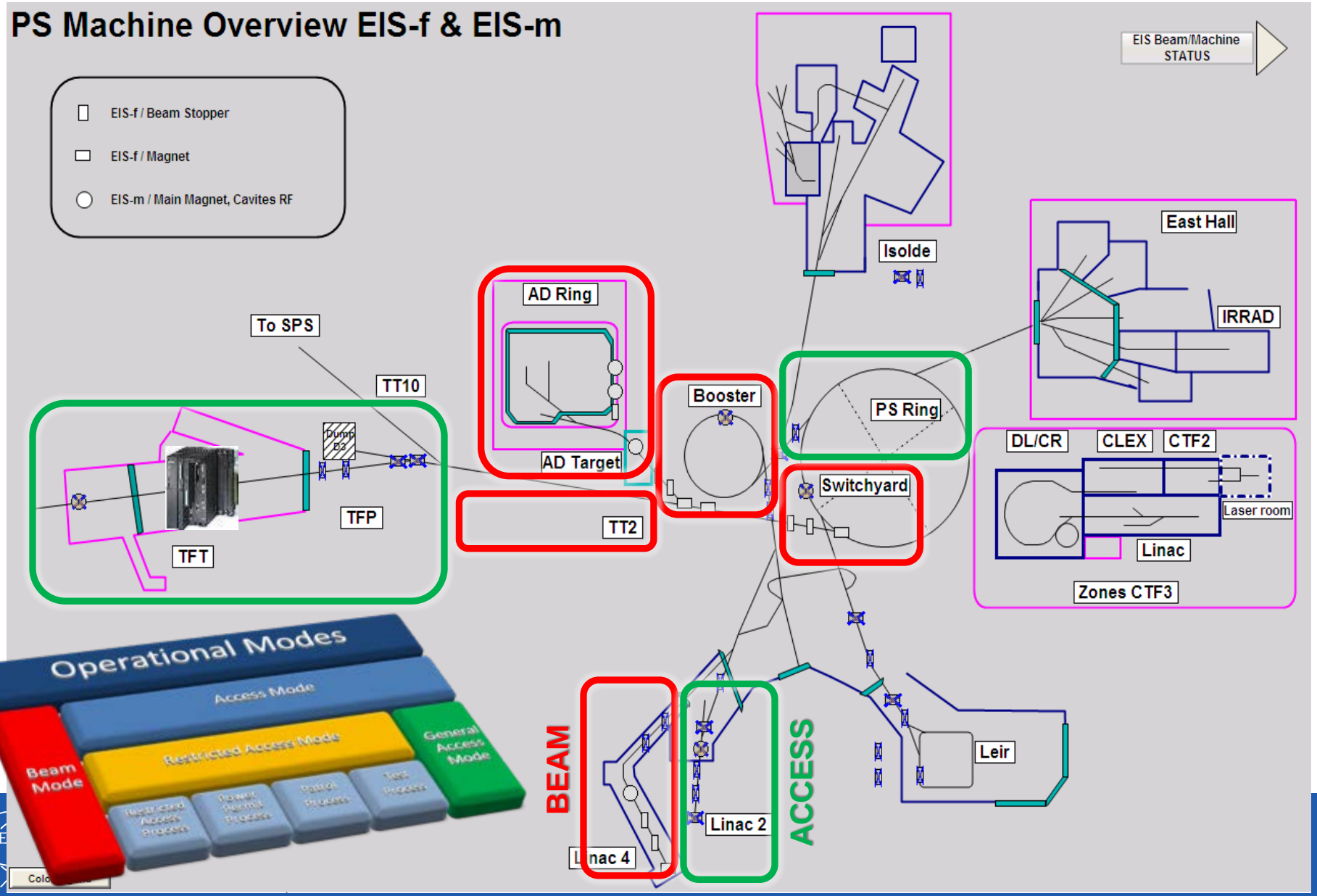
PS-PPS Project Scope



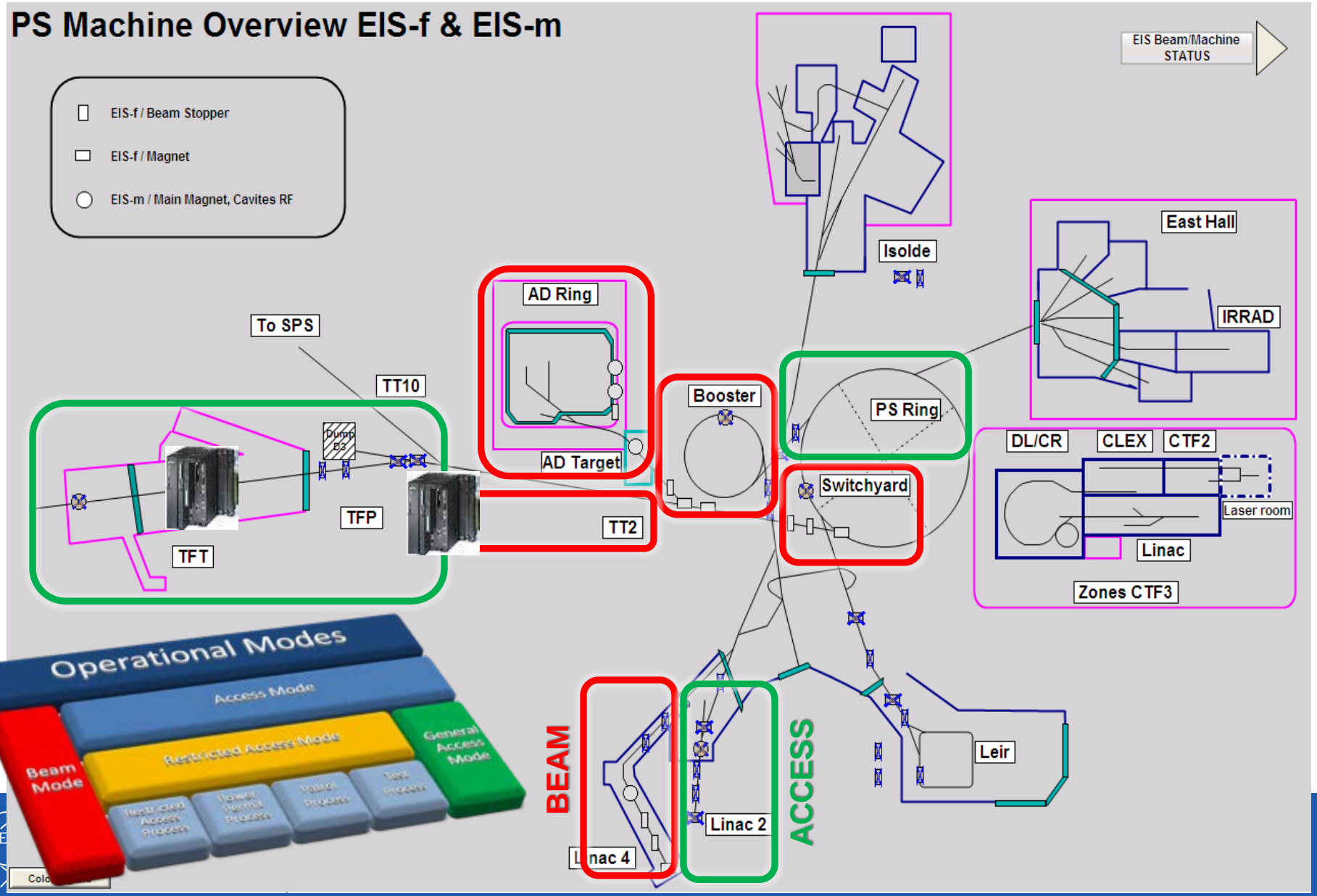
PS-PPS Project Scope



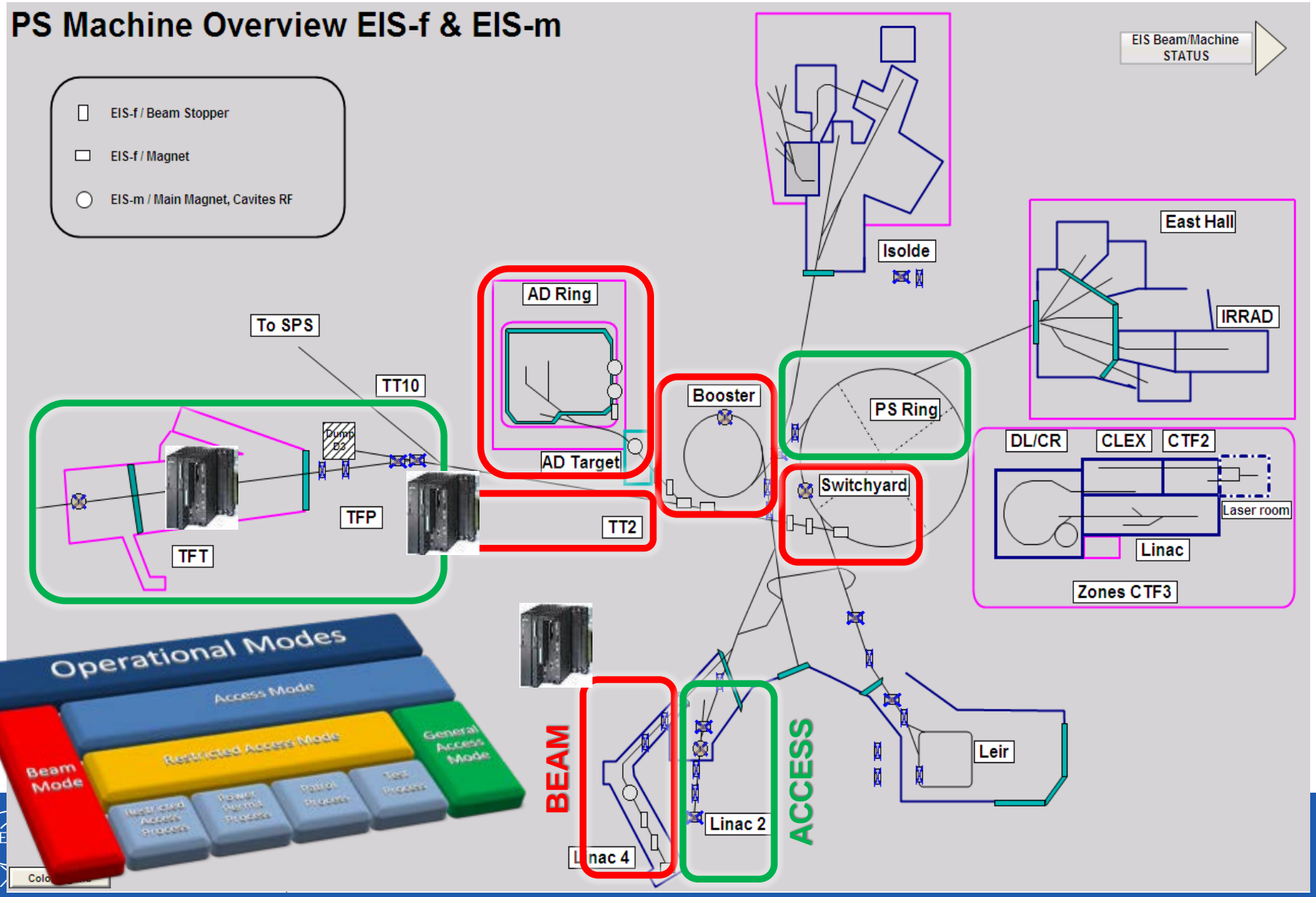
PS-PPS Project Scope



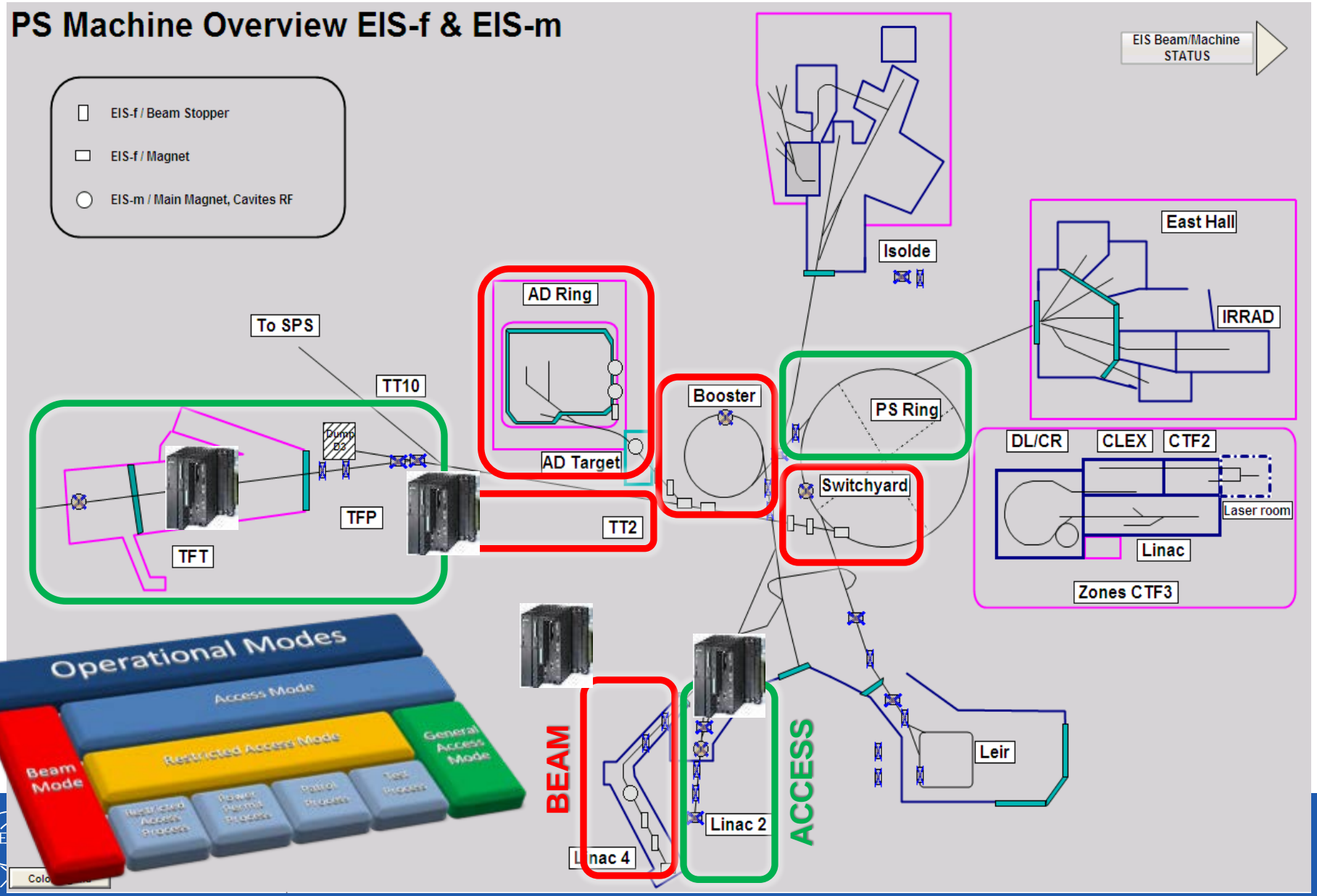
PS-PPS Project Scope



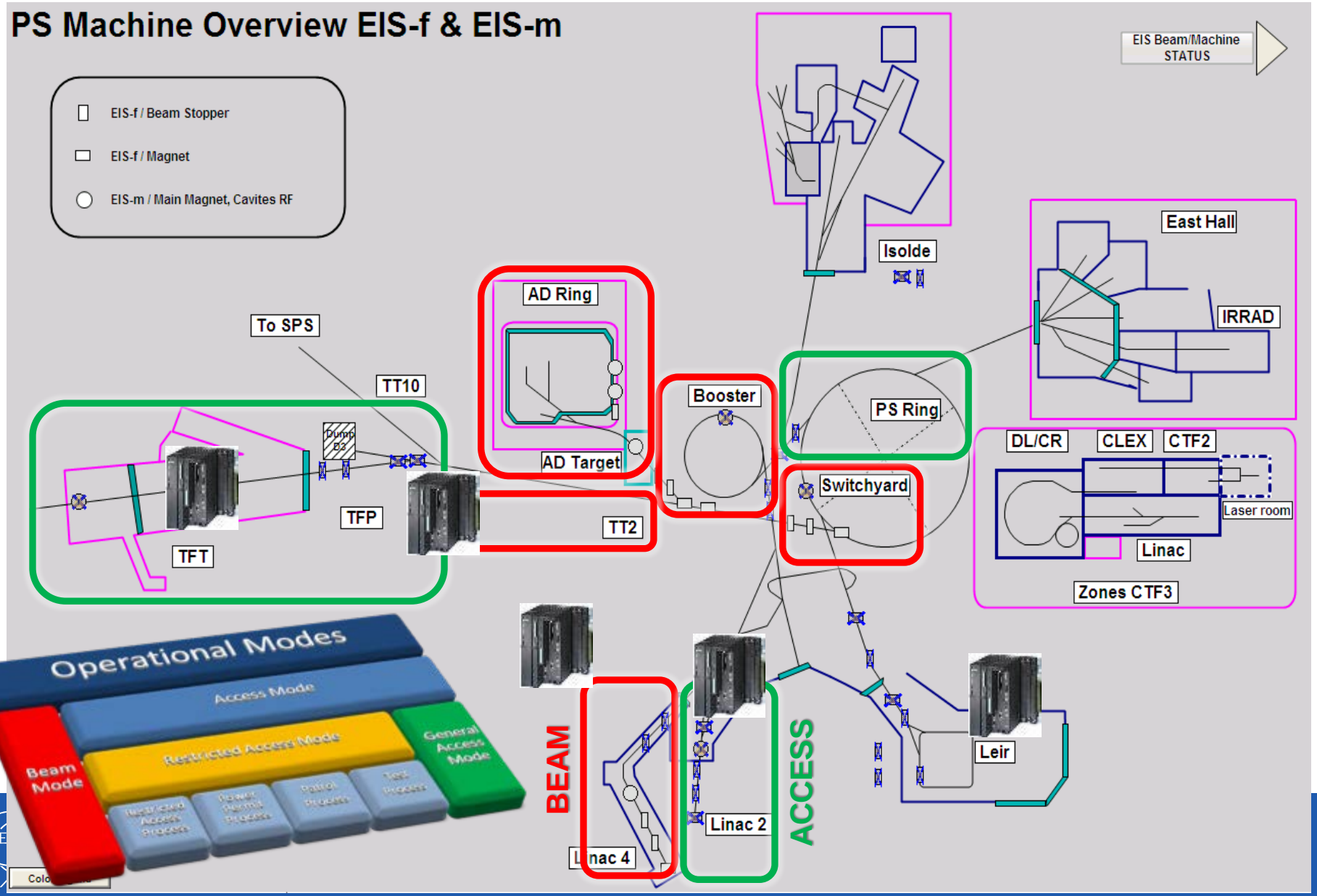
PS-PPS Project Scope



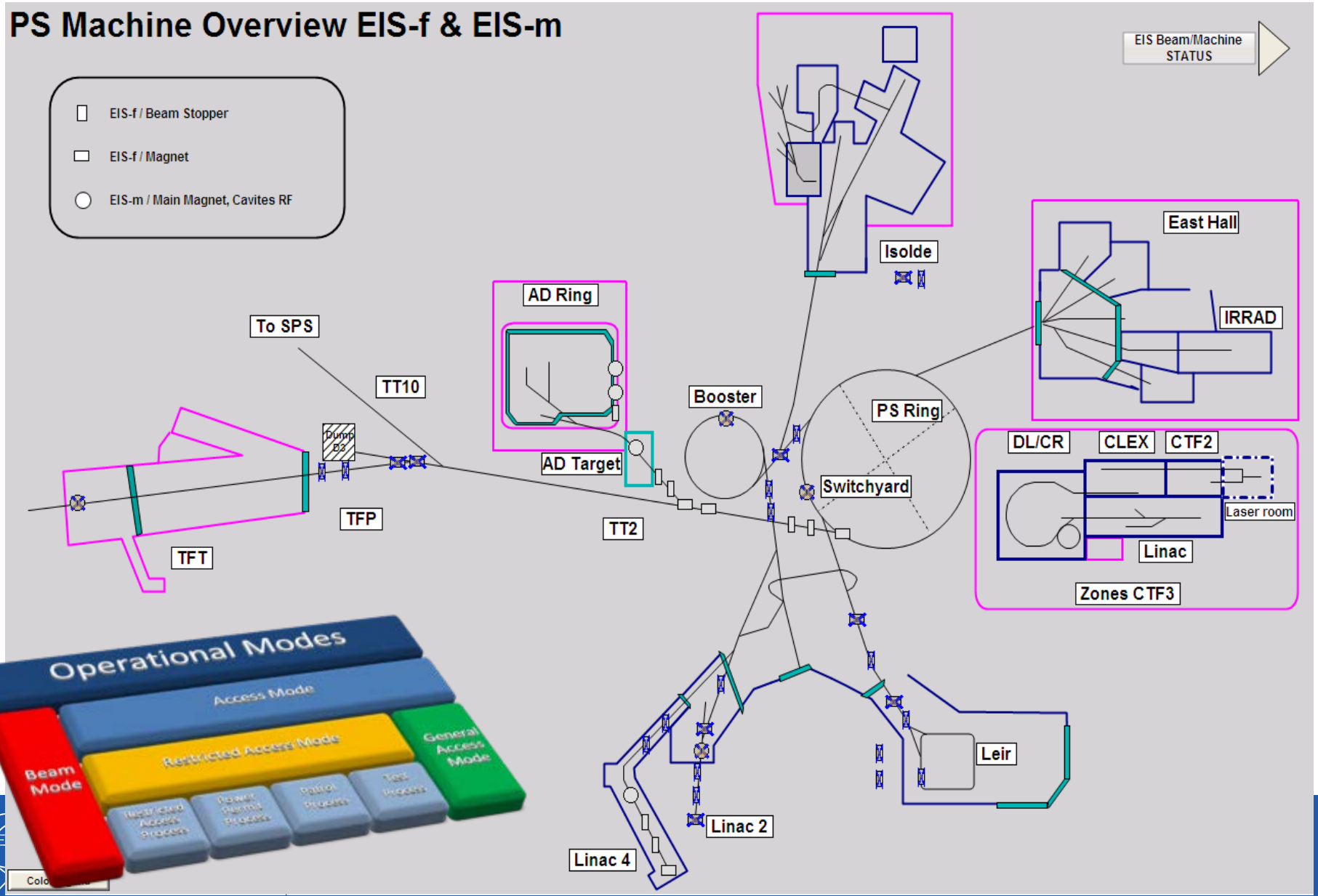
PS-PPS Project Scope



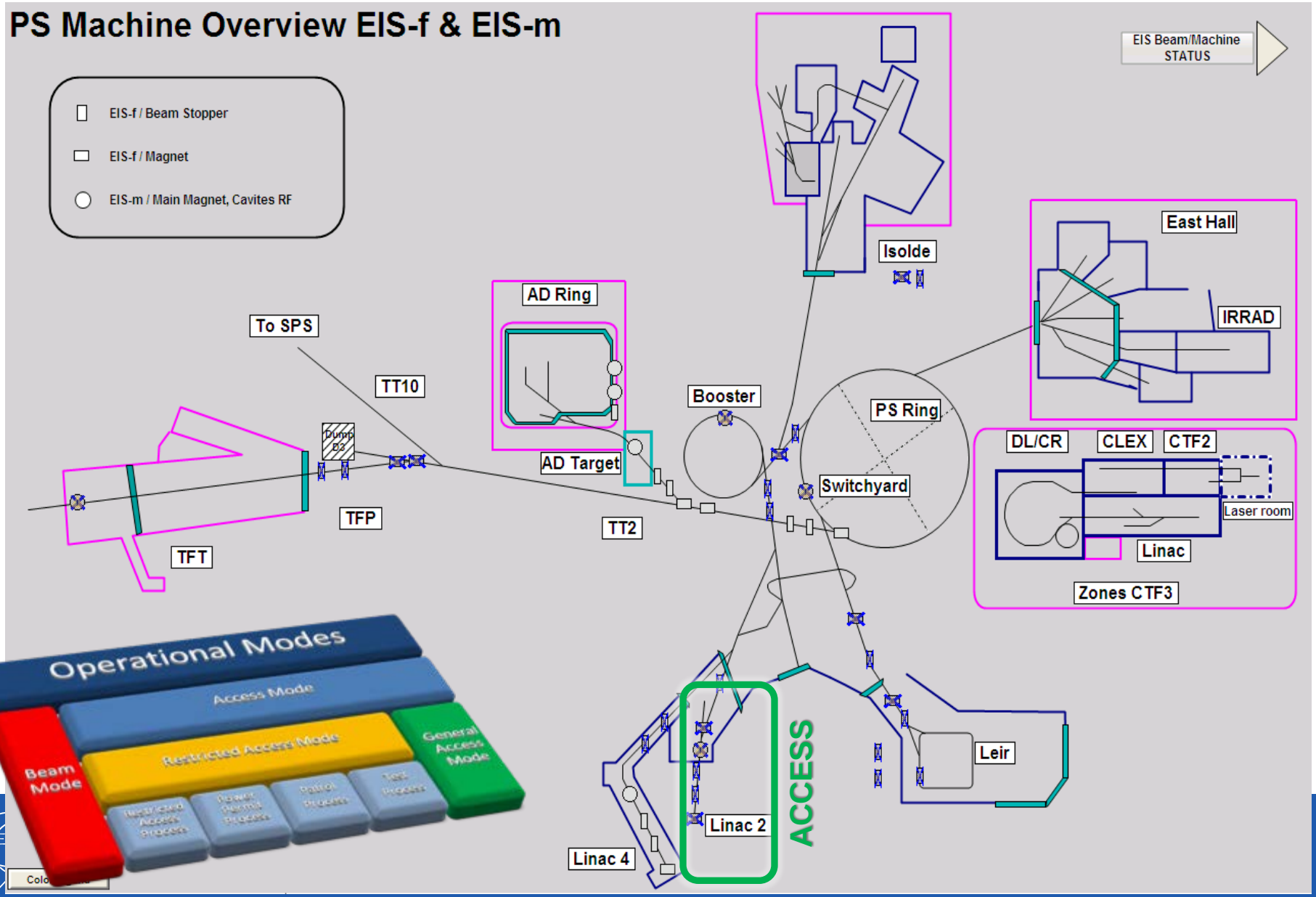
PS-PPS Project Scope



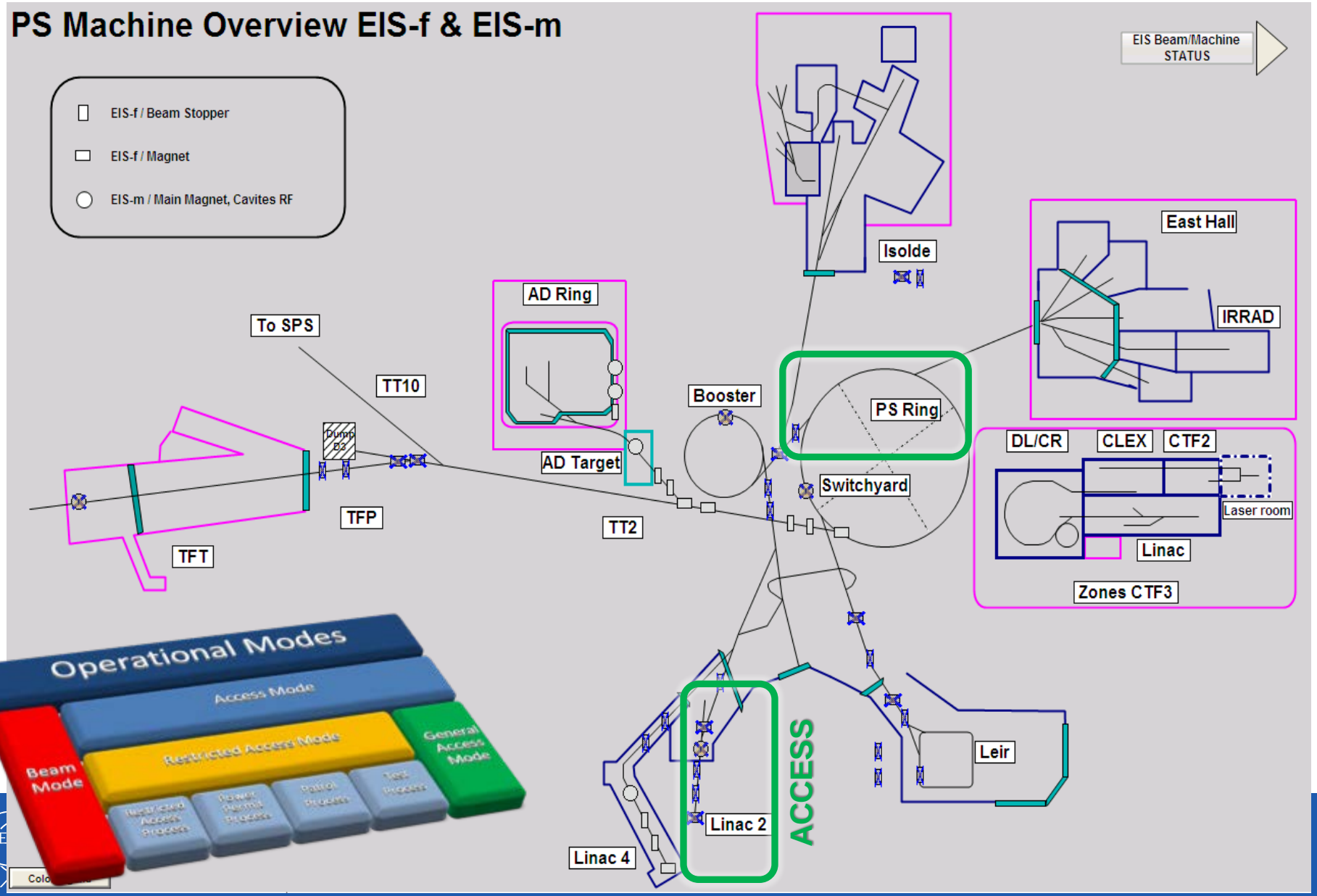
PS-PPS Project Scope



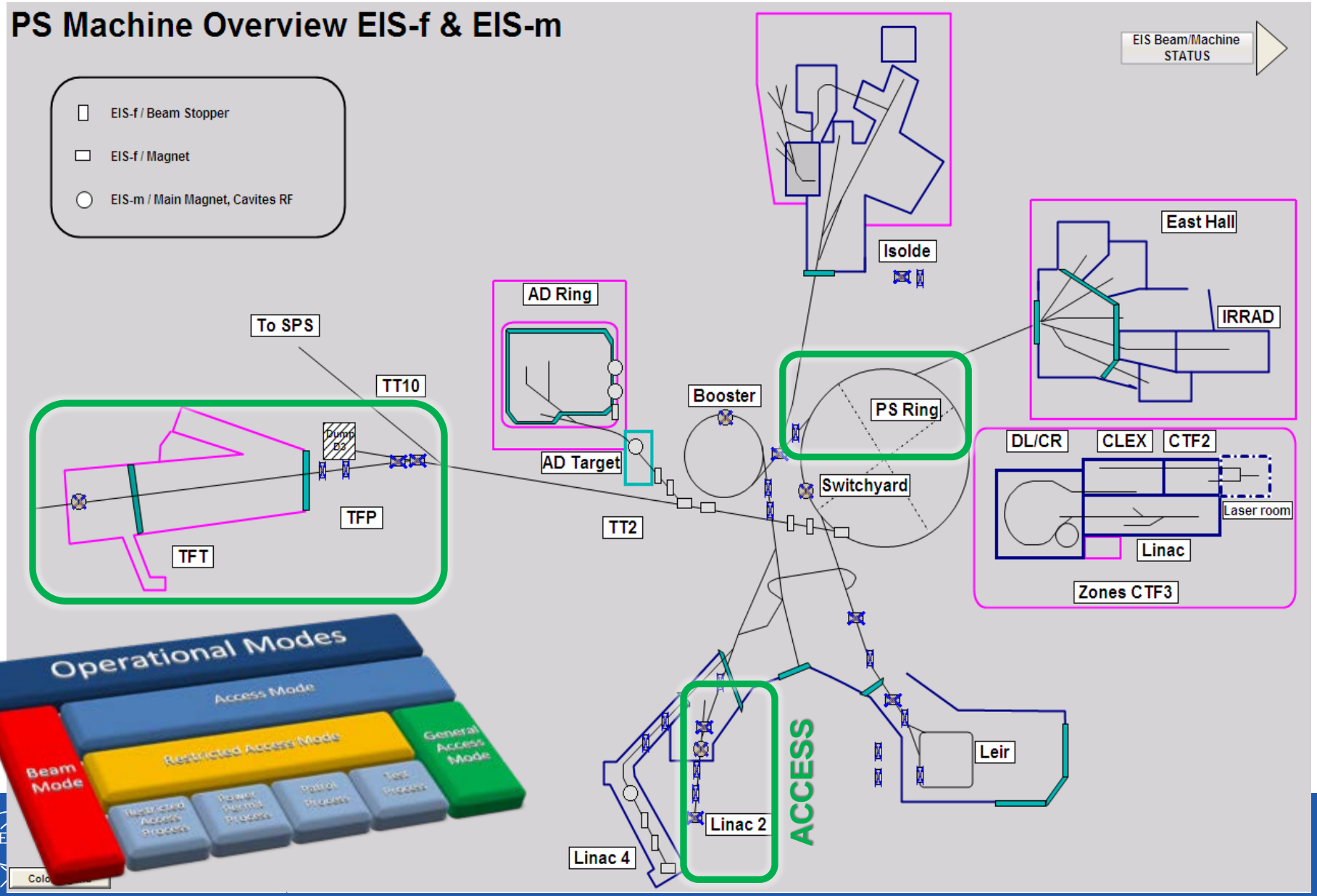
PS-PPS Project Scope



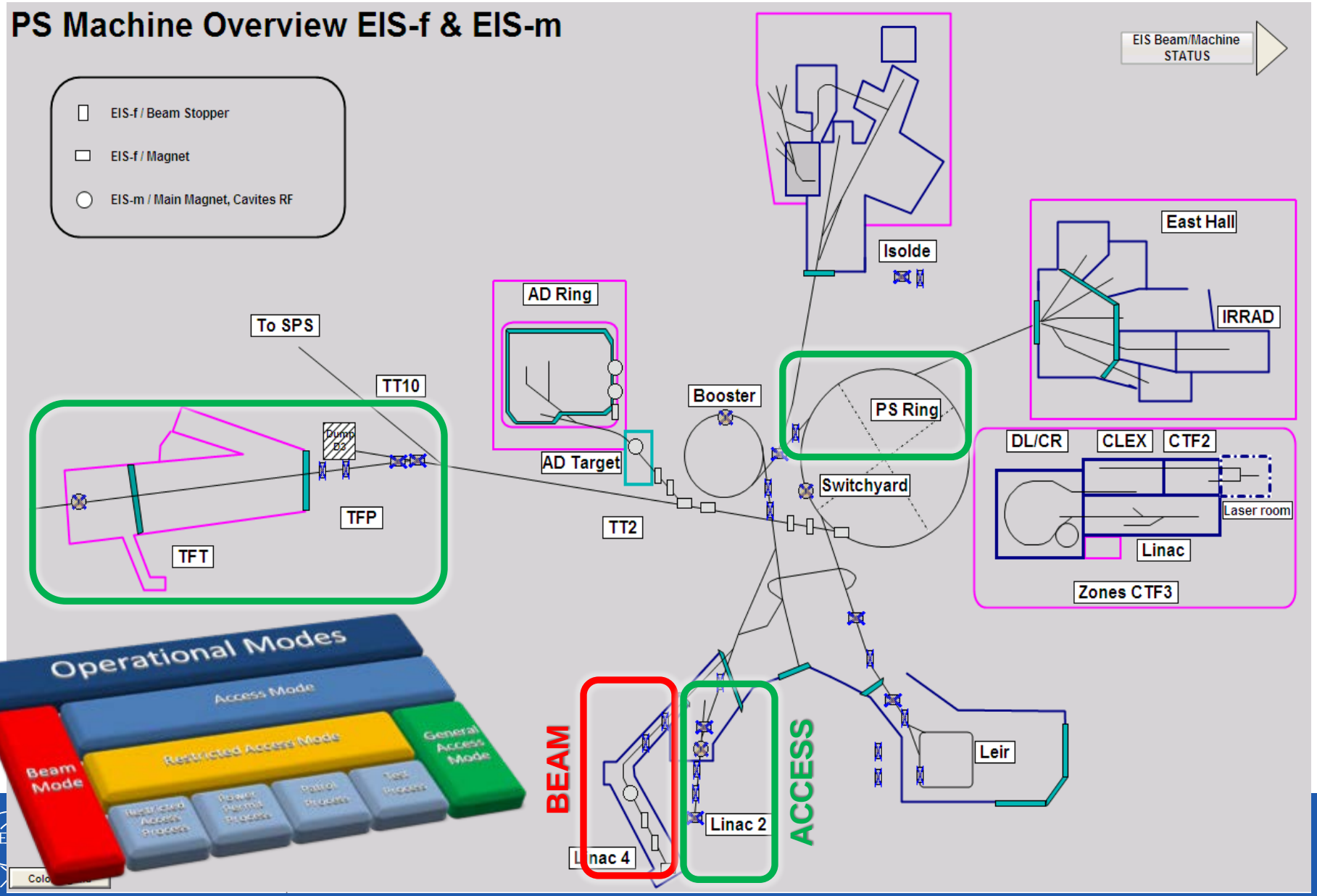
PS-PPS Project Scope



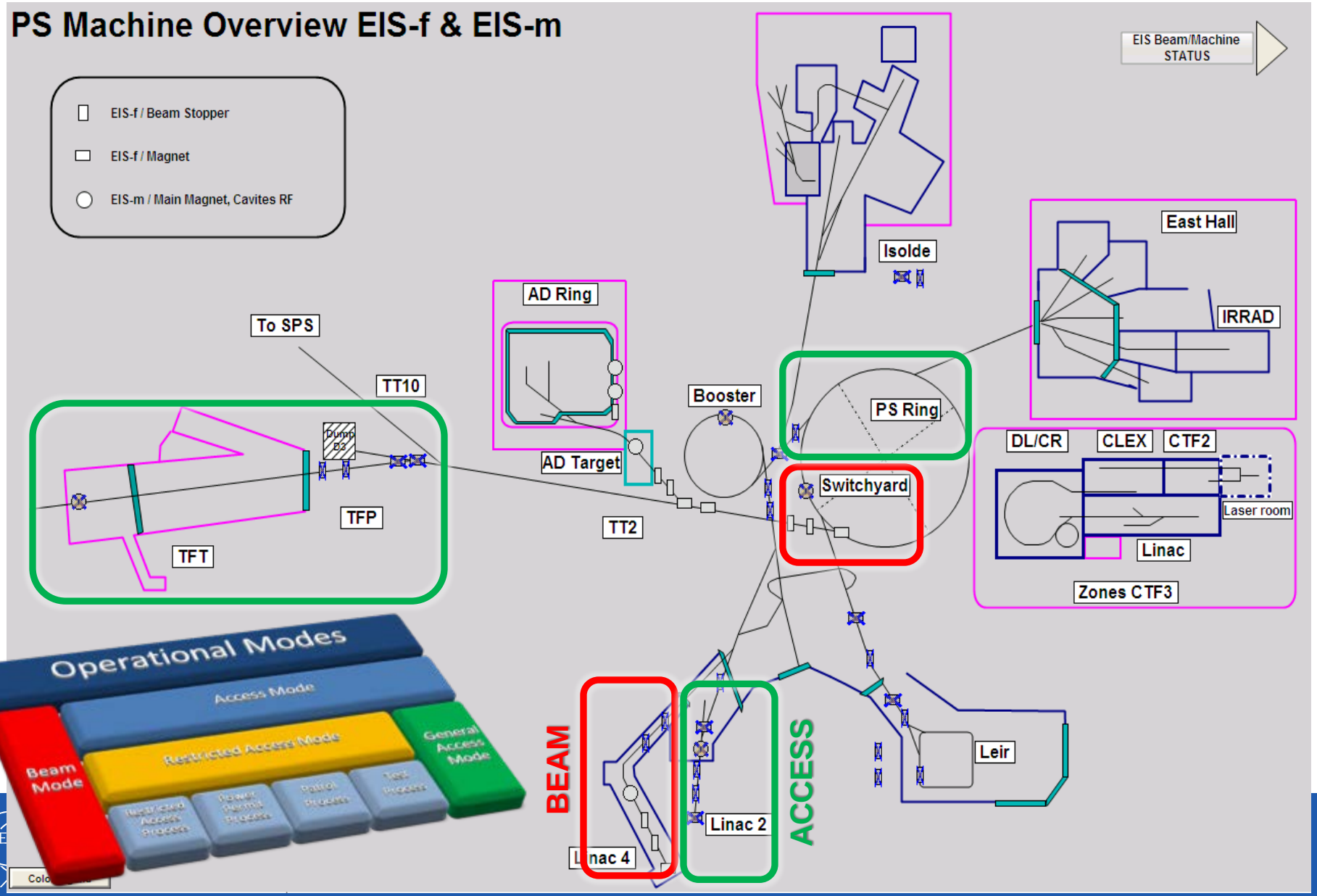
PS-PPS Project Scope



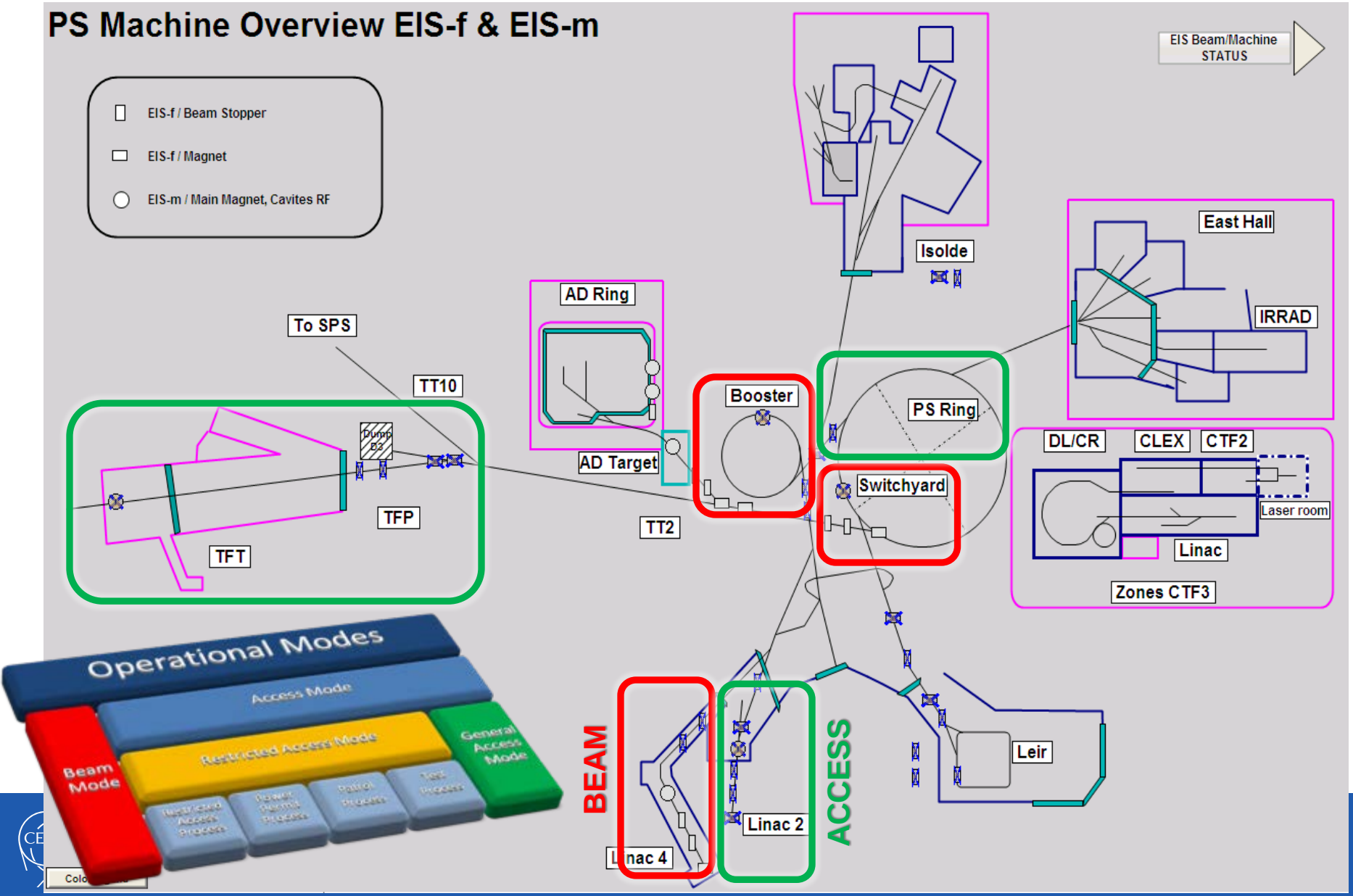
PS-PPS Project Scope



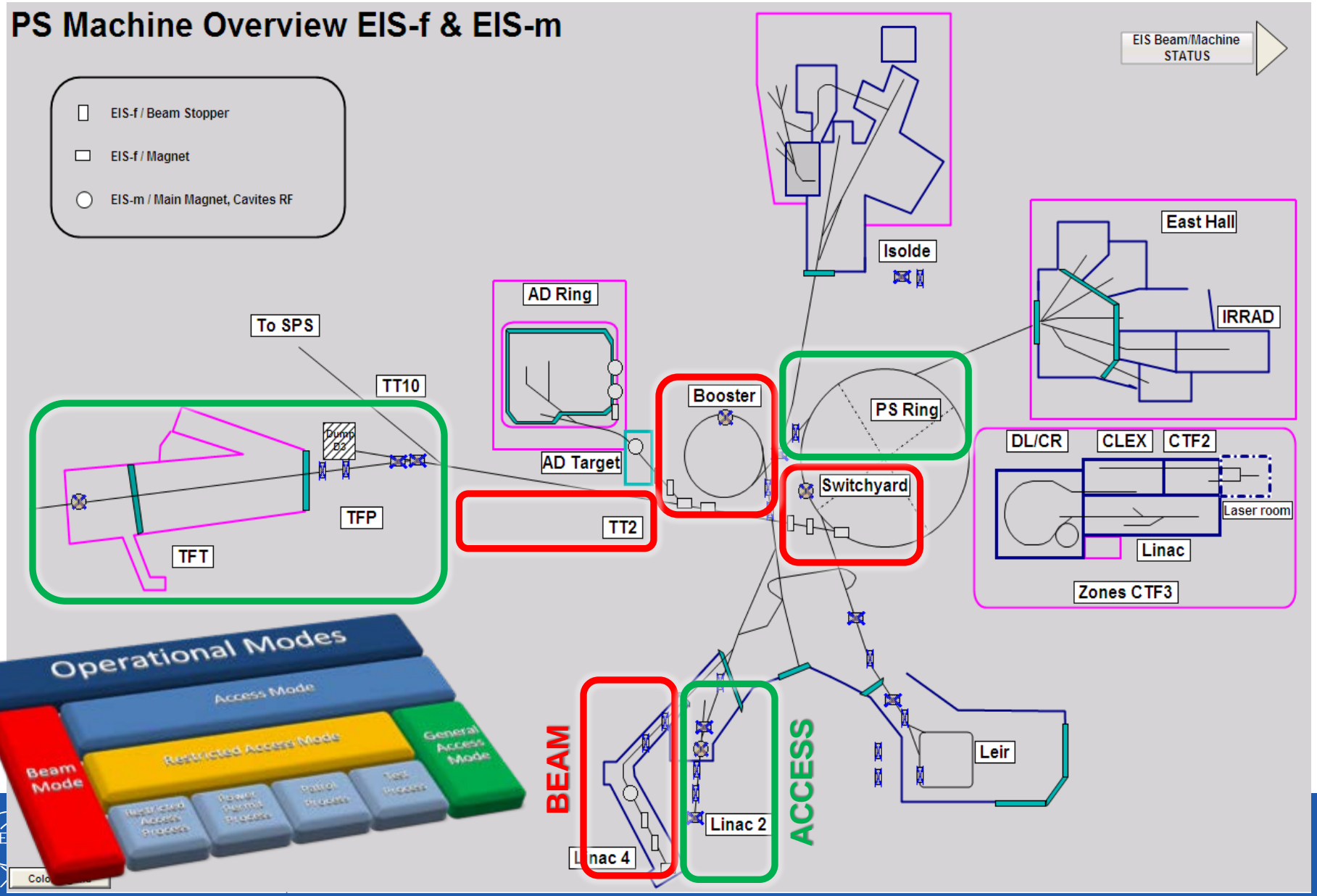
PS-PPS Project Scope



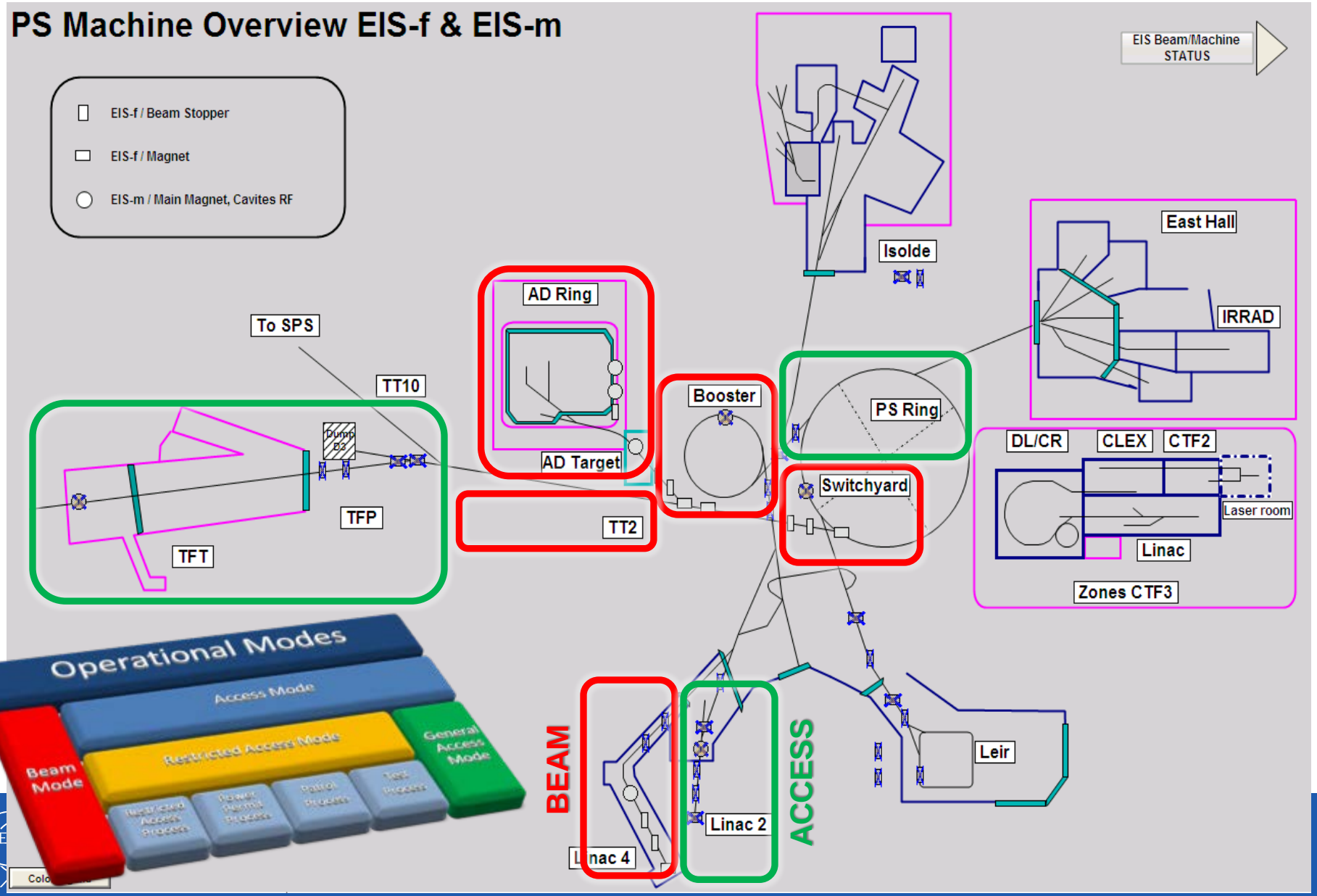
PS-PPS Project Scope



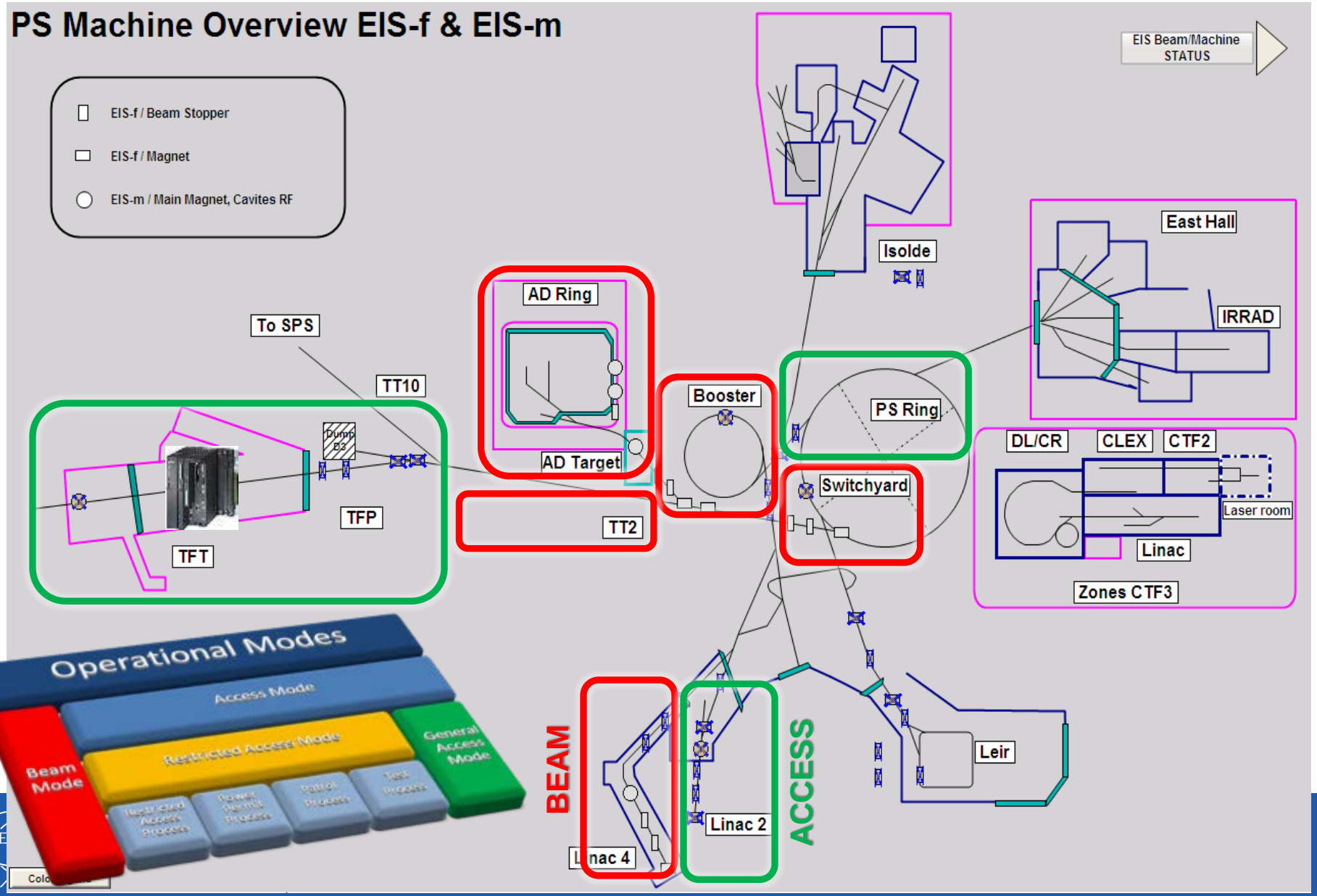
PS-PPS Project Scope



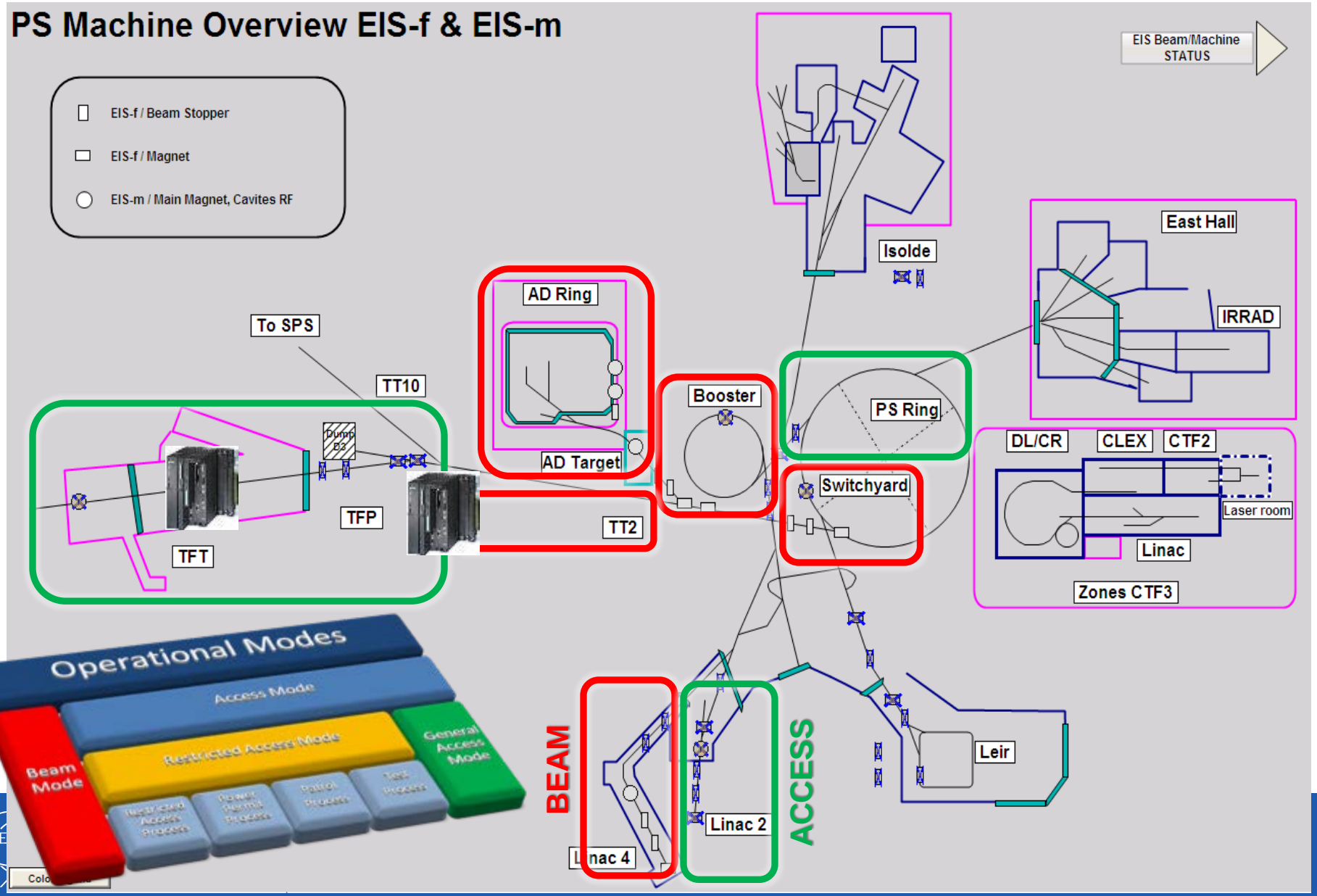
PS-PPS Project Scope



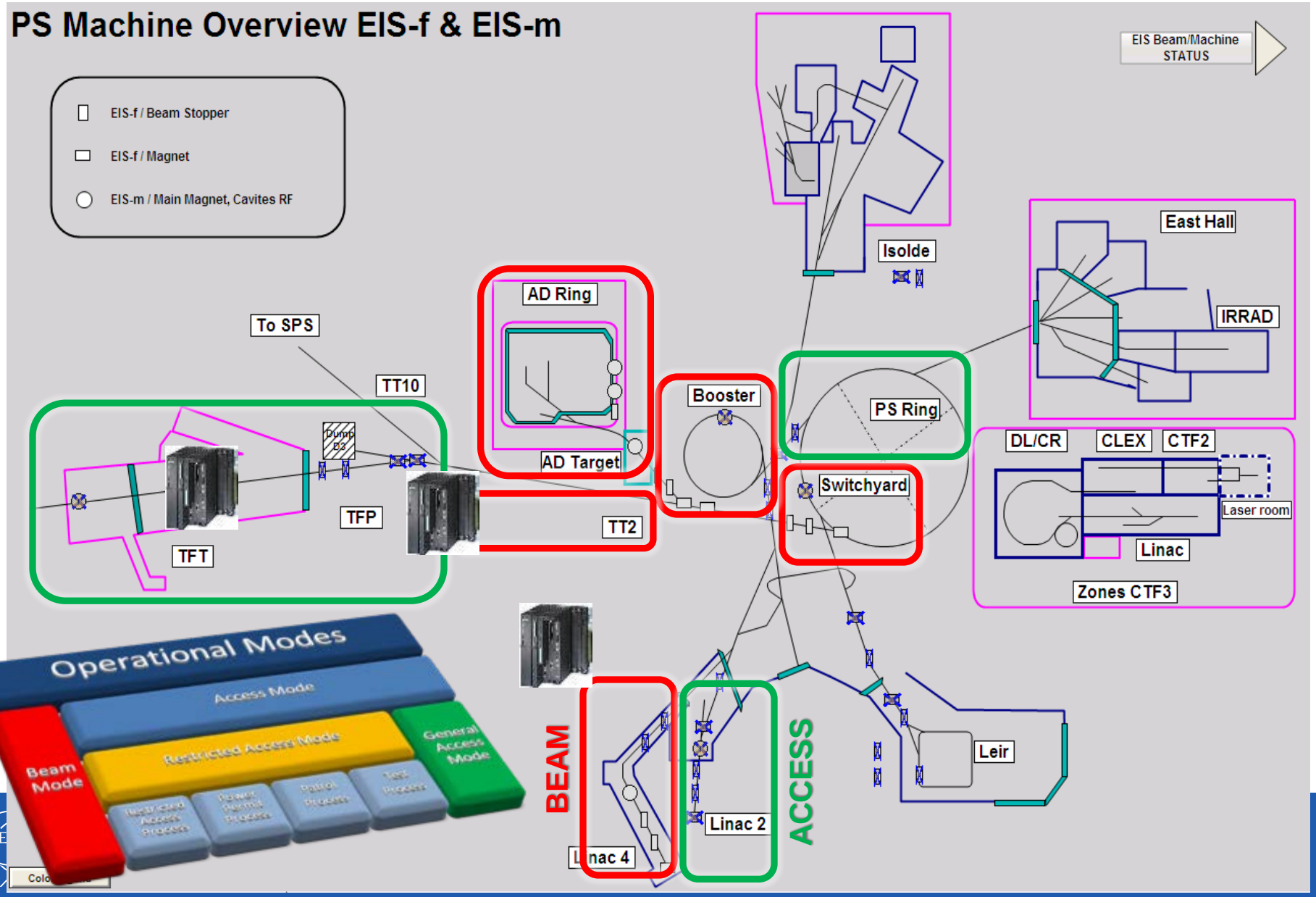
PS-PPS Project Scope



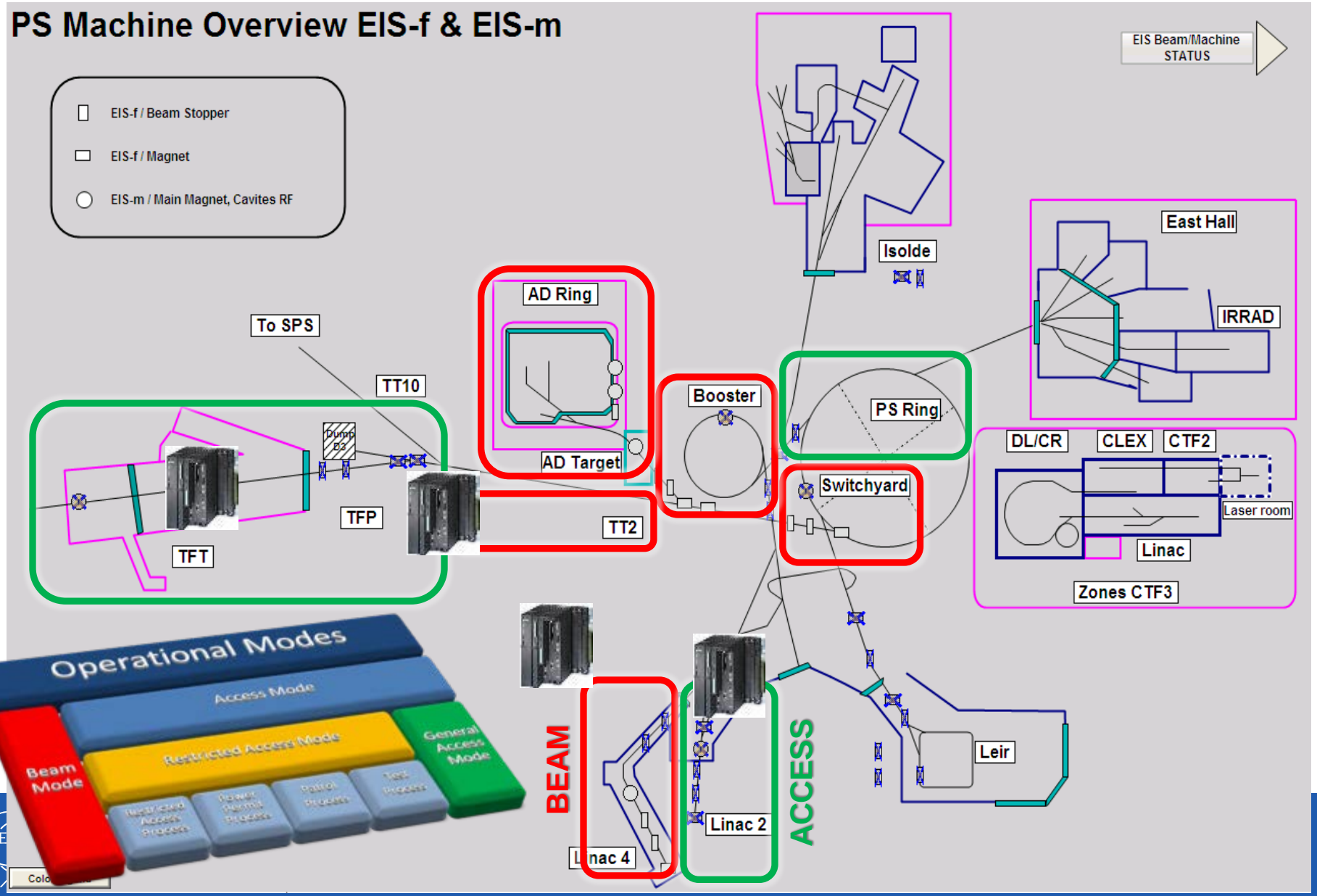
PS-PPS Project Scope



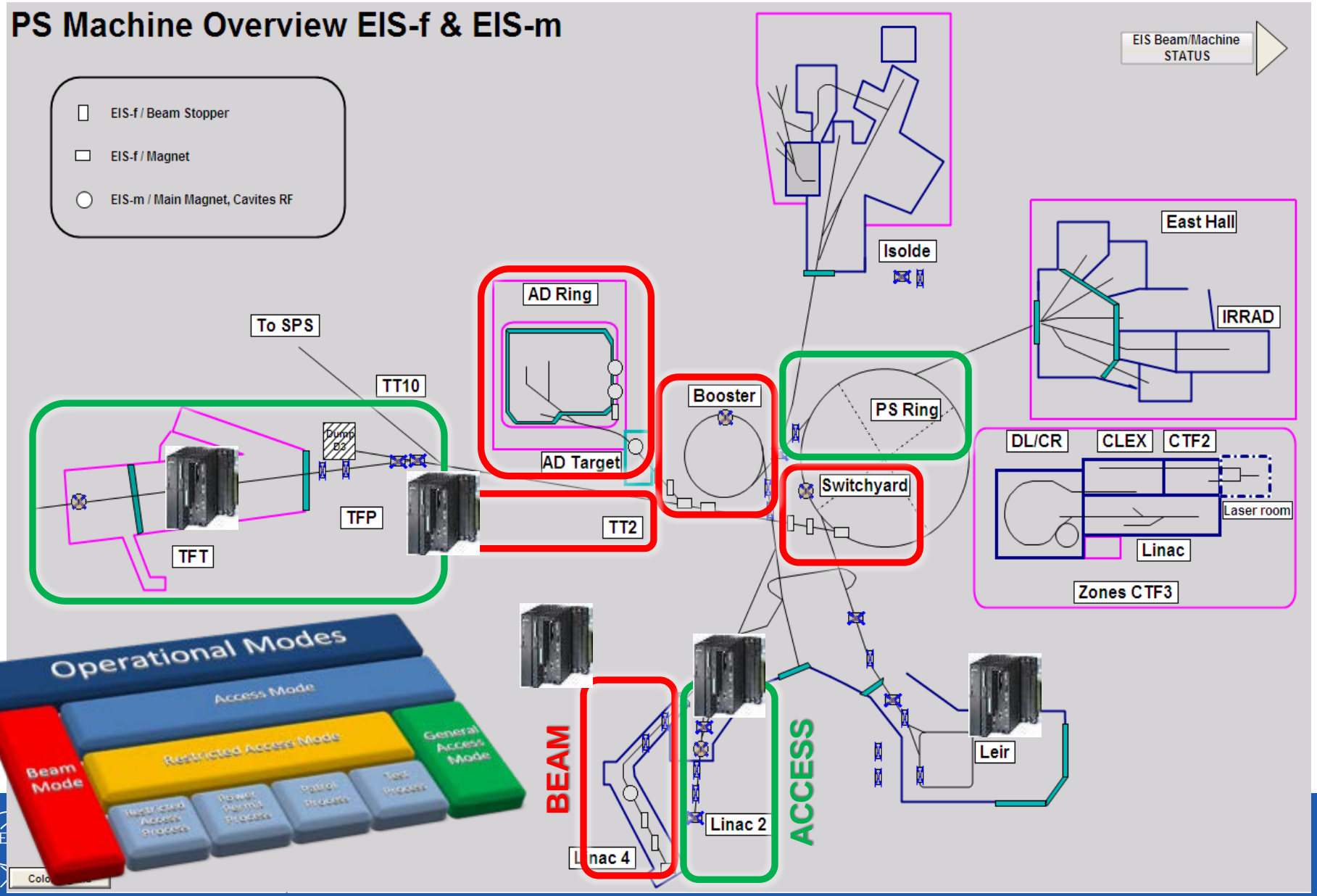
PS-PPS Project Scope



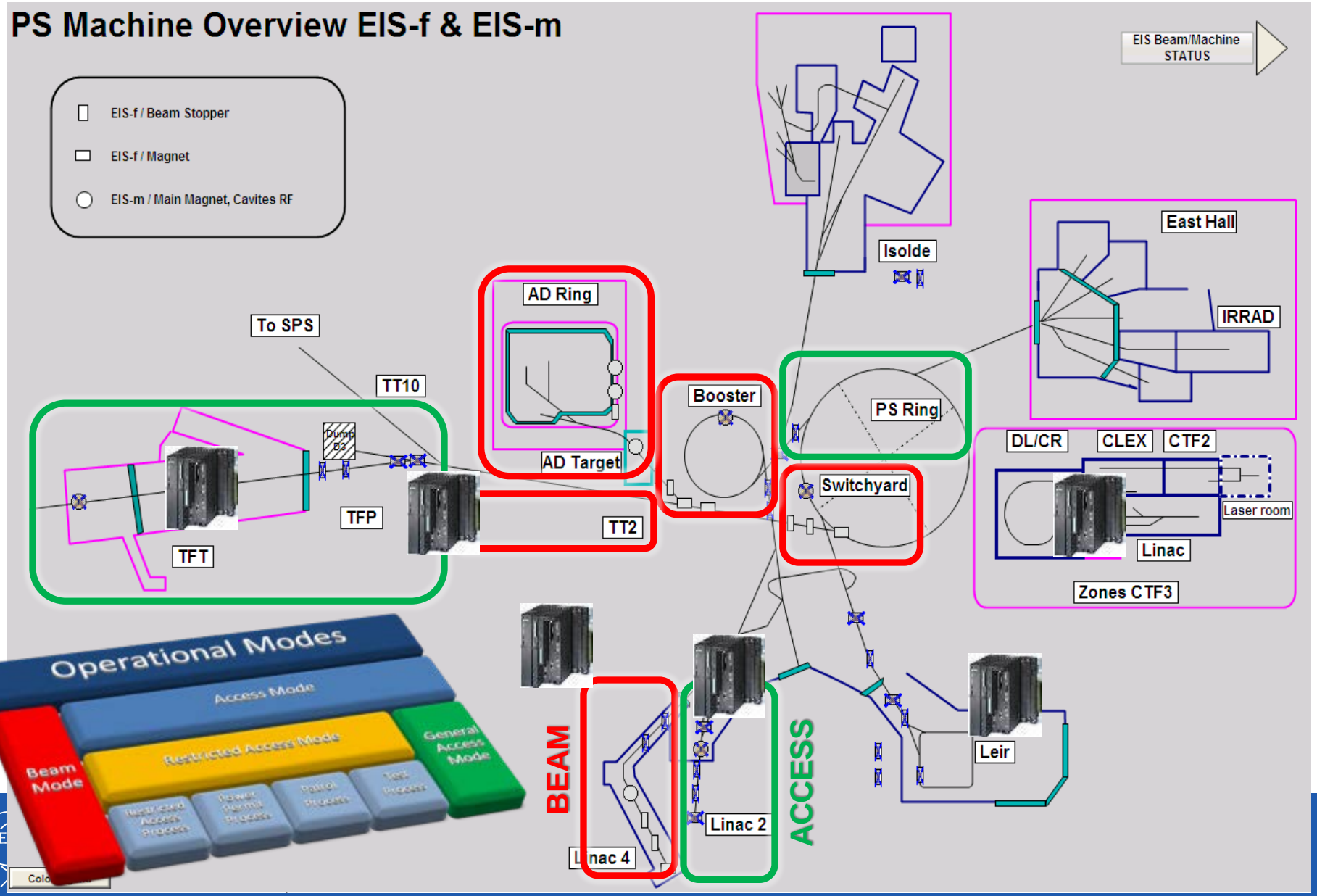
PS-PPS Project Scope



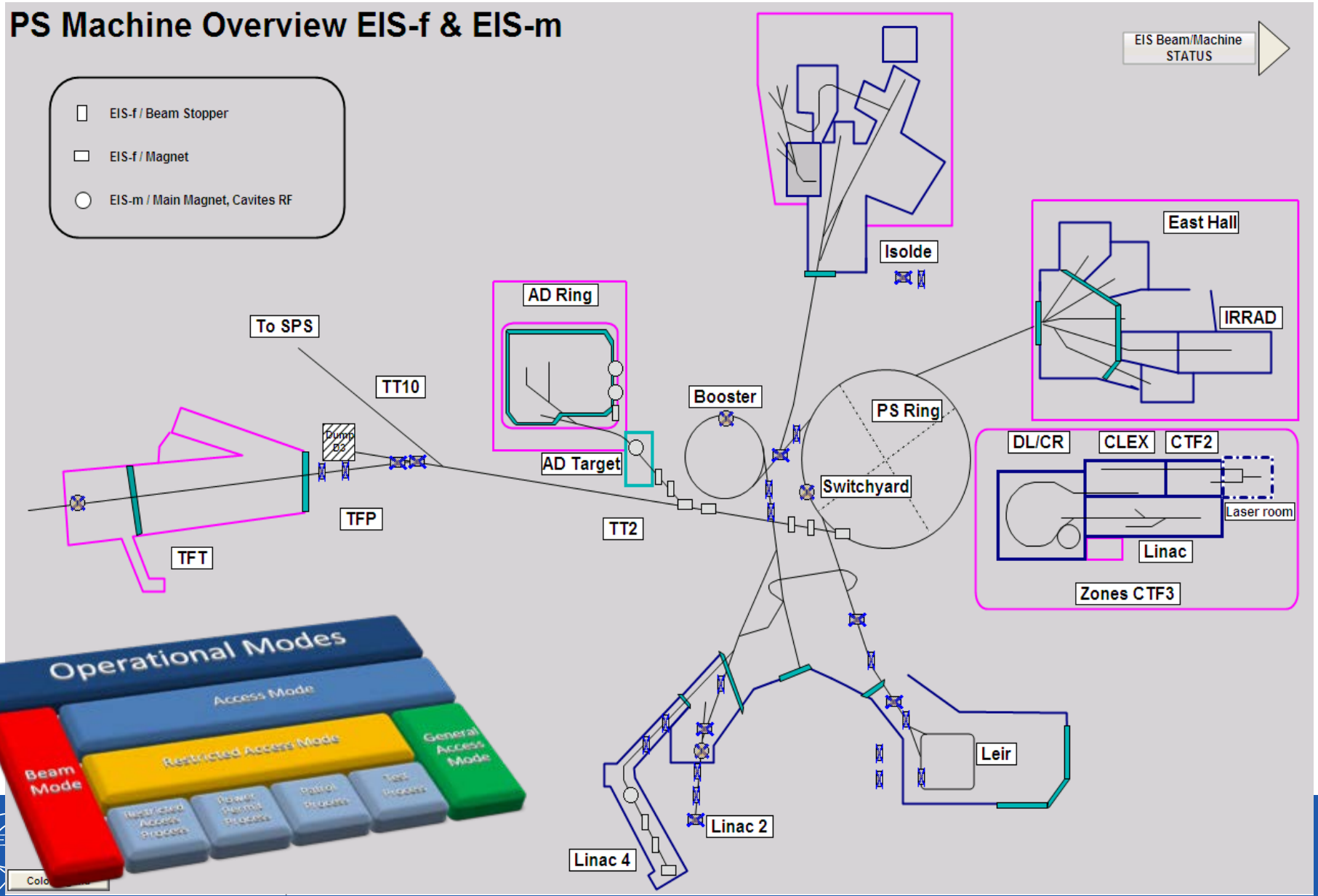
PS-PPS Project Scope



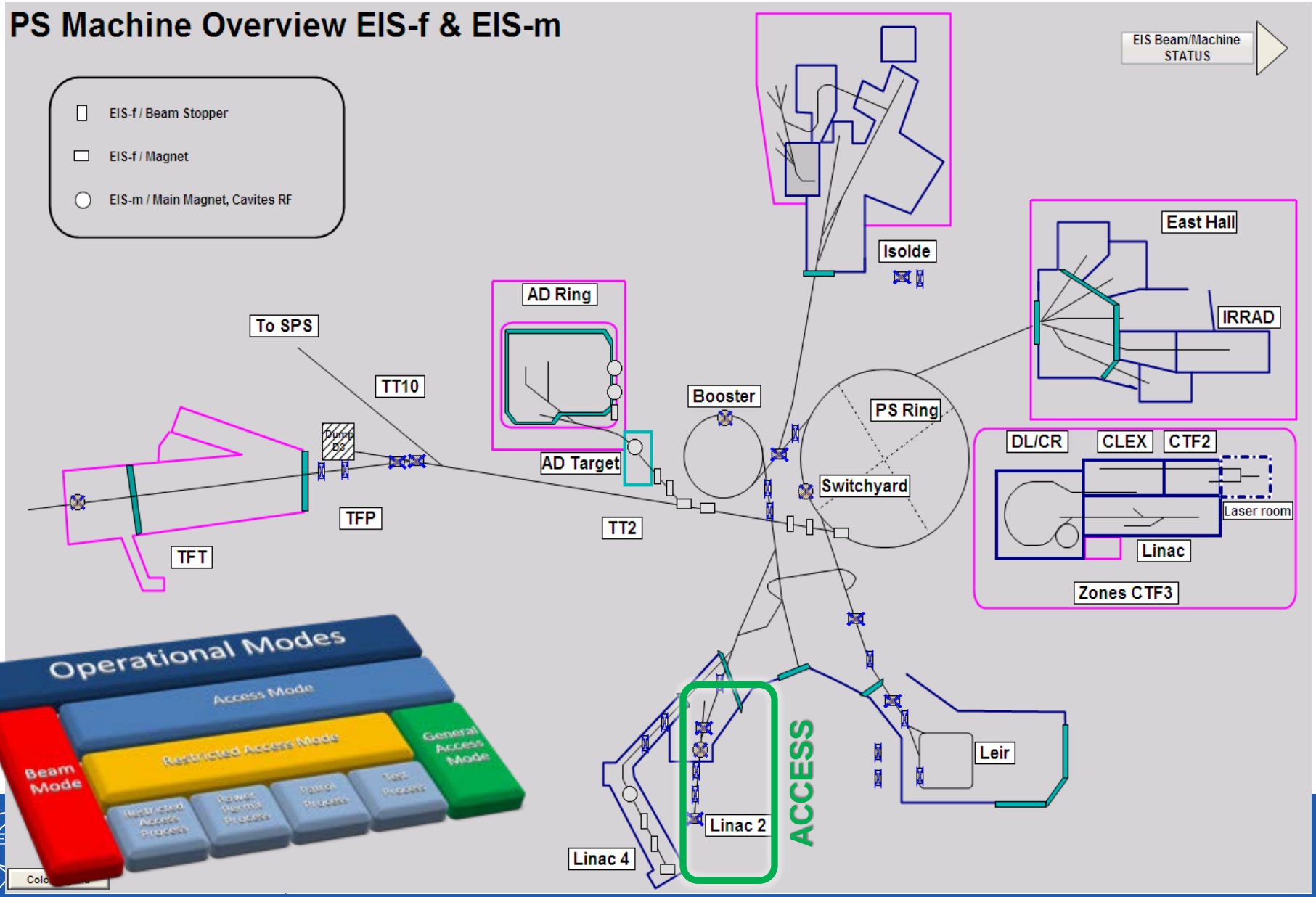
PS-PPS Project Scope



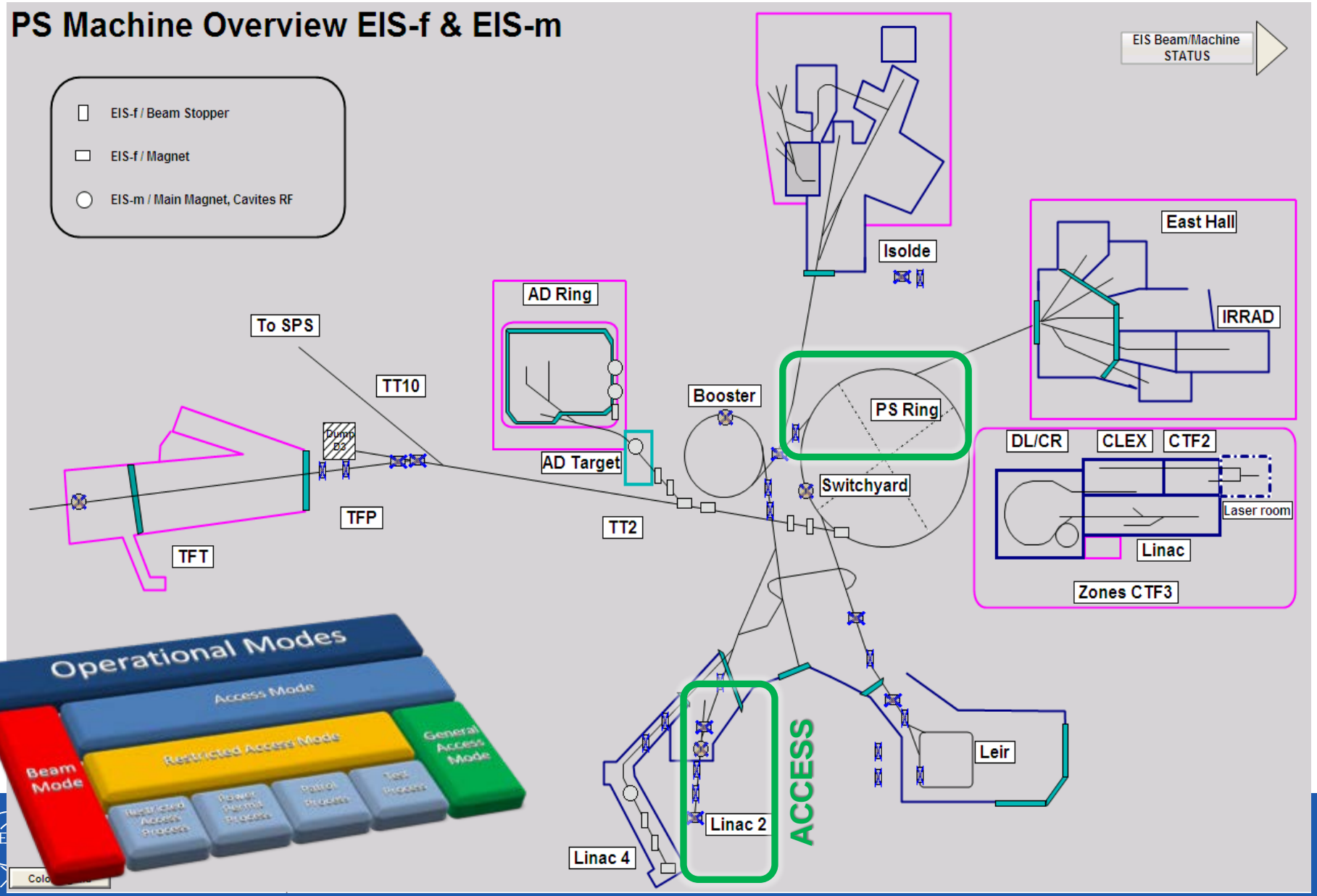
PS-PPS Project Scope



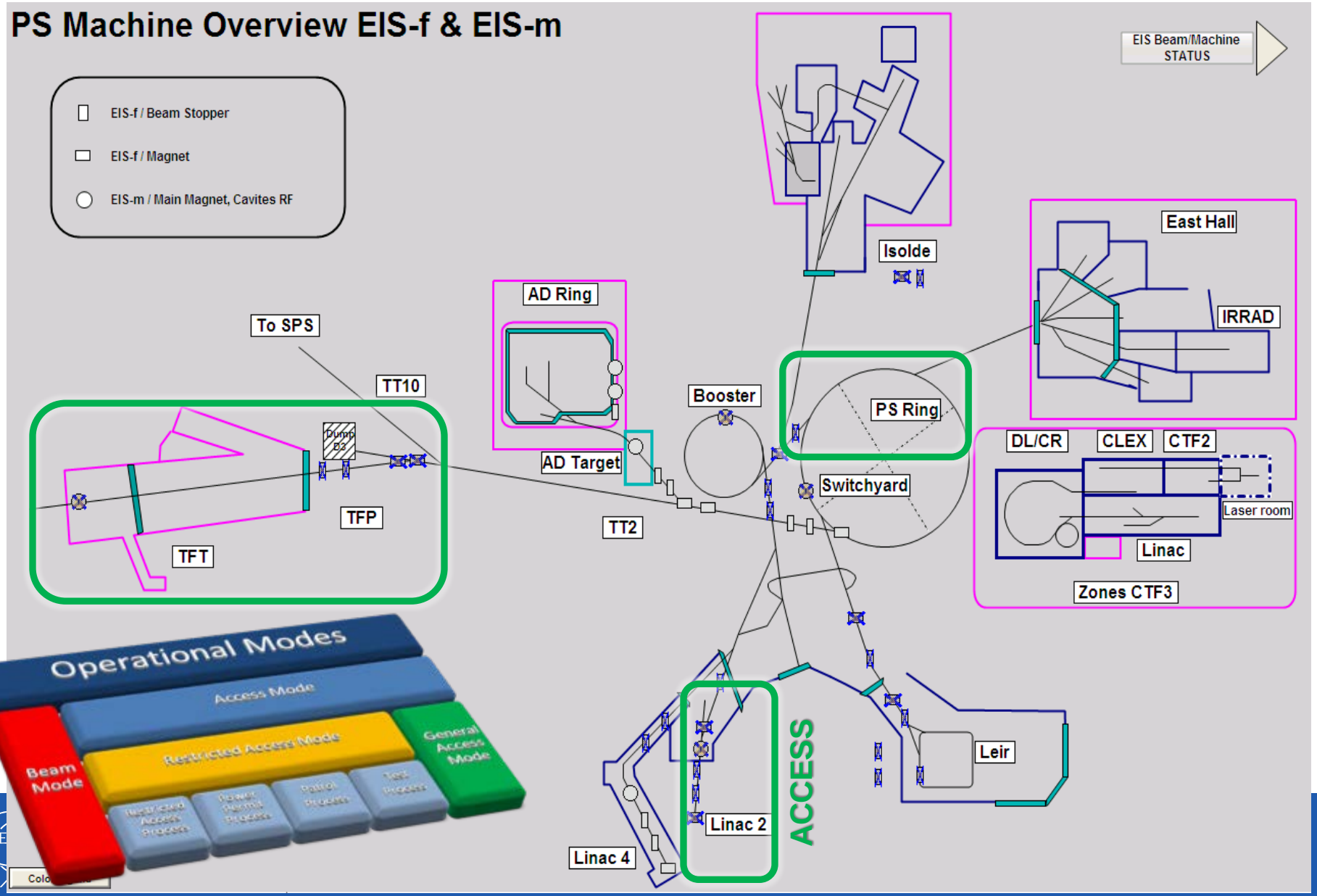
PS-PPS Project Scope



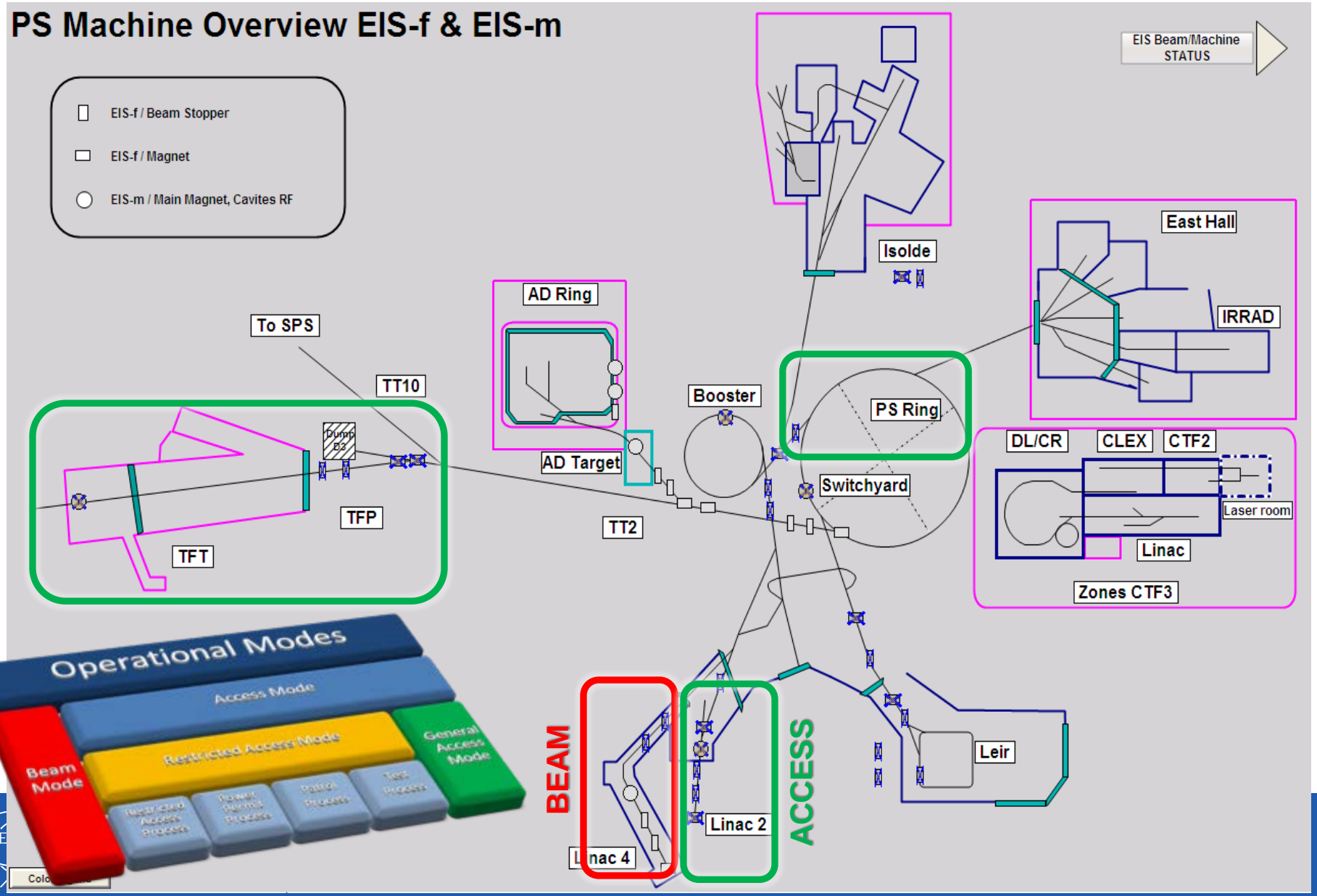
PS-PPS Project Scope



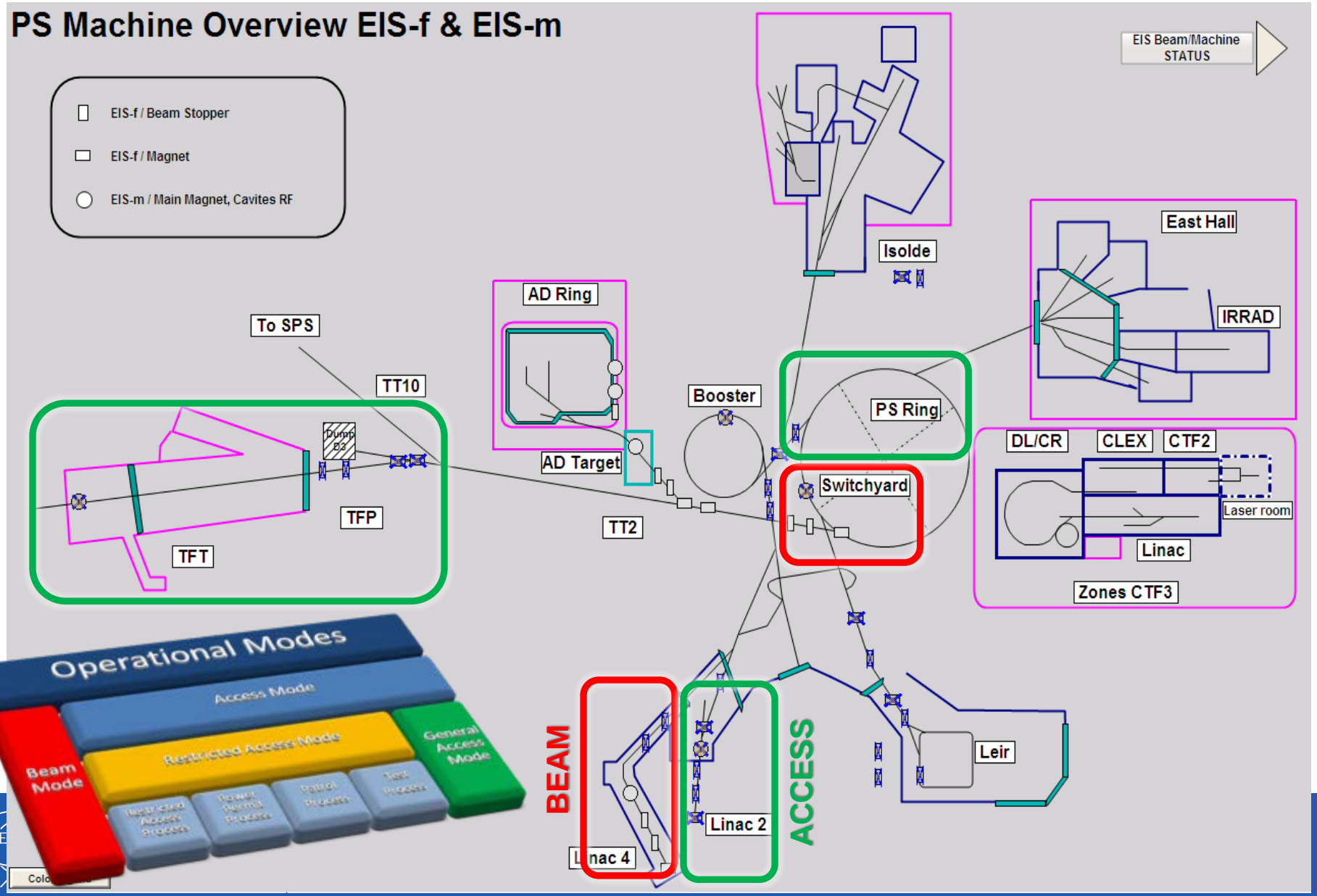
PS-PPS Project Scope



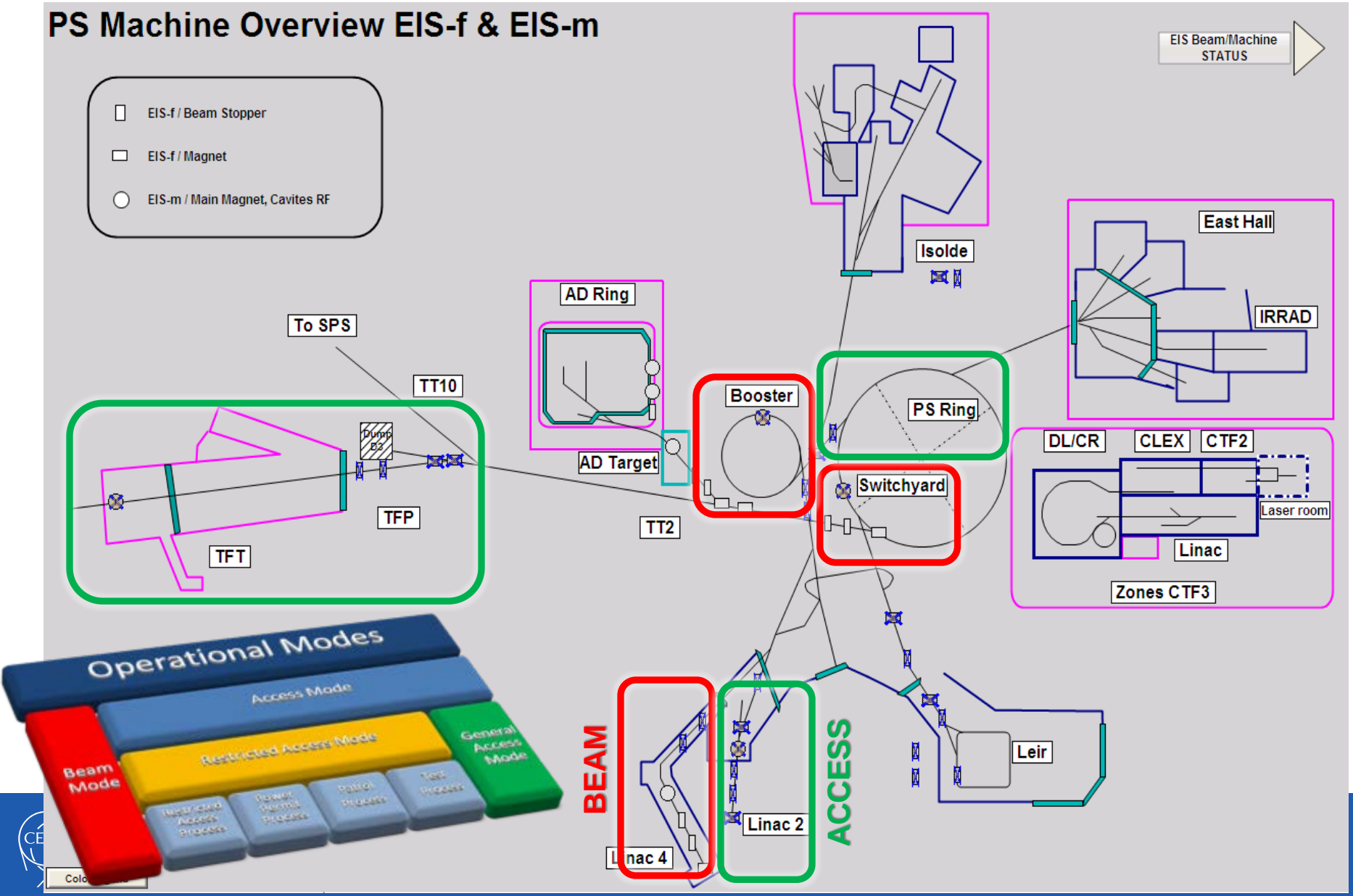
PS-PPS Project Scope



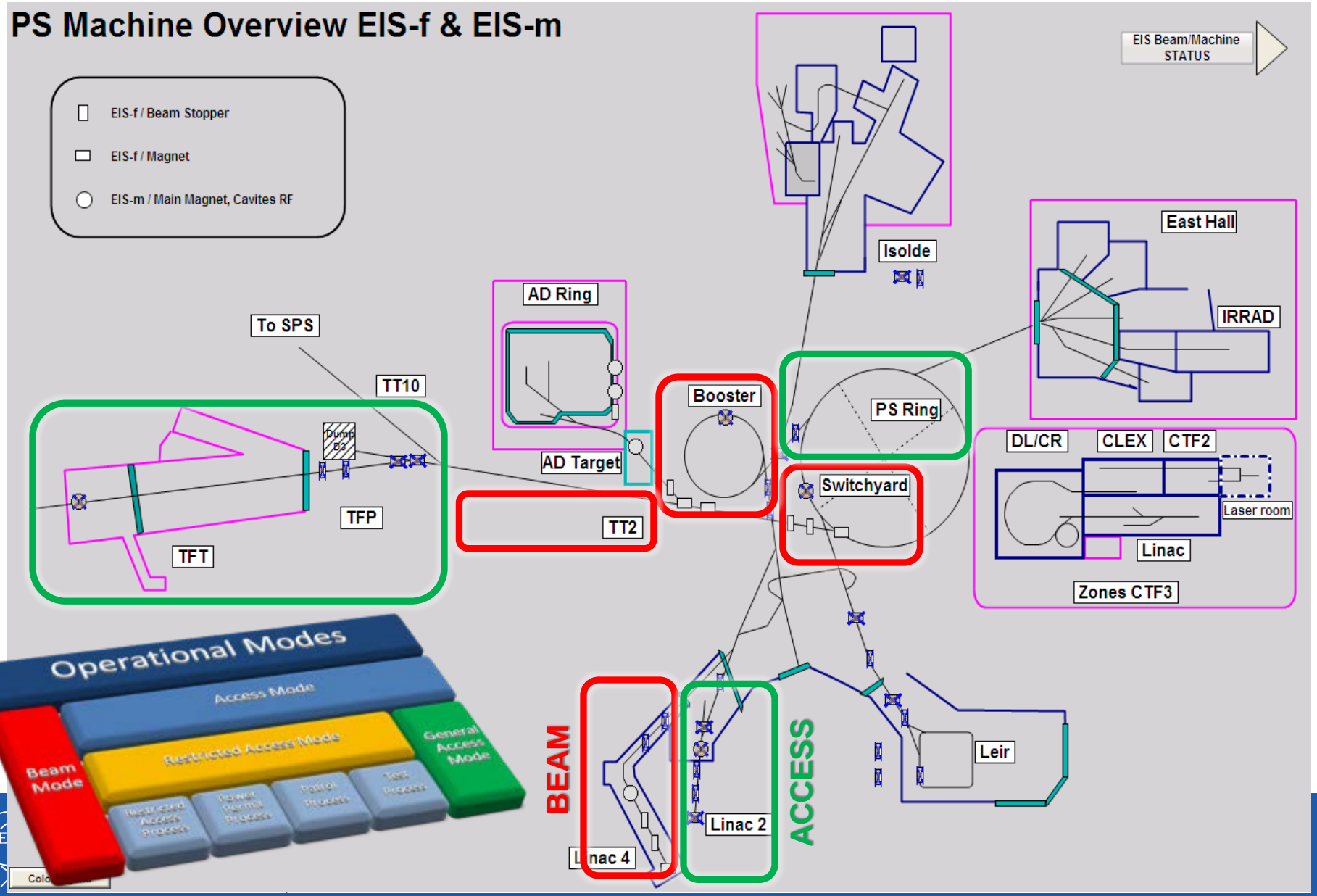
PS-PPS Project Scope



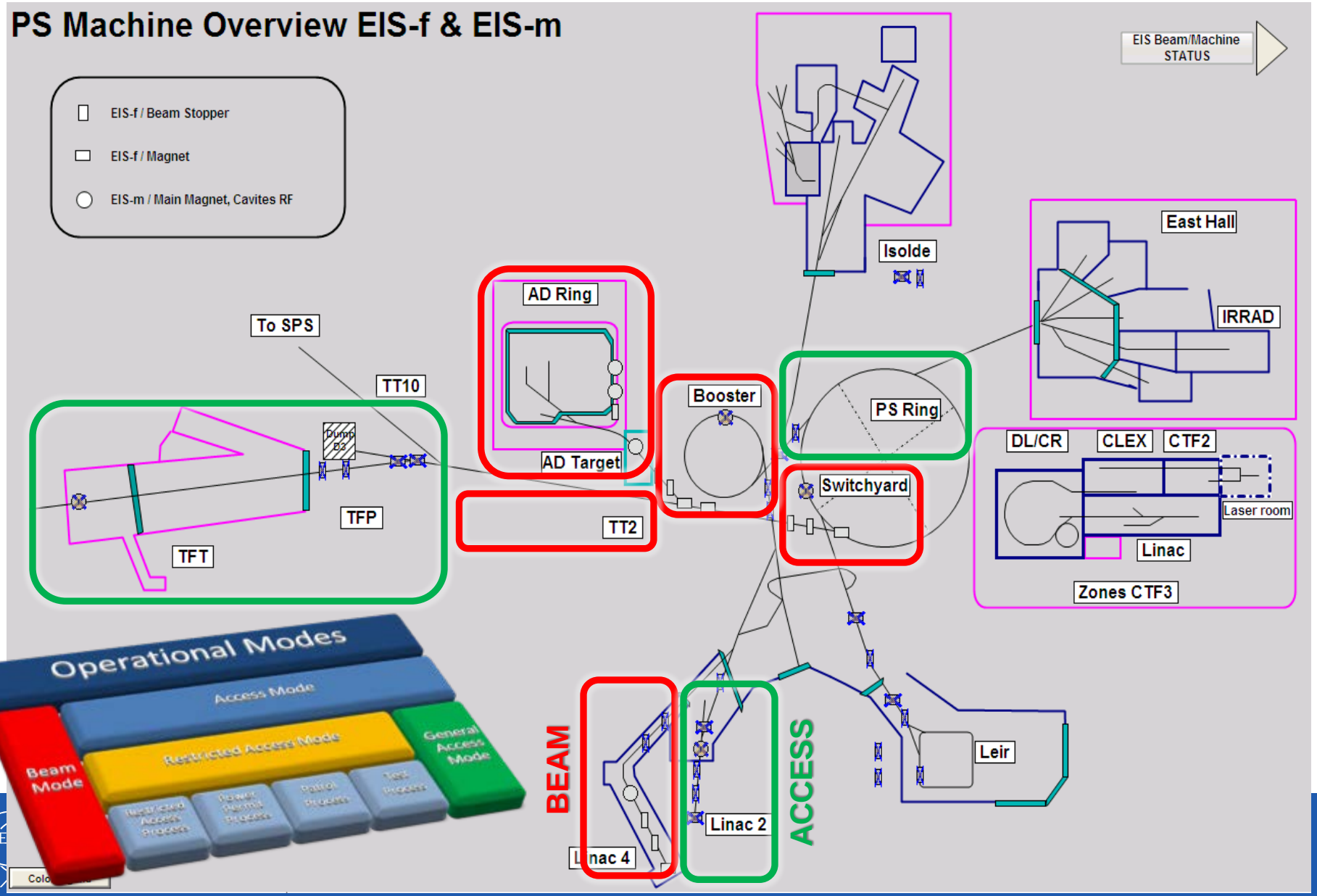
PS-PPS Project Scope



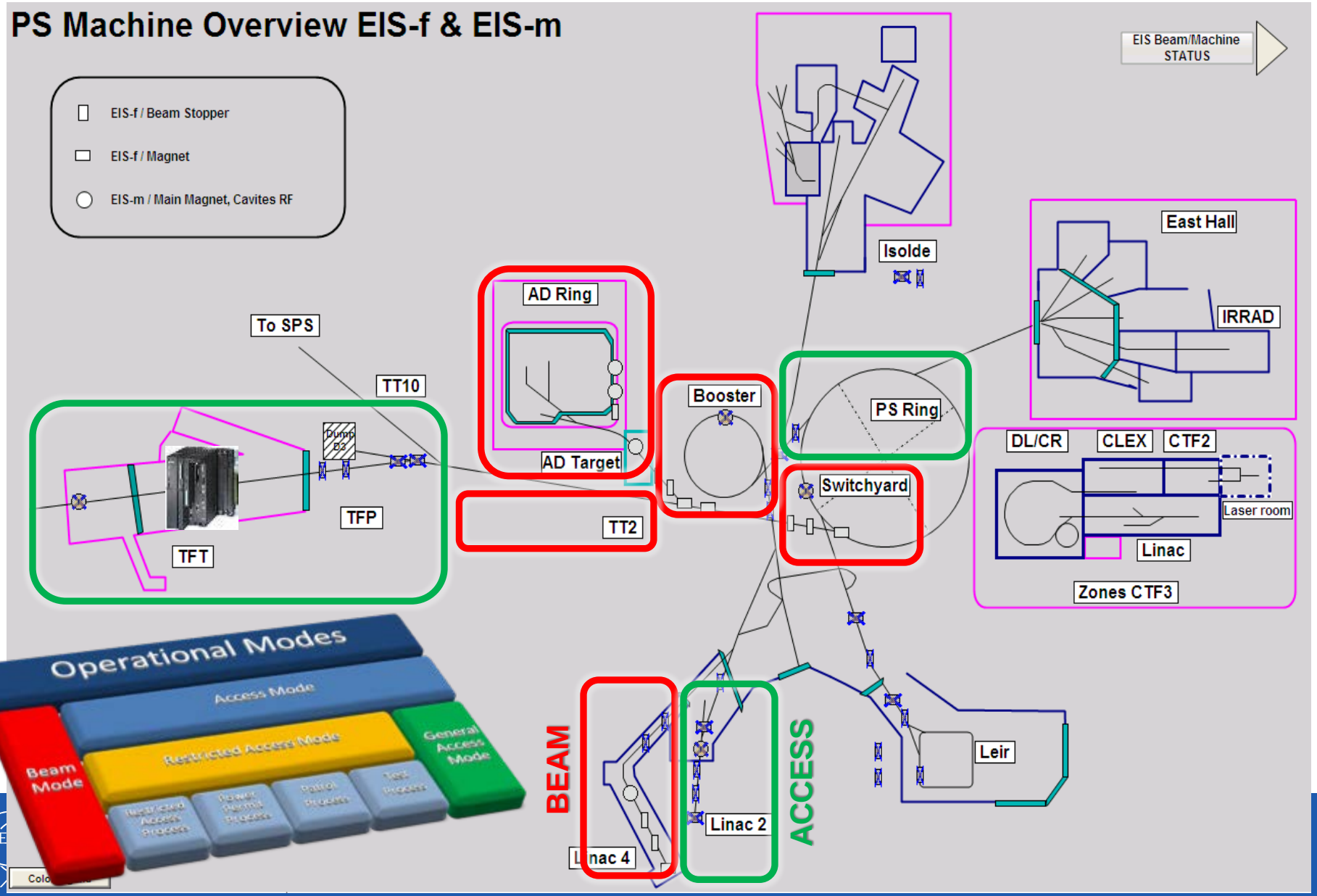
PS-PPS Project Scope



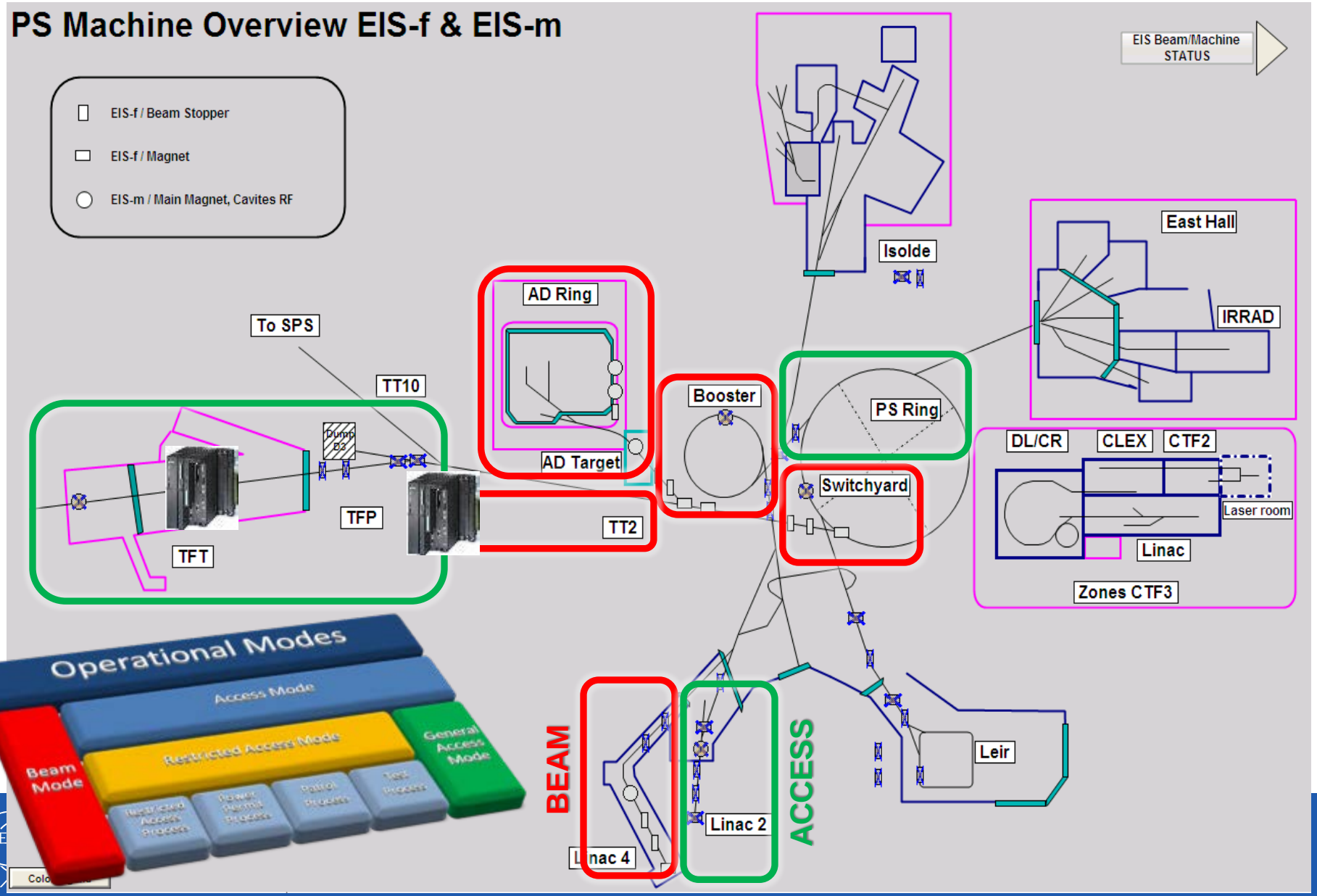
PS-PPS Project Scope



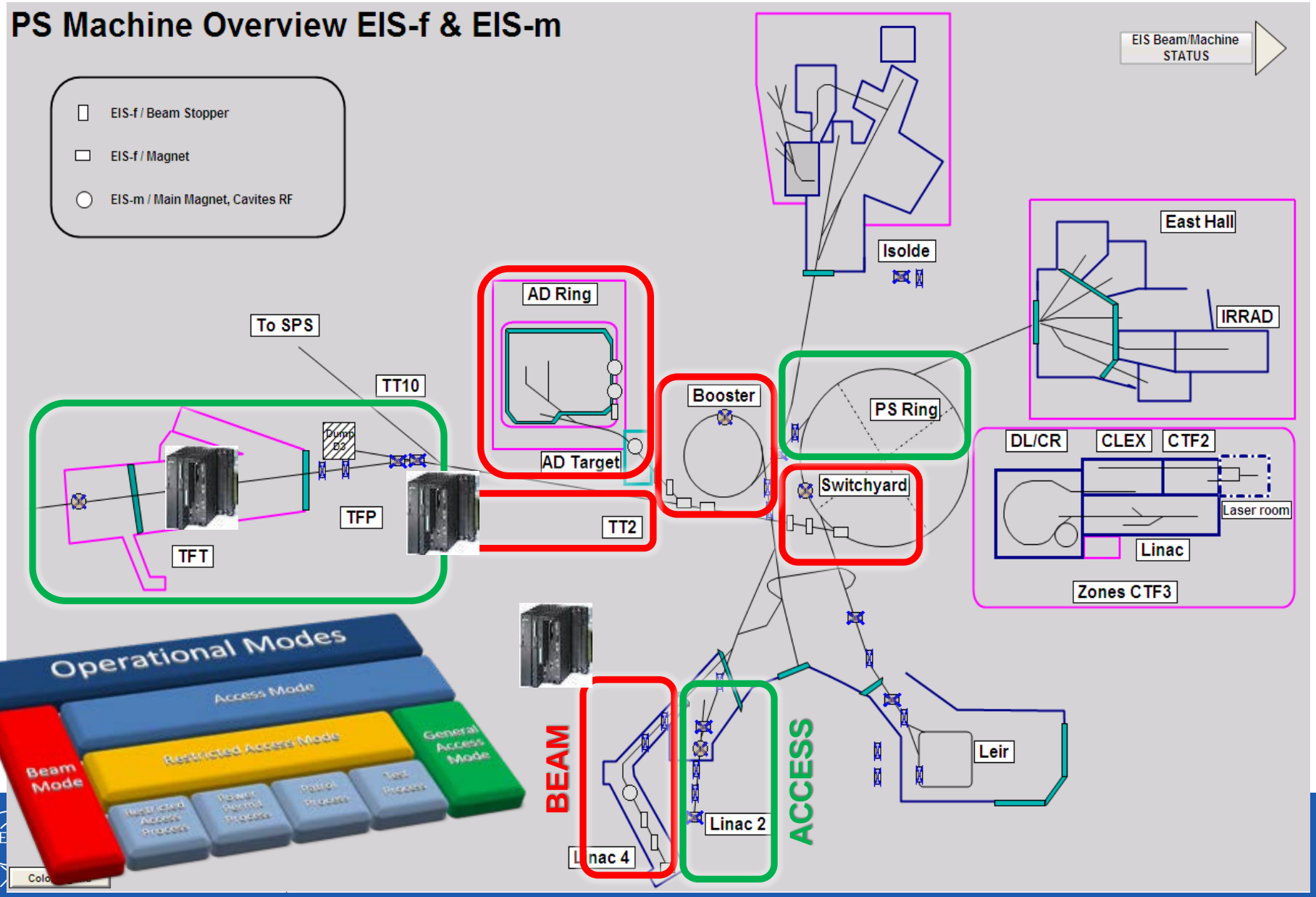
PS-PPS Project Scope



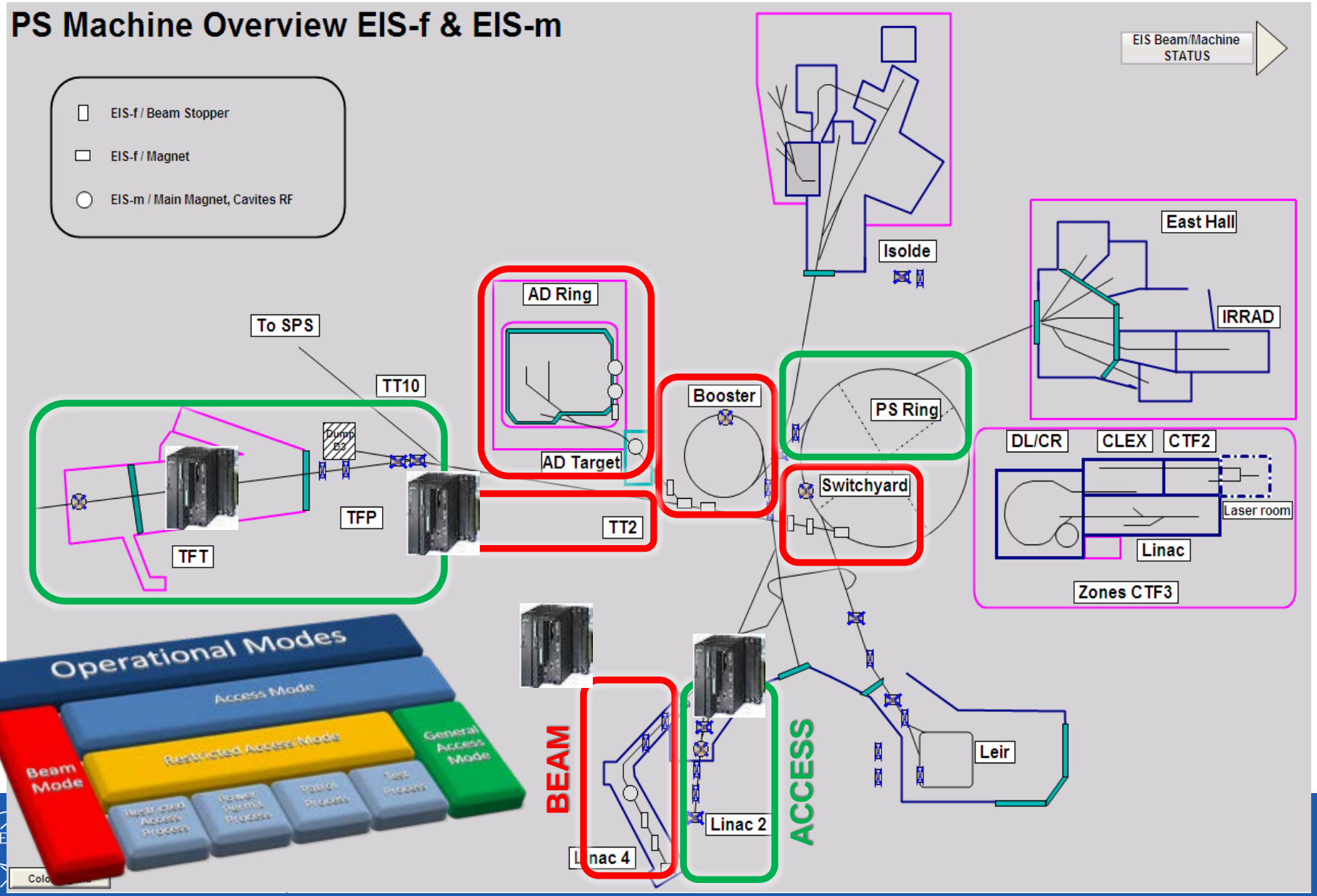
PS-PPS Project Scope



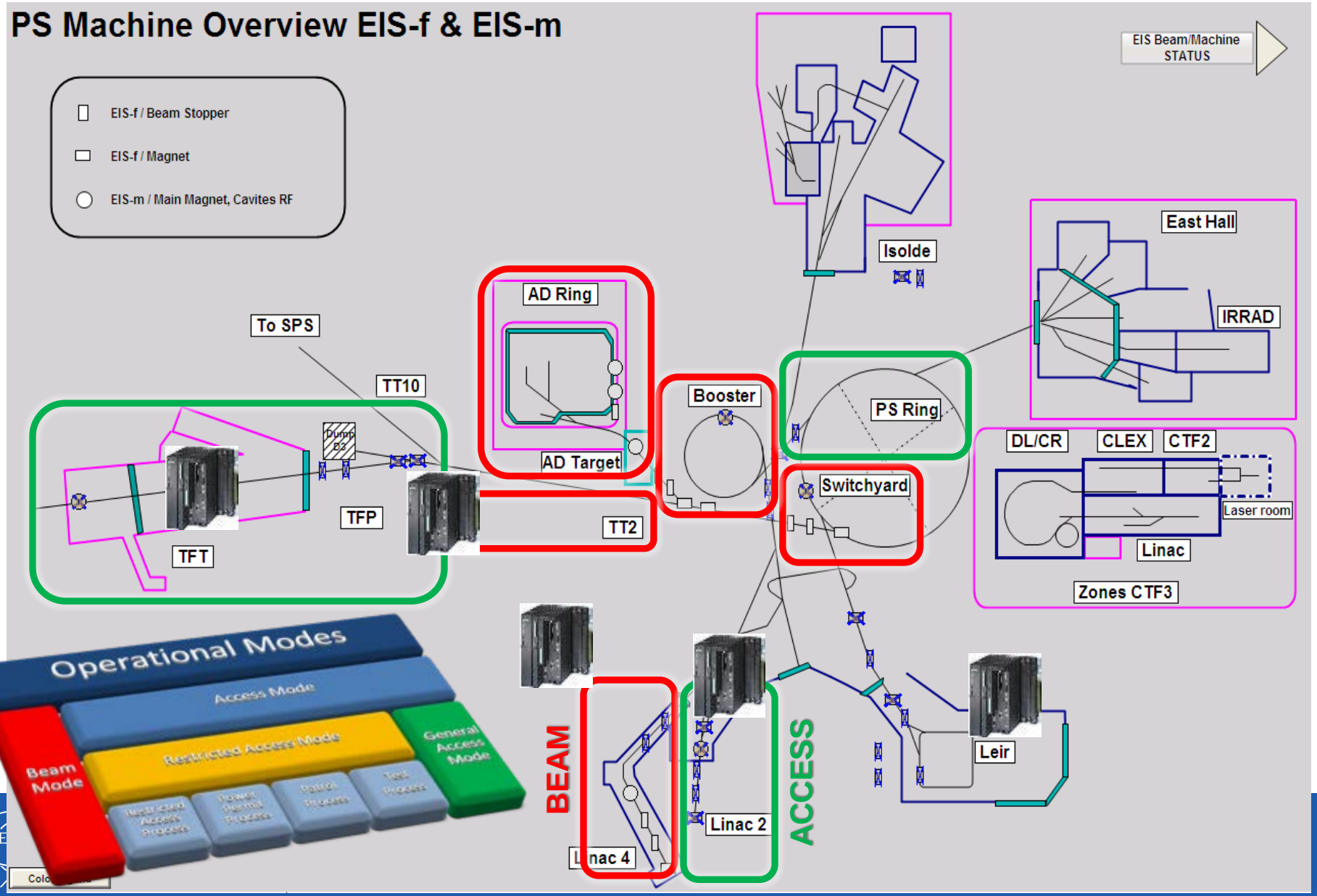
PS-PPS Project Scope



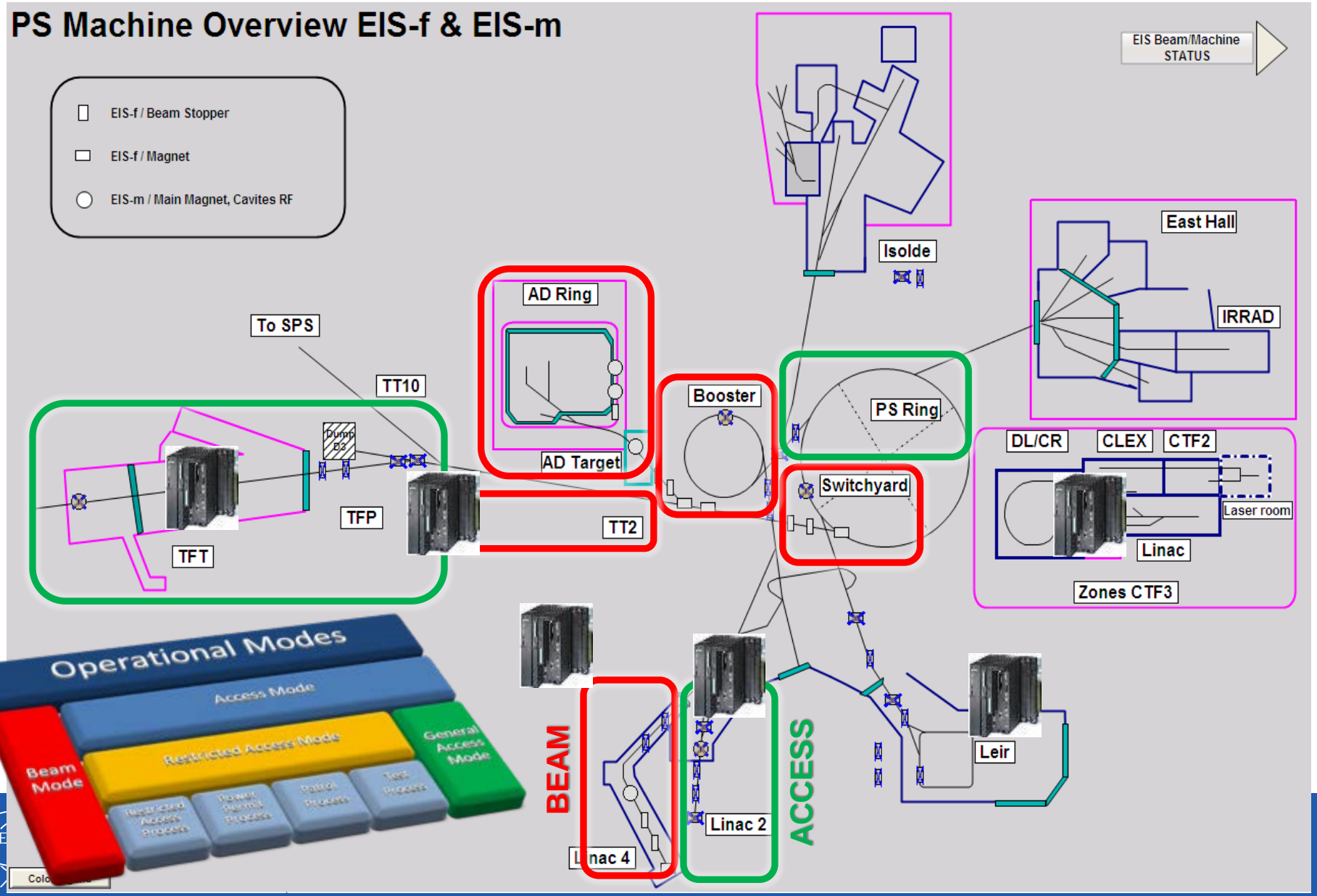
PS-PPS Project Scope



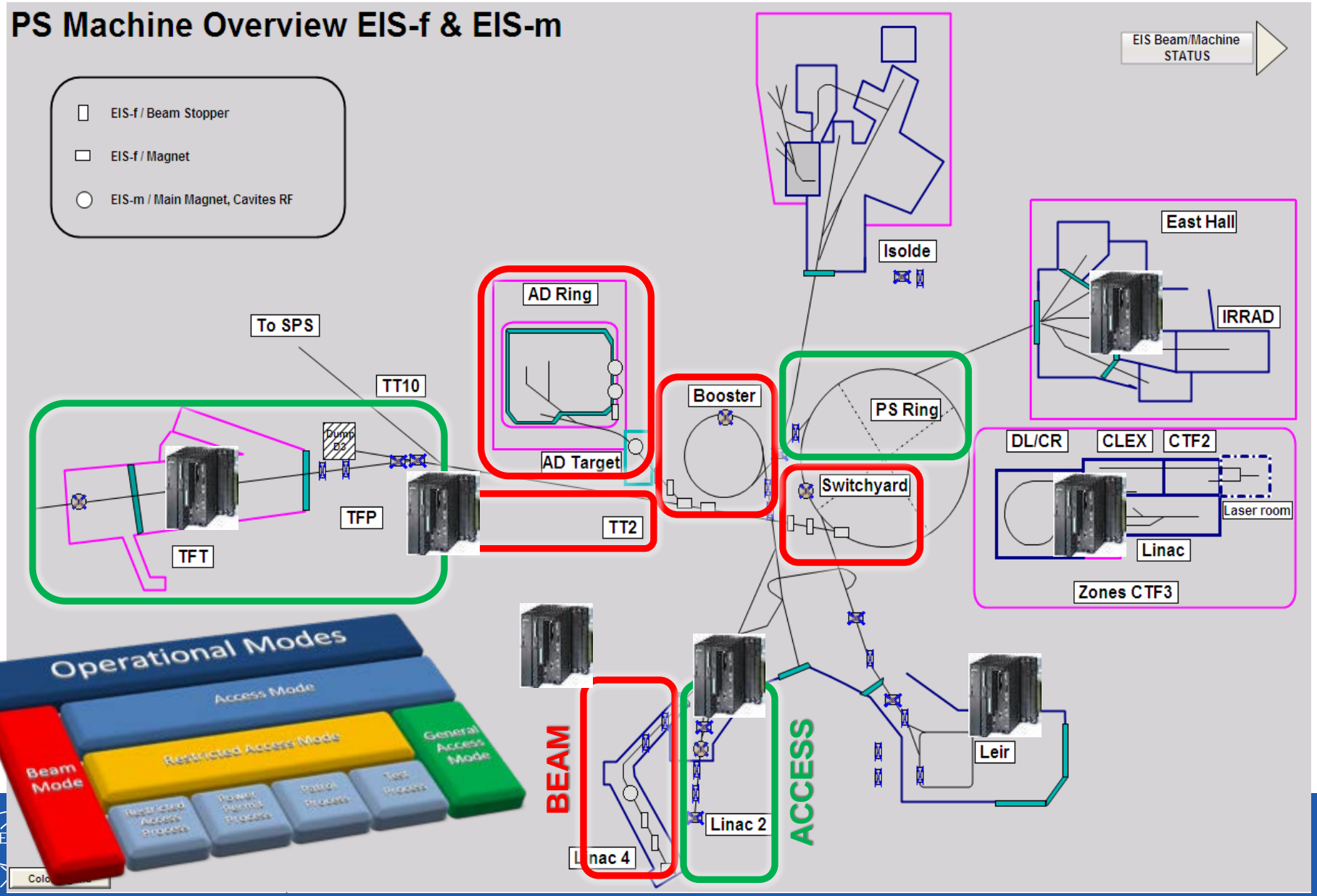
PS-PPS Project Scope



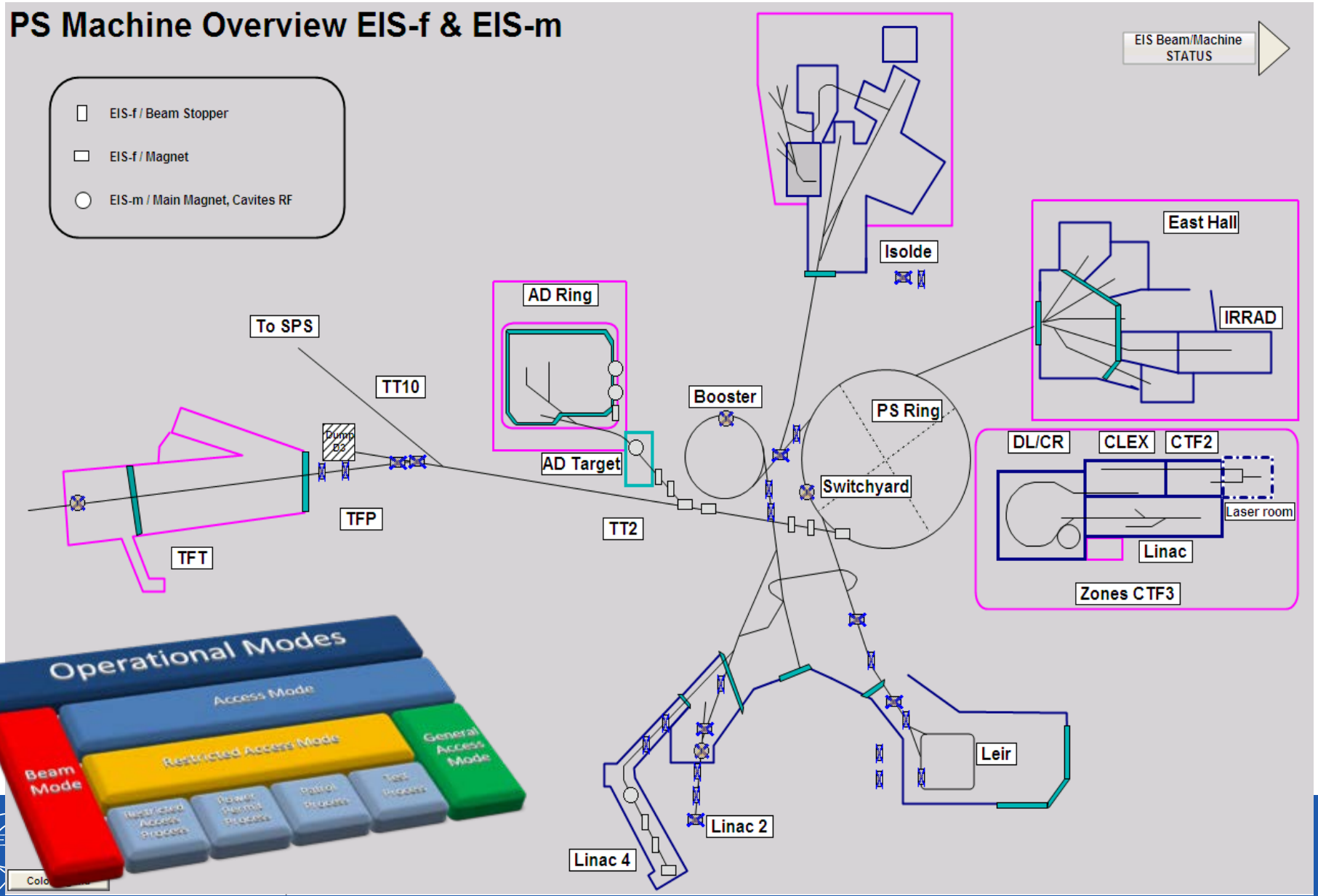
PS-PPS Project Scope



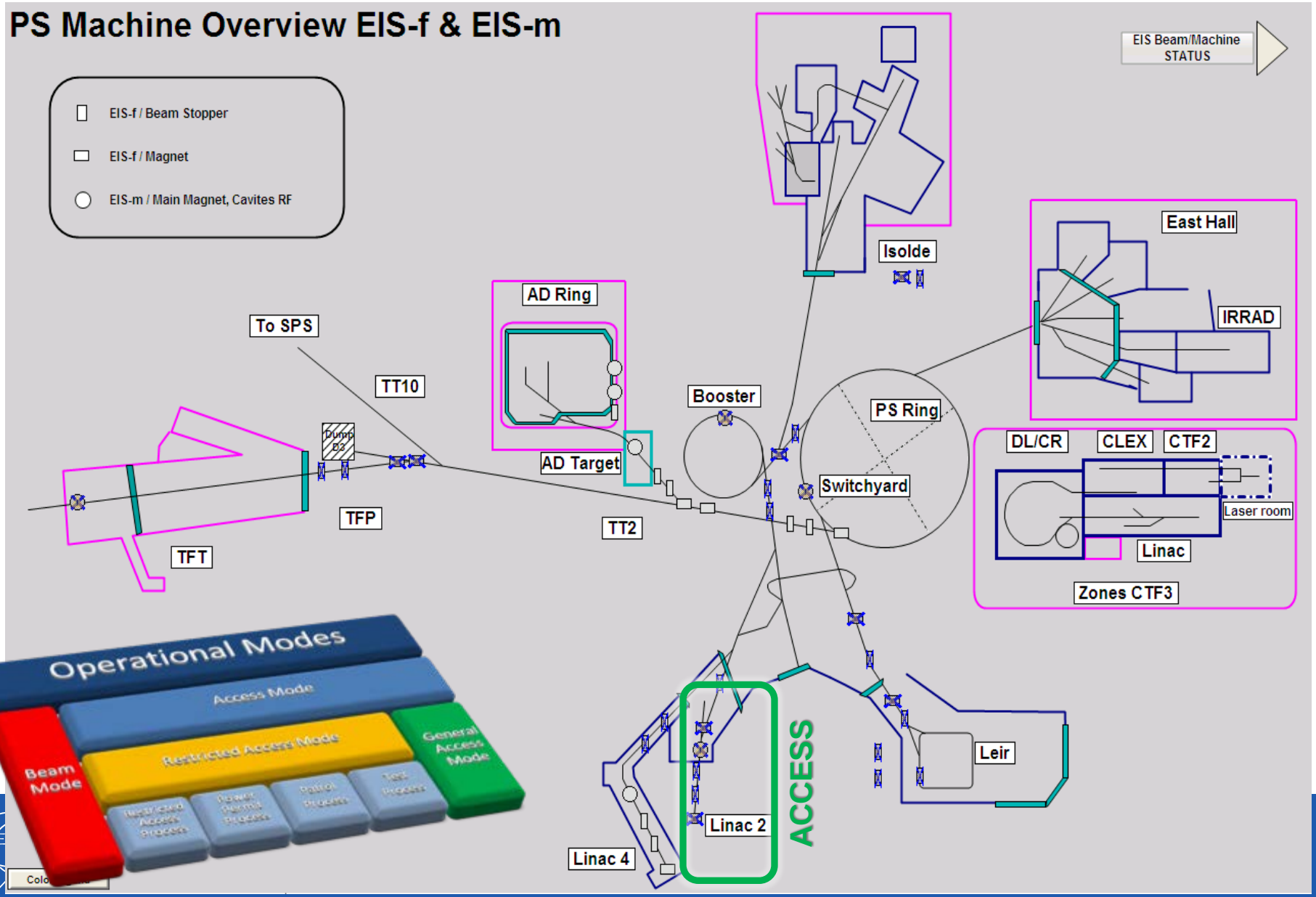
PS-PPS Project Scope



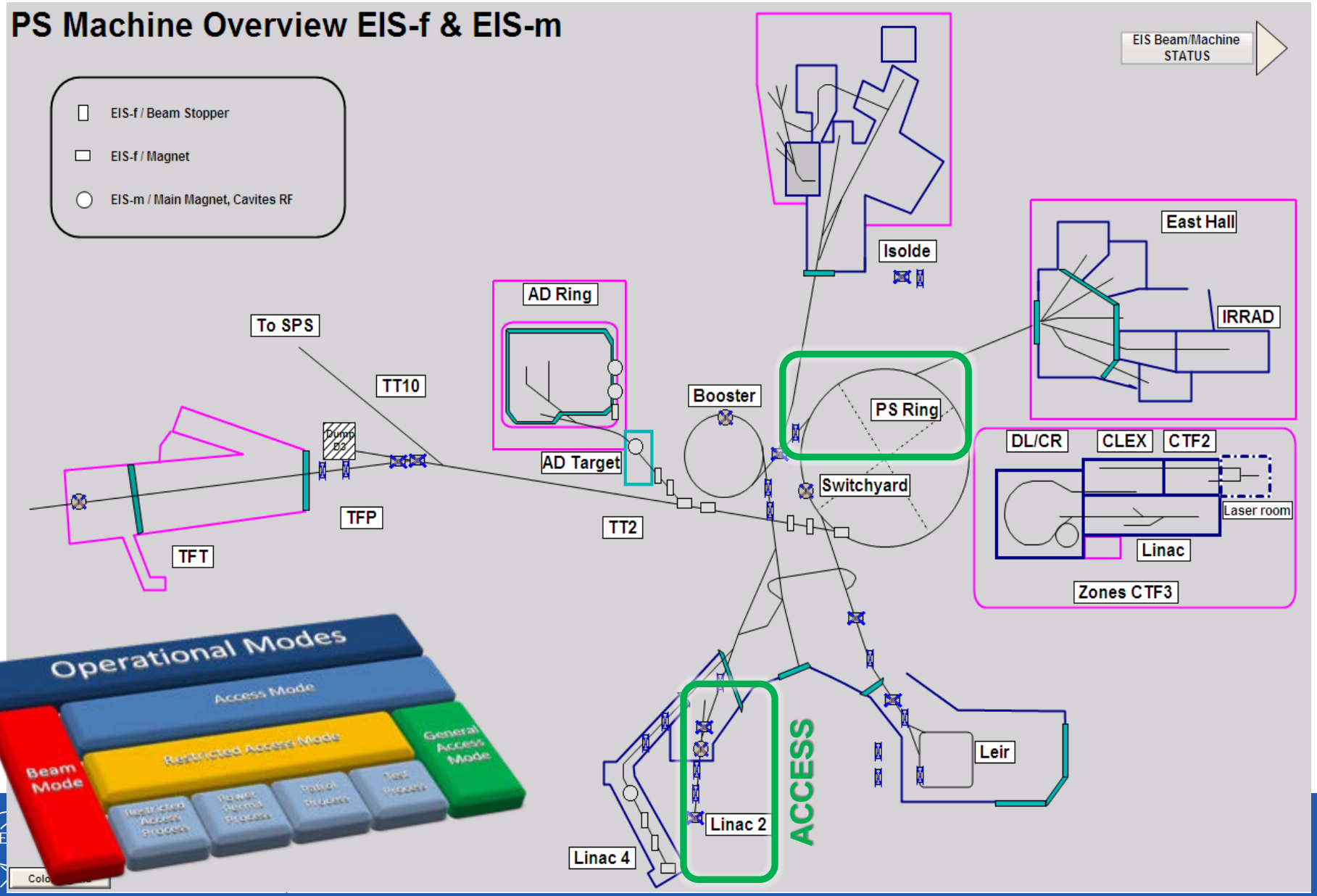
PS-PPS Project Scope



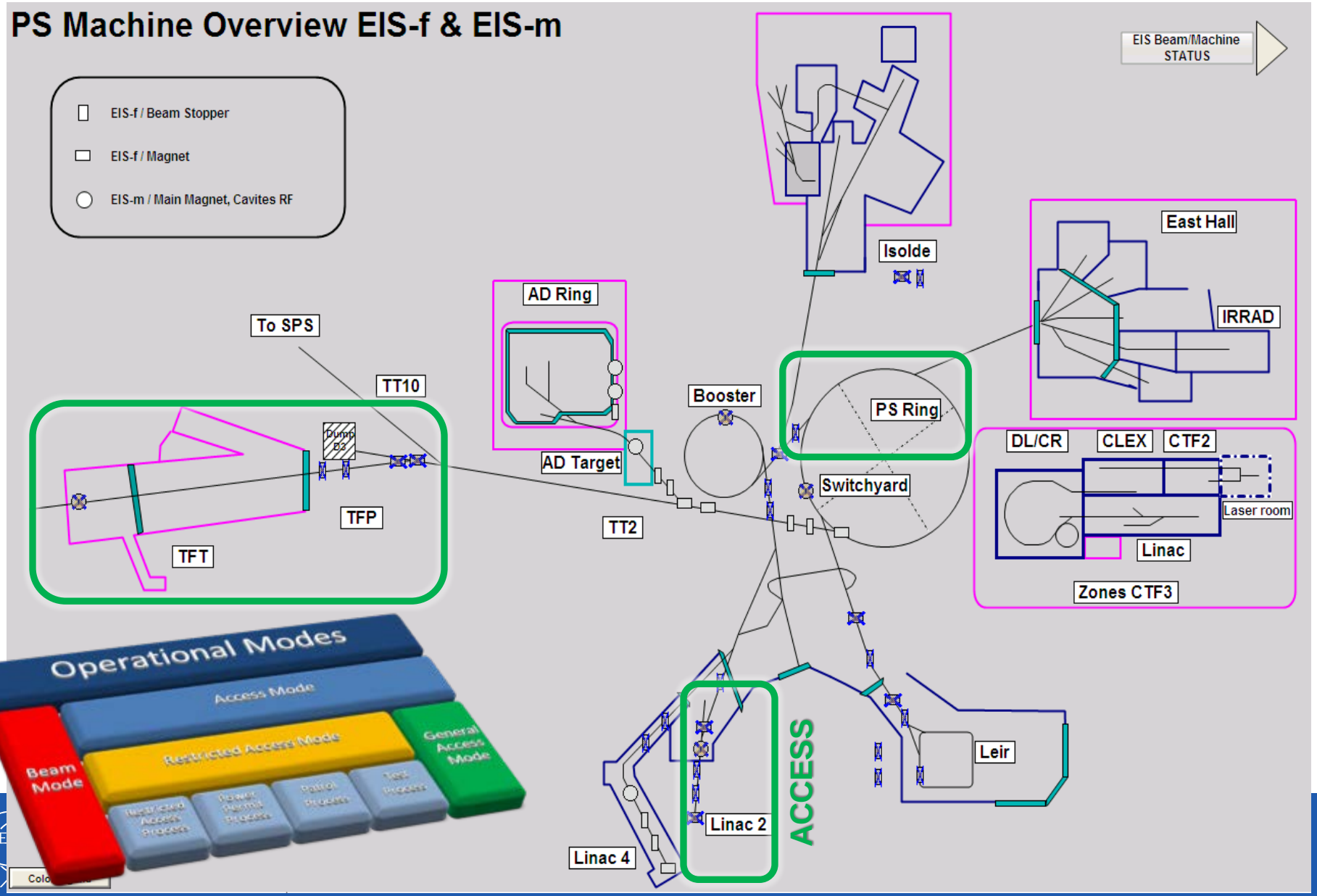
PS-PPS Project Scope



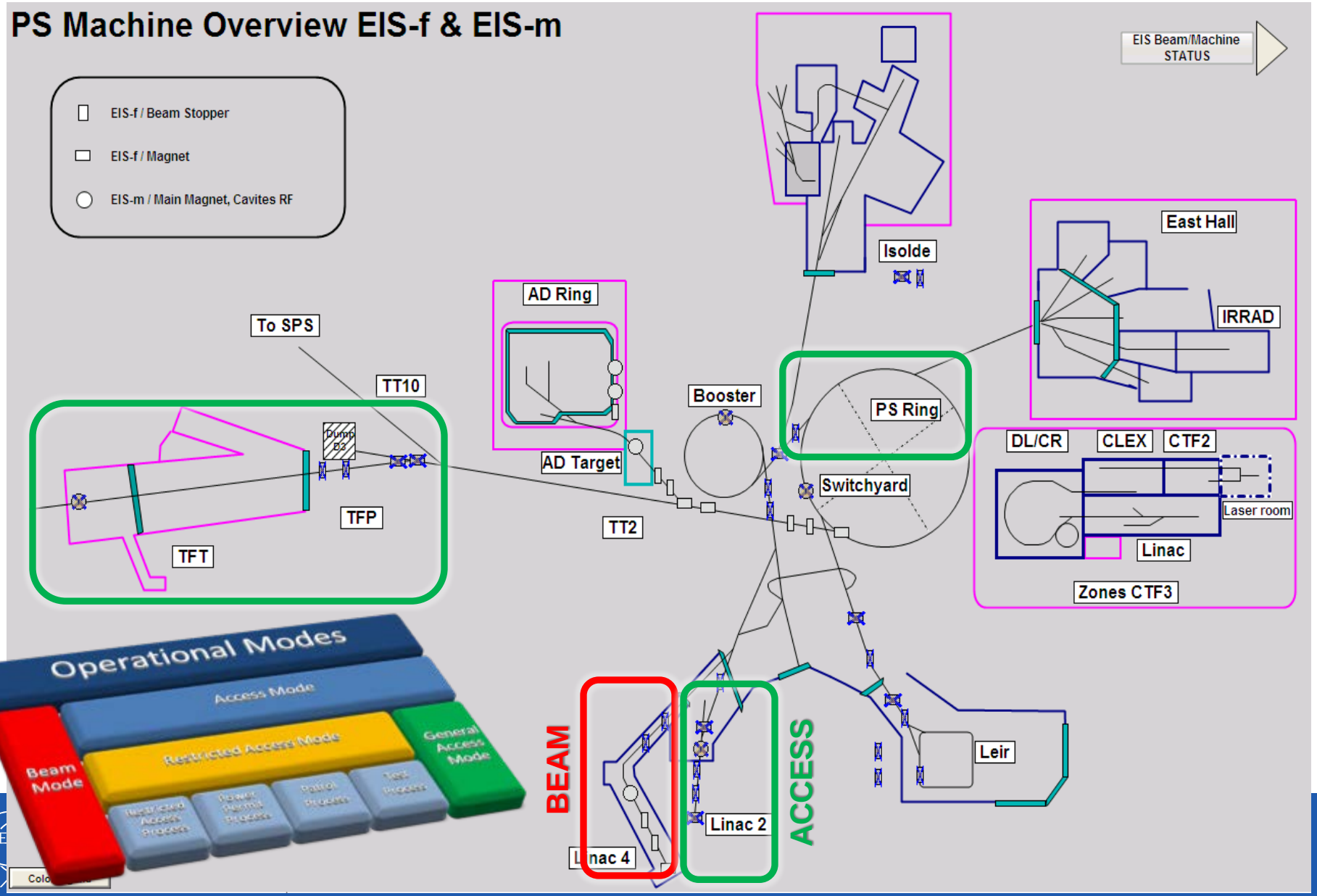
PS-PPS Project Scope



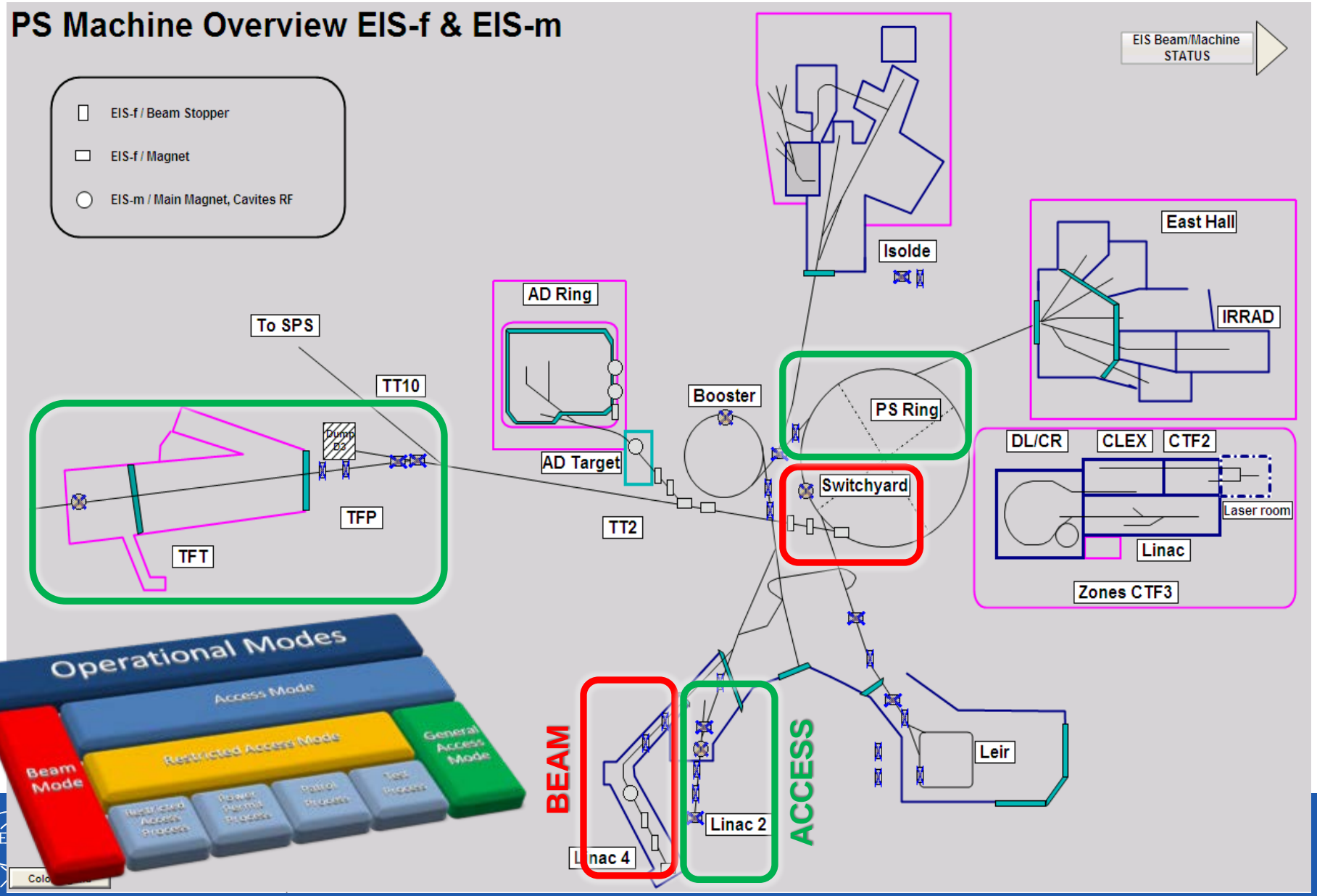
PS-PPS Project Scope



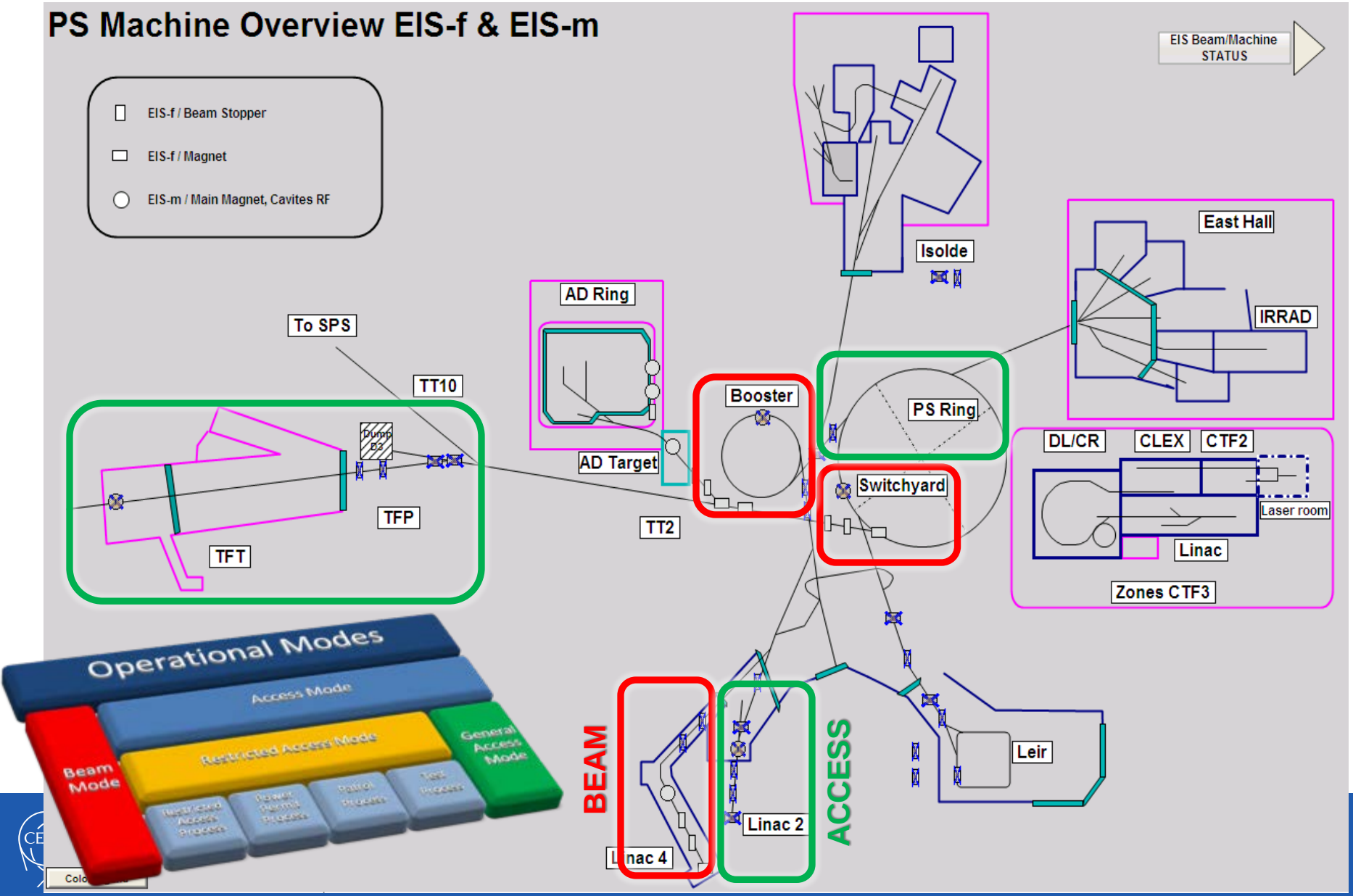
PS-PPS Project Scope



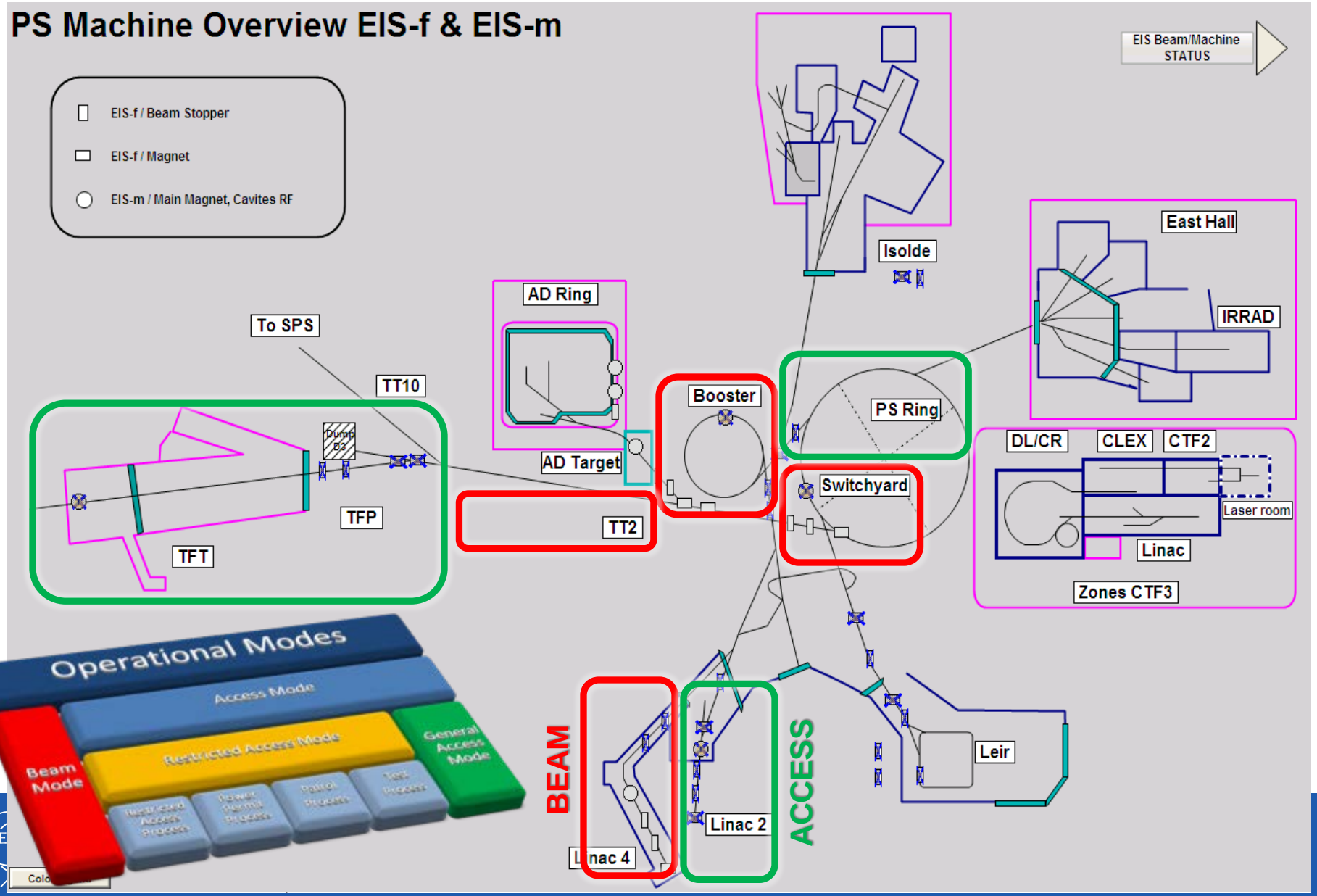
PS-PPS Project Scope



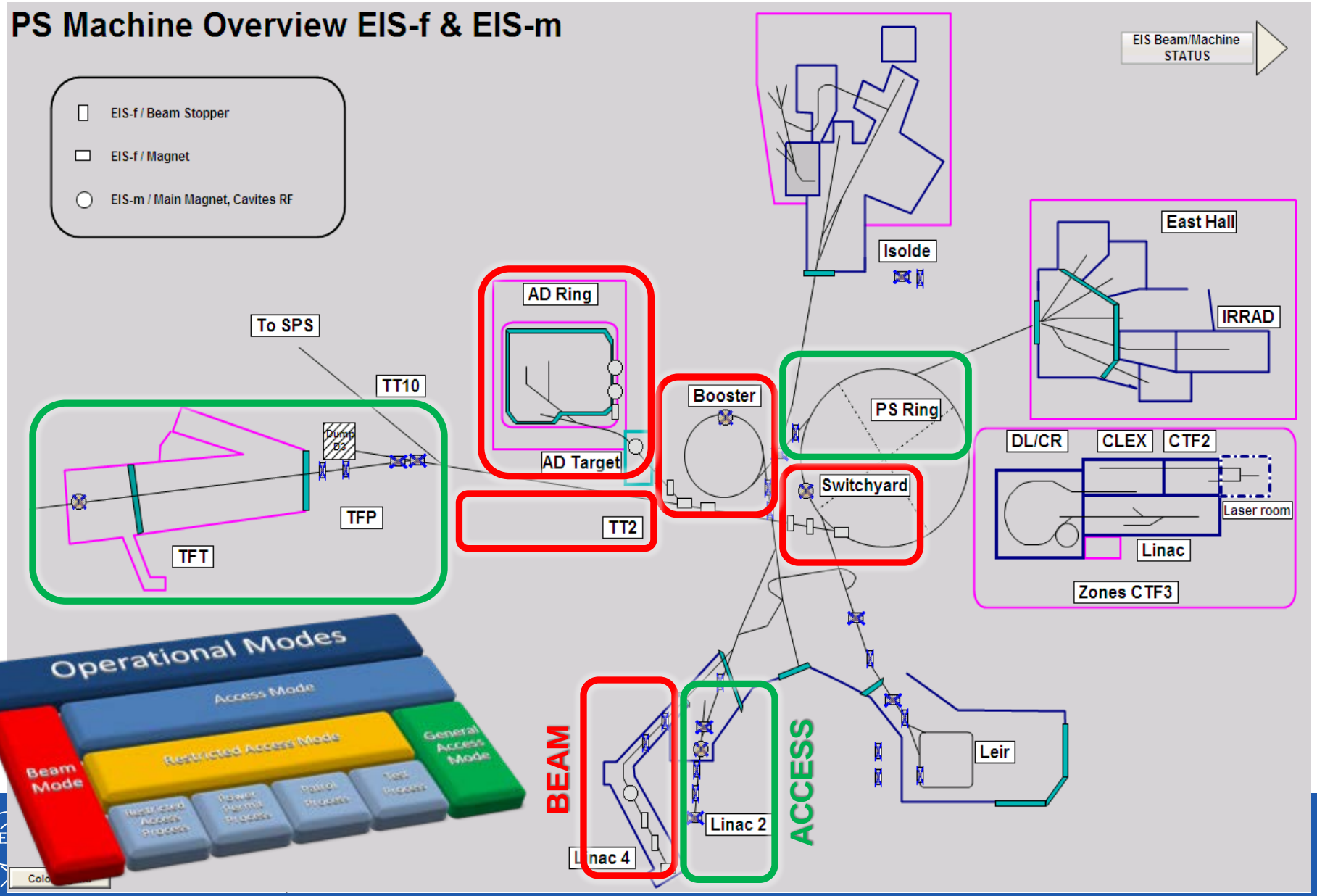
PS-PPS Project Scope



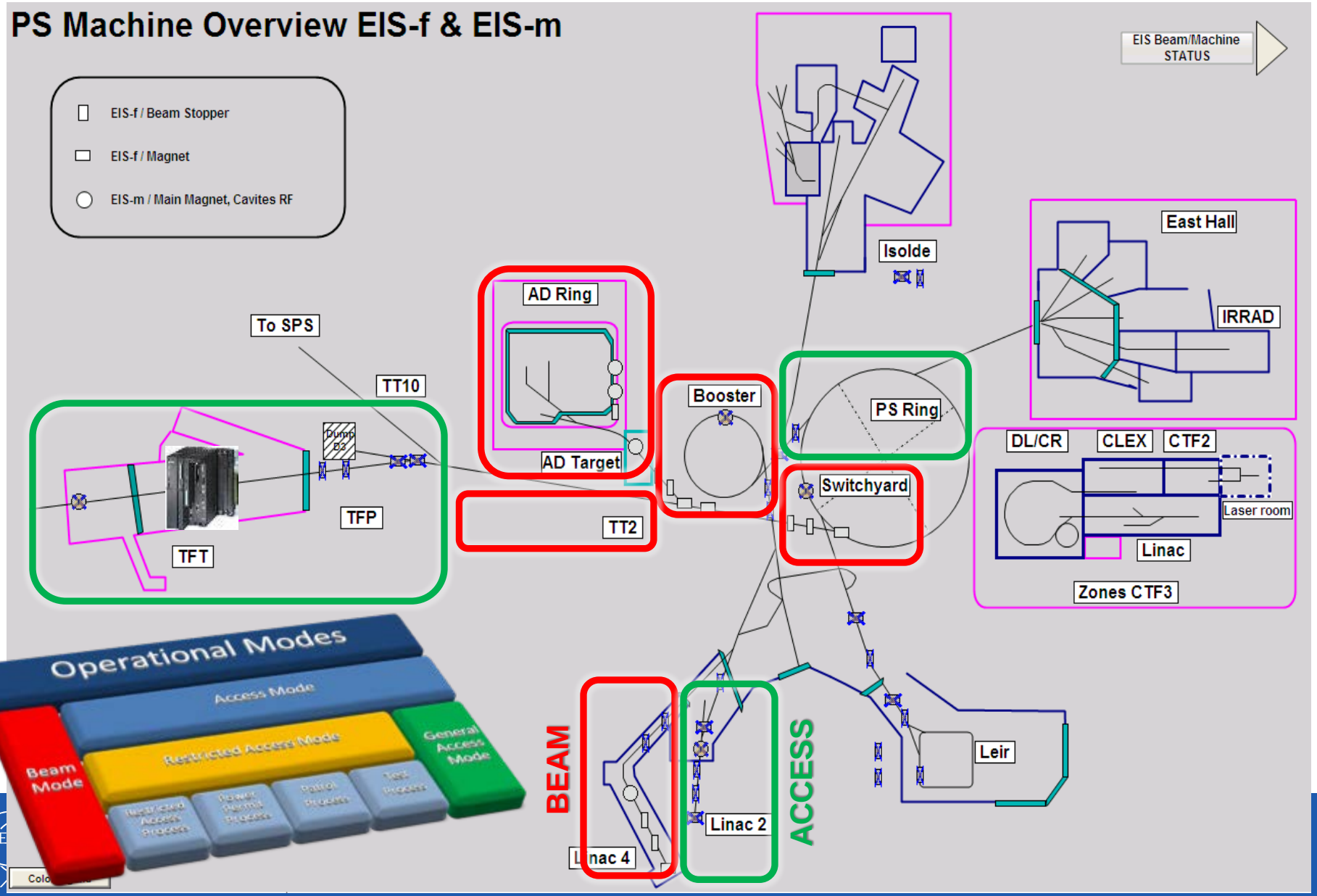
PS-PPS Project Scope



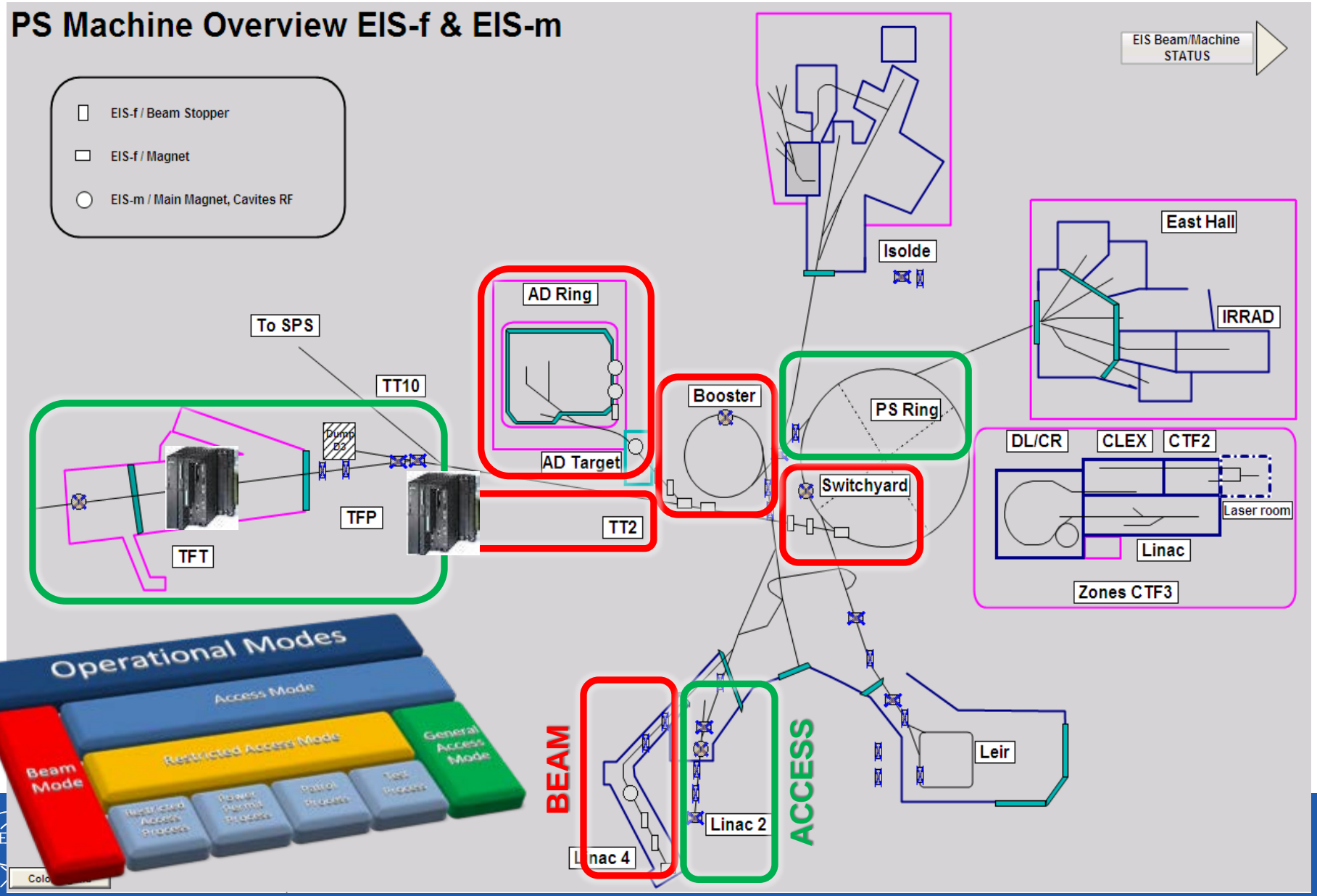
PS-PPS Project Scope



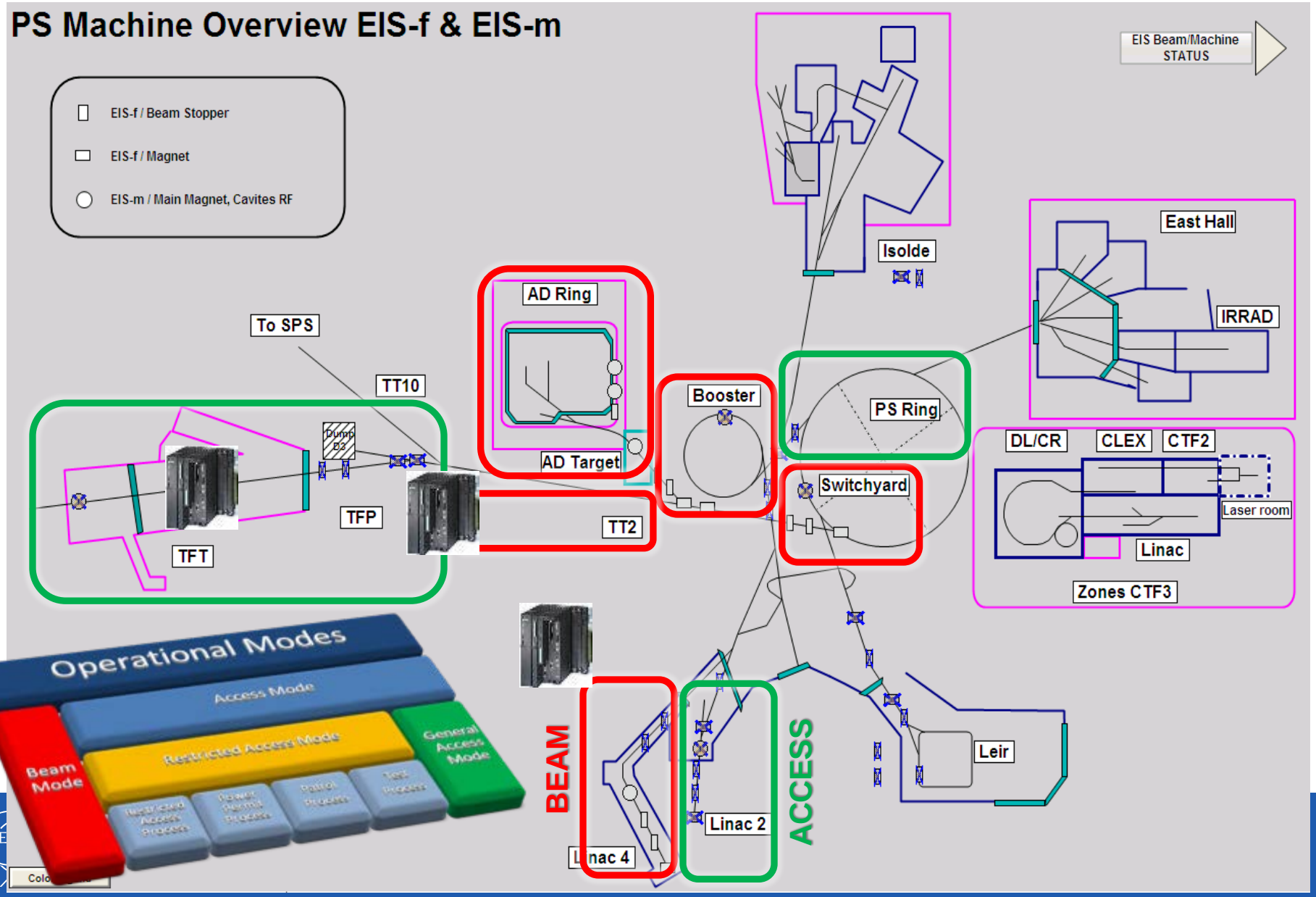
PS-PPS Project Scope



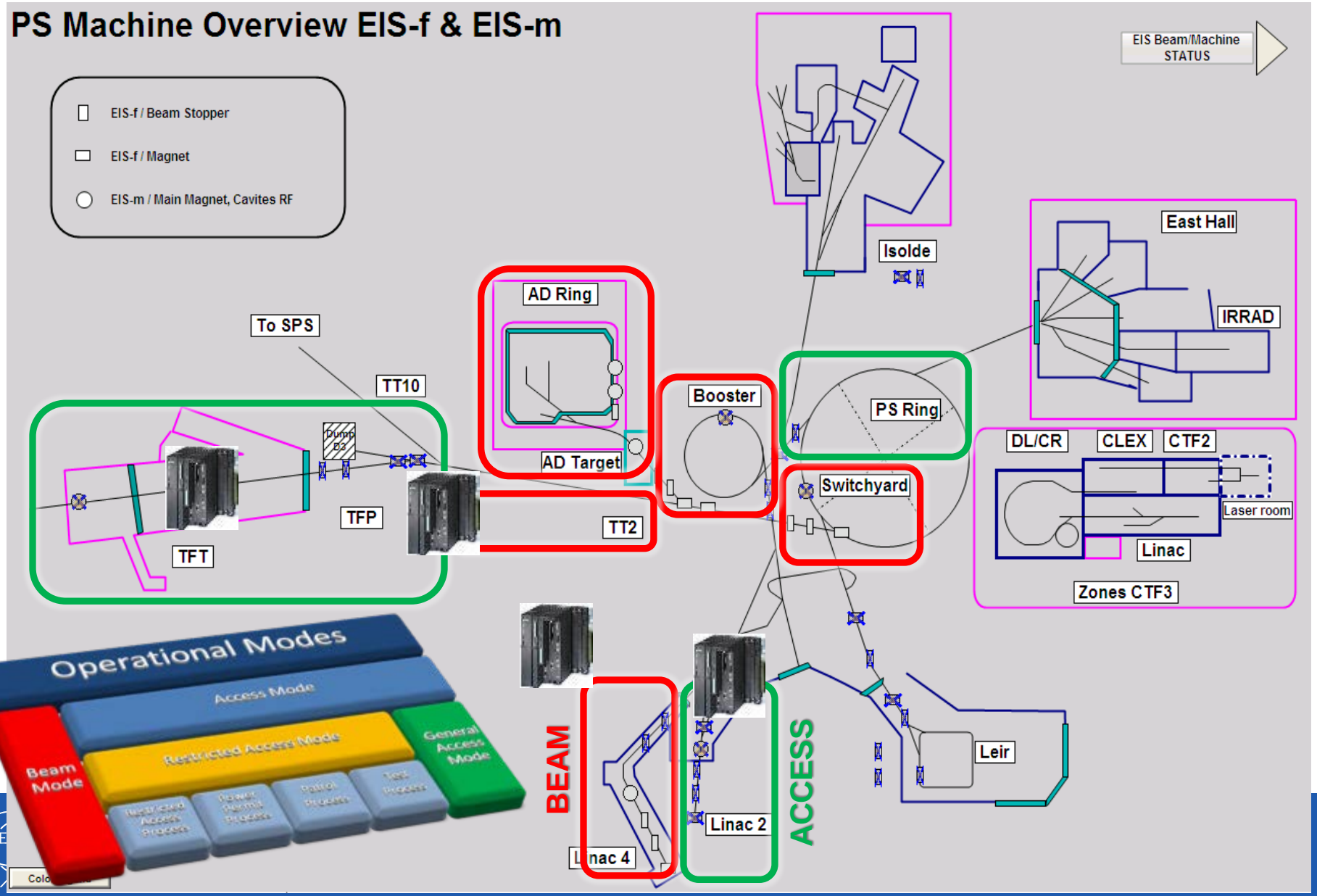
PS-PPS Project Scope



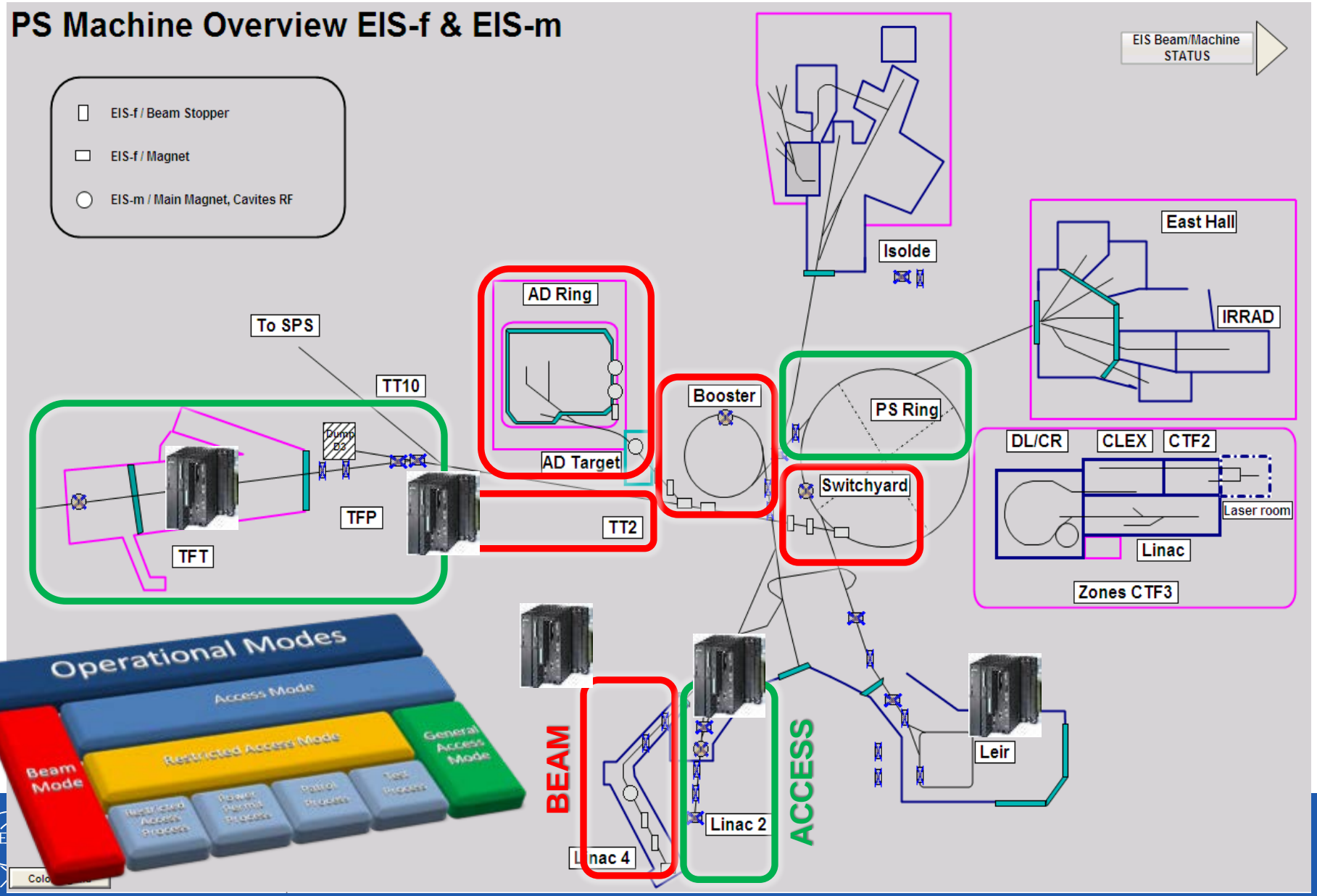
PS-PPS Project Scope



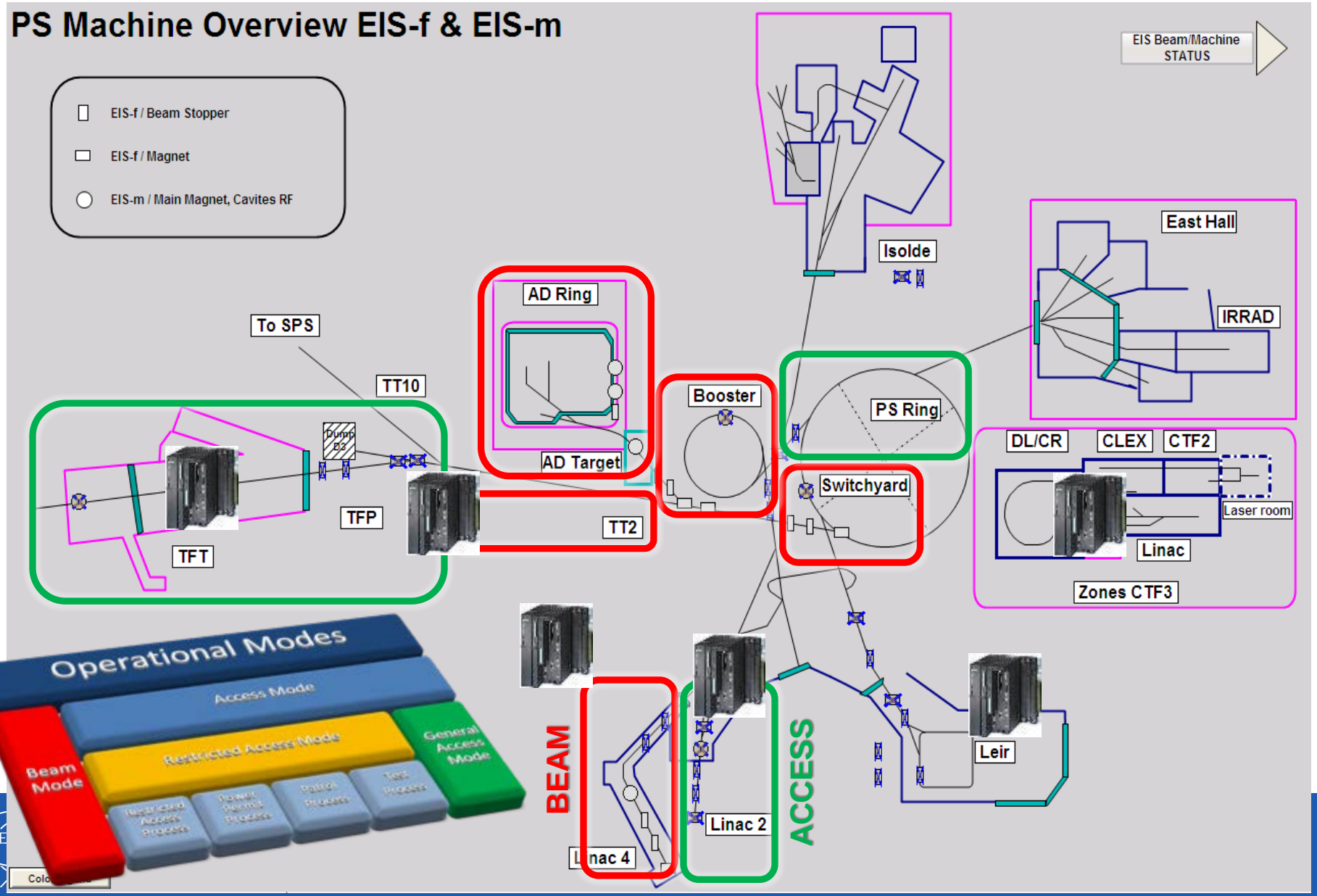
PS-PPS Project Scope



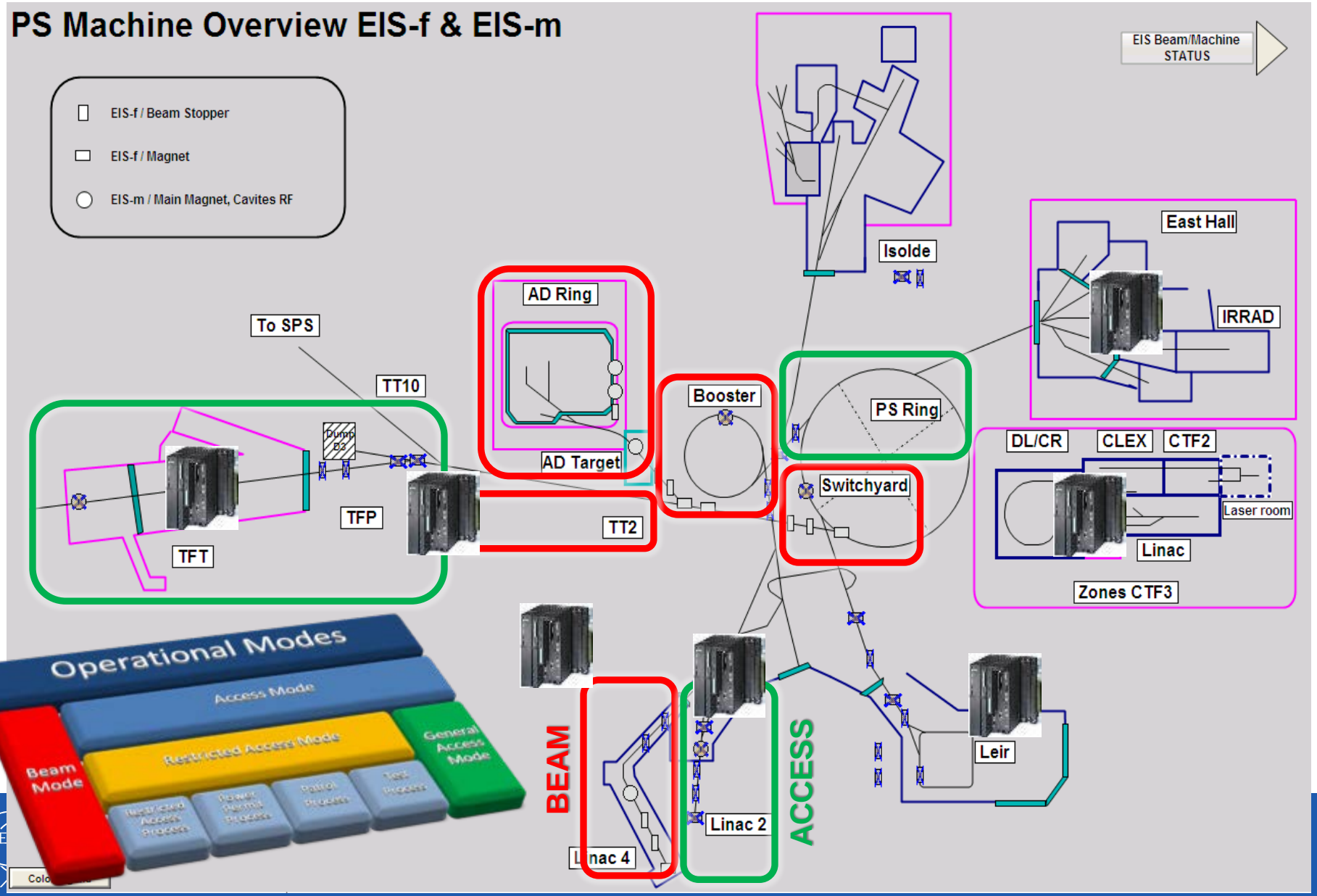
PS-PPS Project Scope



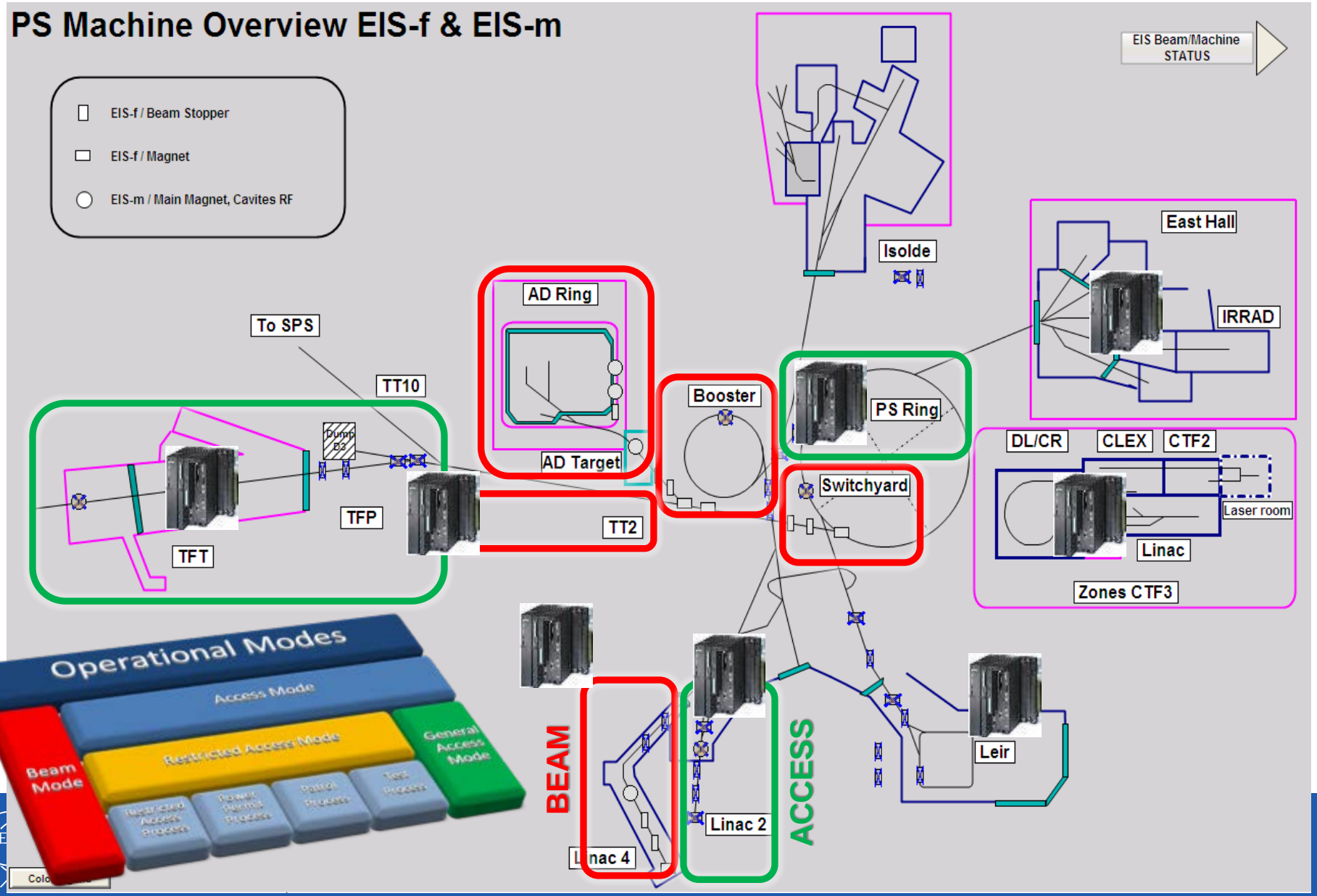
PS-PPS Project Scope



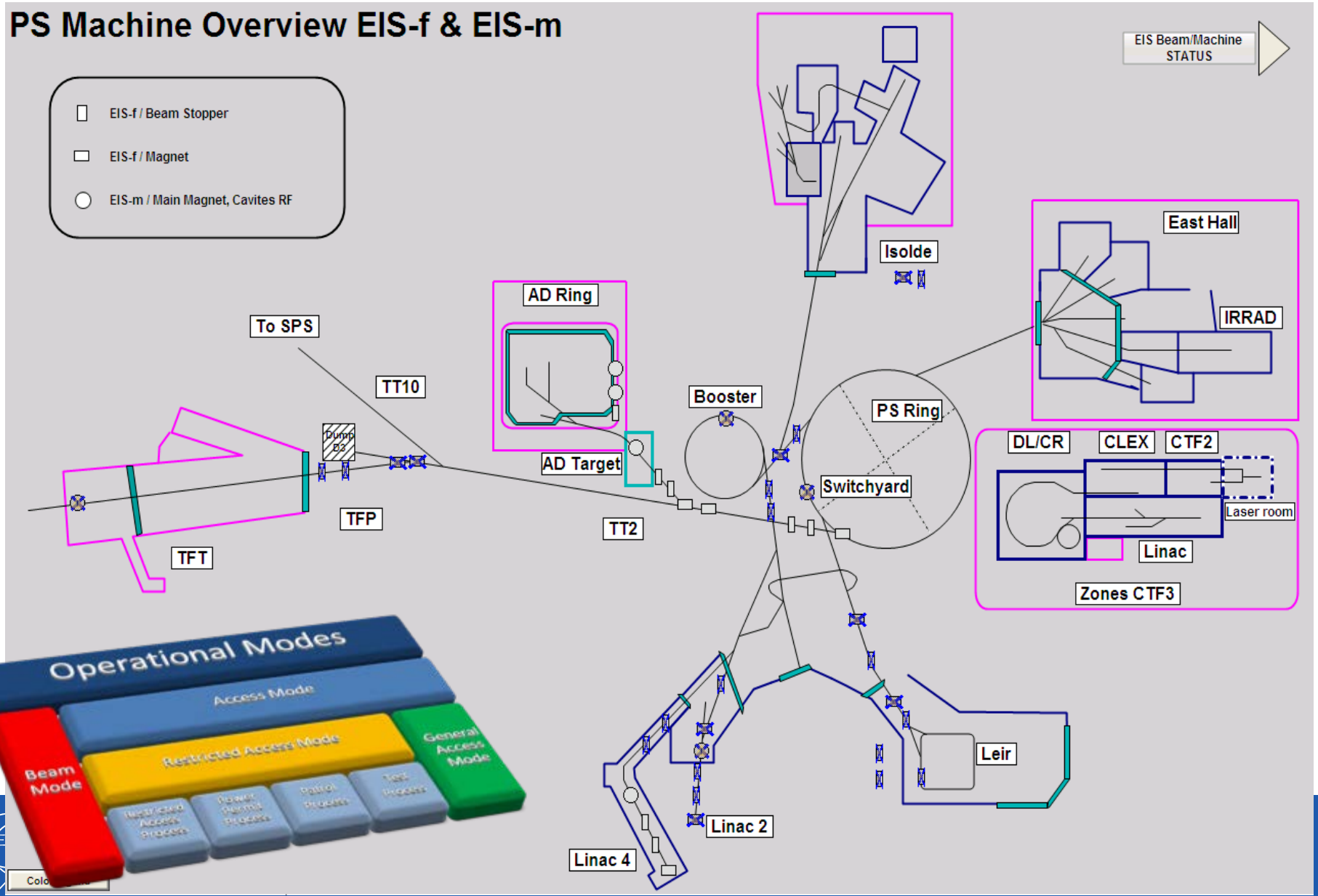
PS-PPS Project Scope



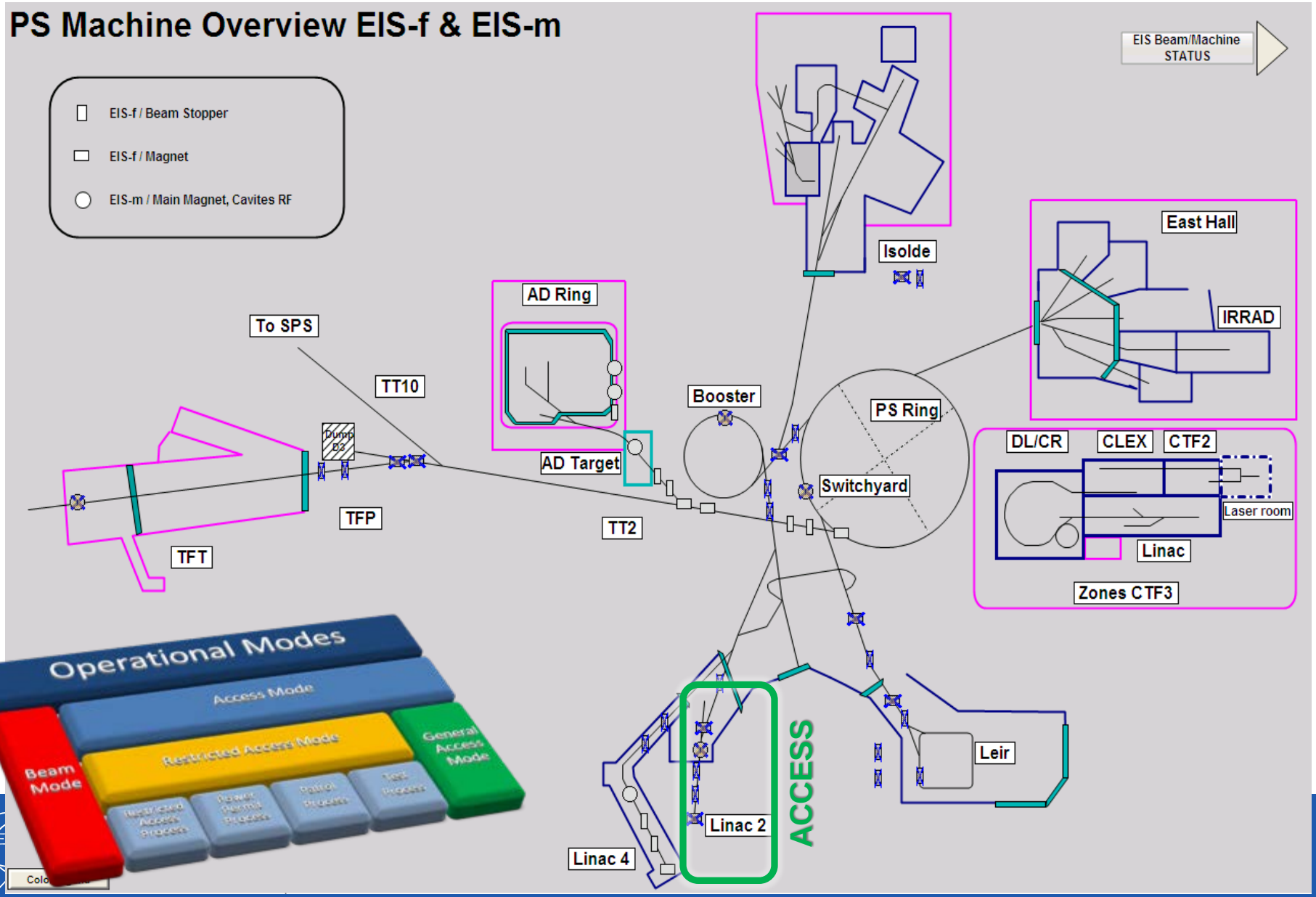
PS-PPS Project Scope



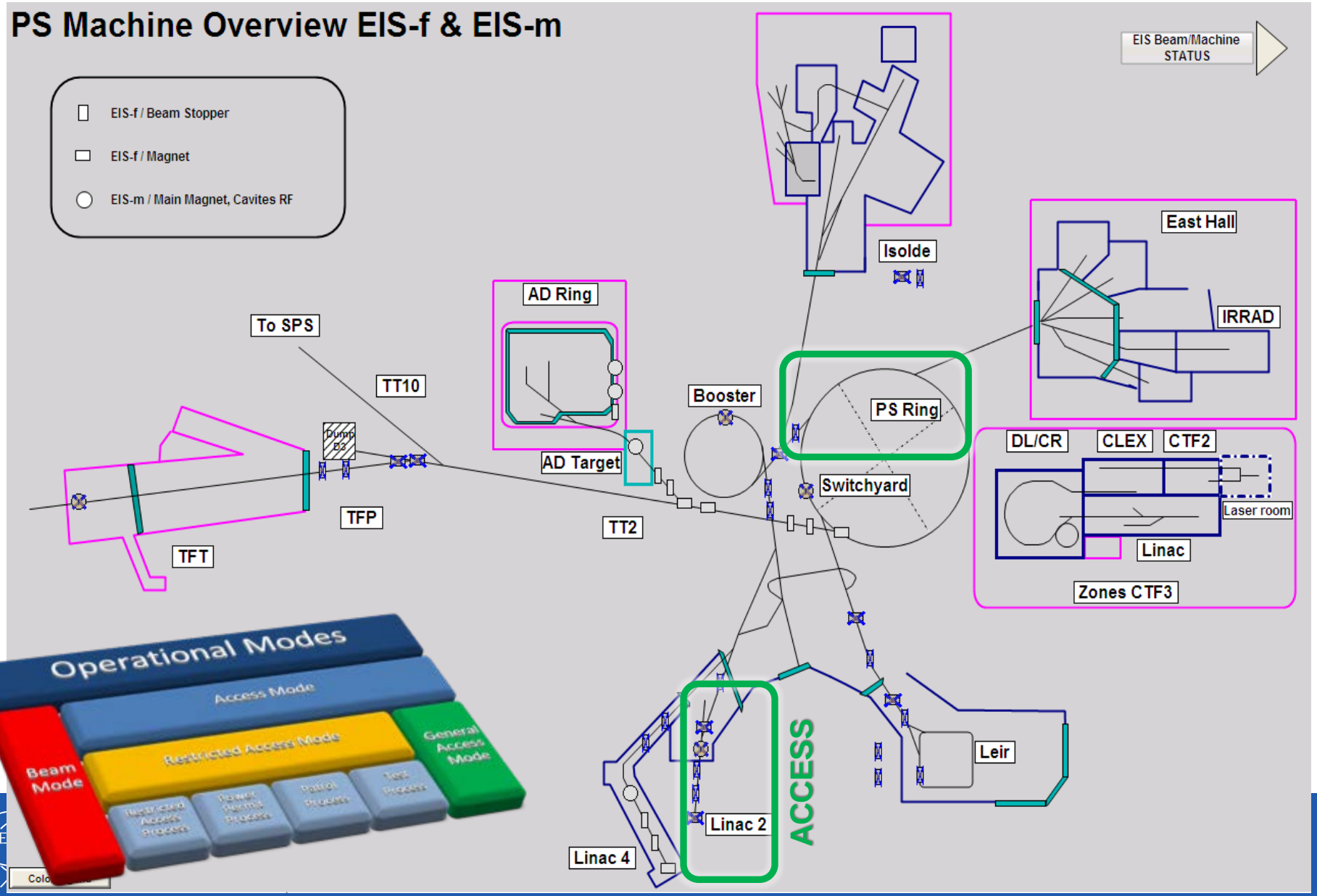
PS-PPS Project Scope



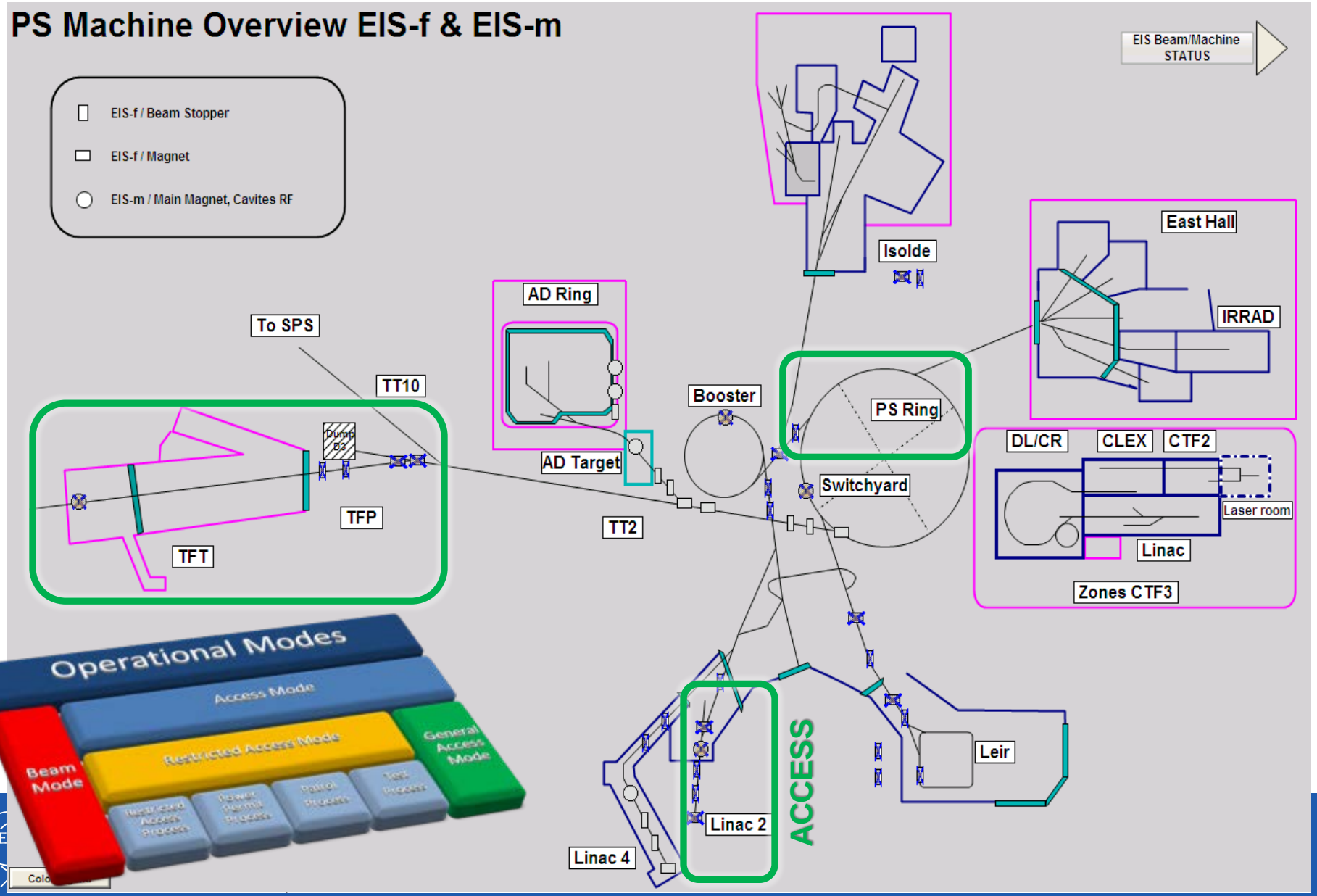
PS-PPS Project Scope



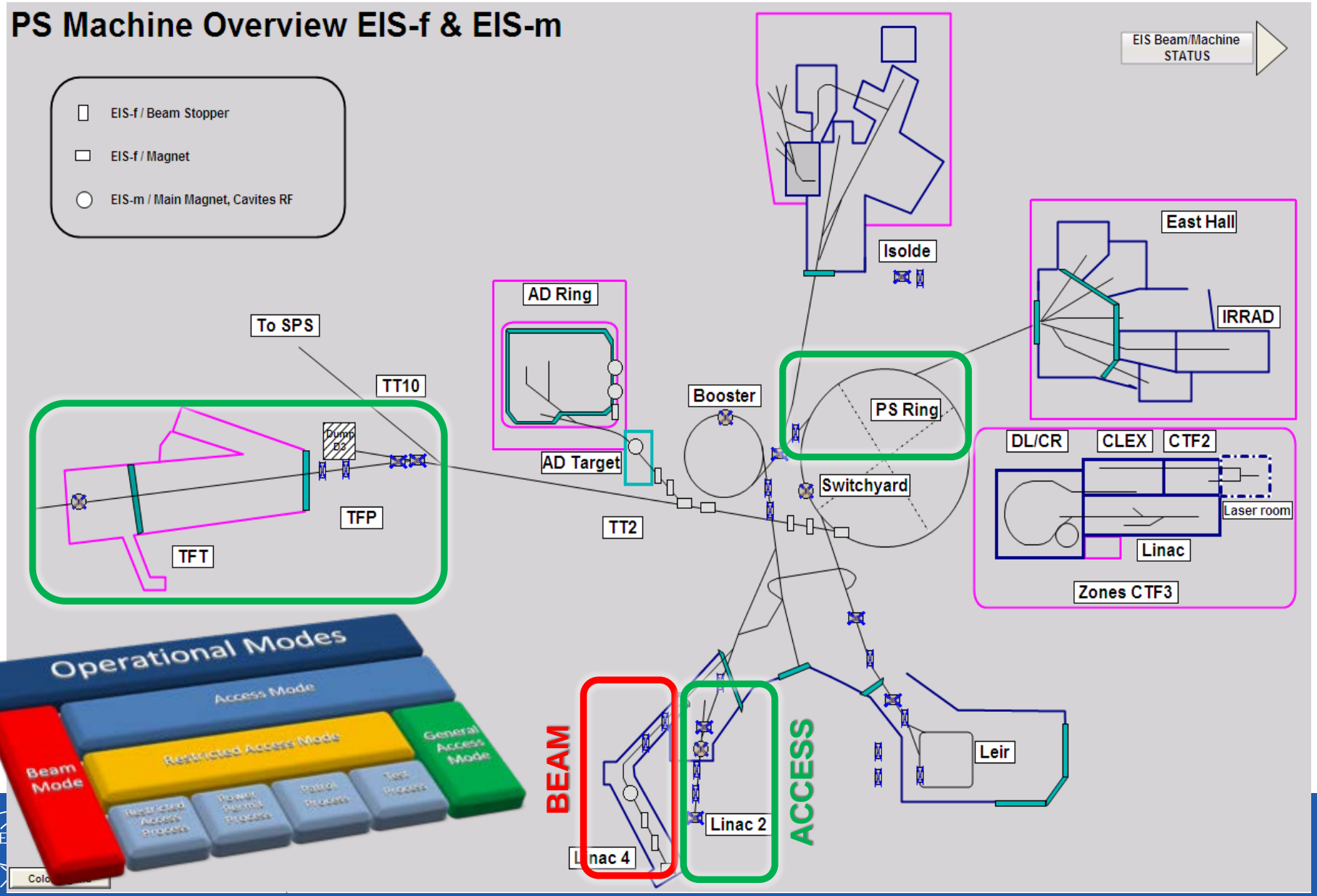
PS-PPS Project Scope



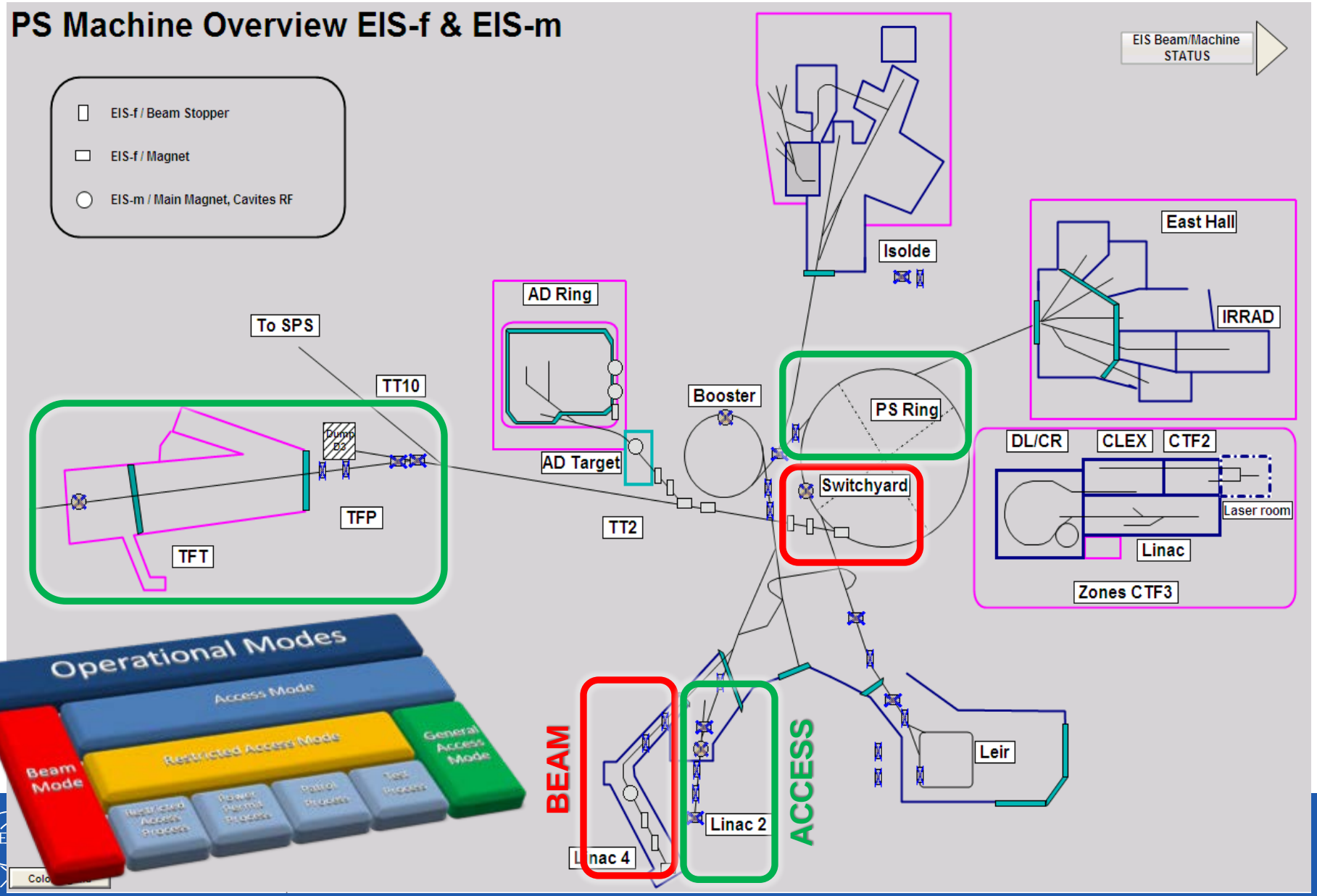
PS-PPS Project Scope



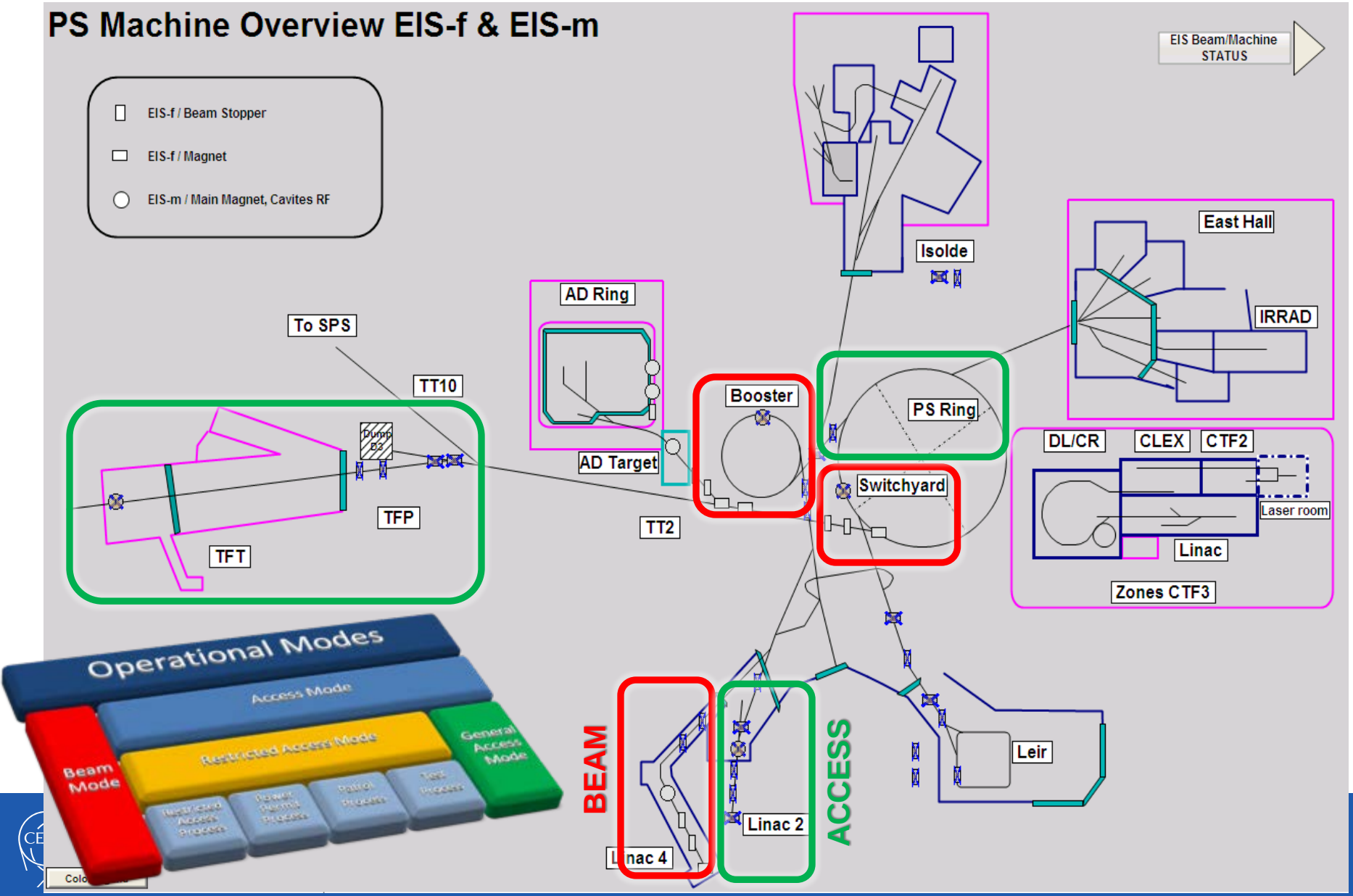
PS-PPS Project Scope



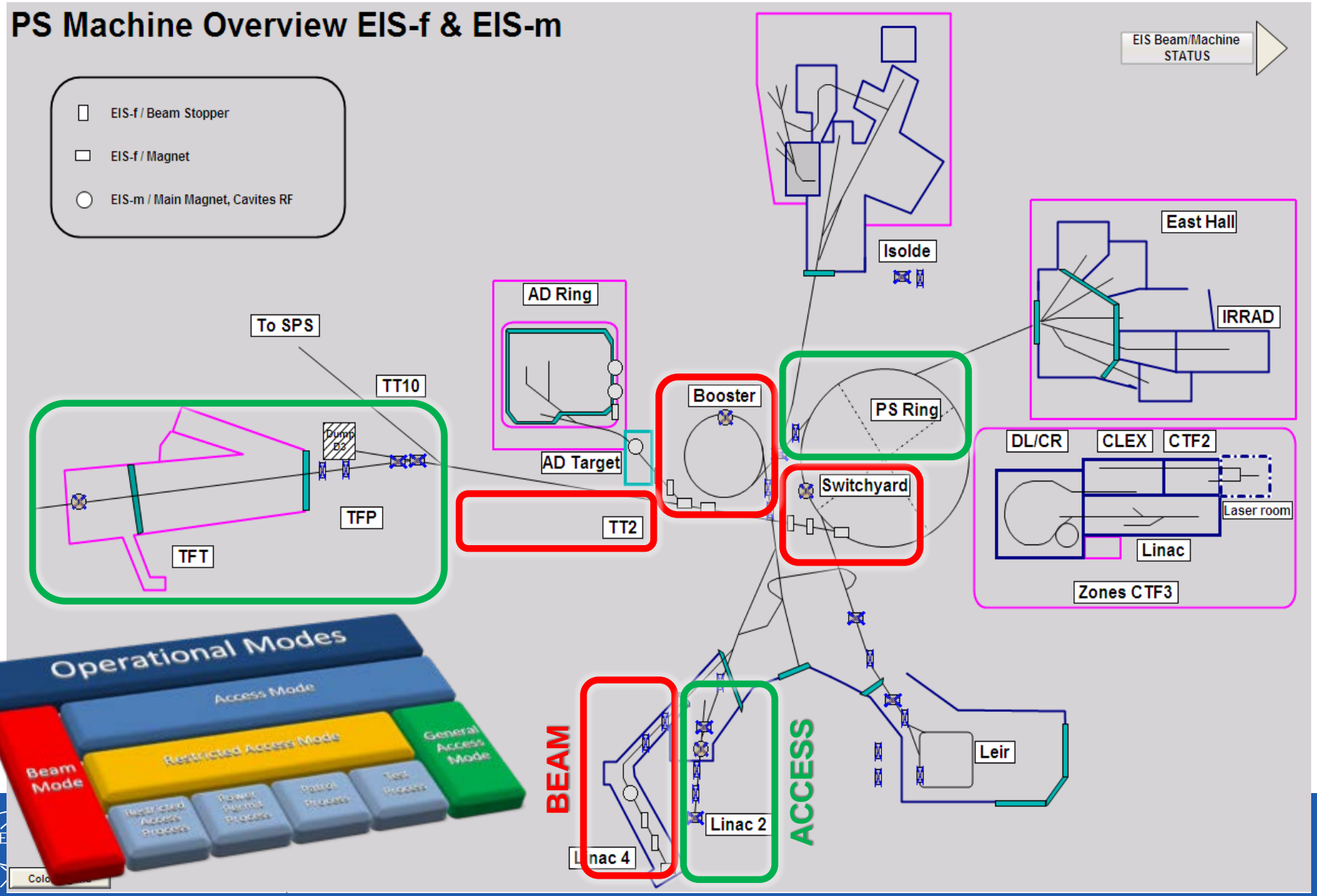
PS-PPS Project Scope



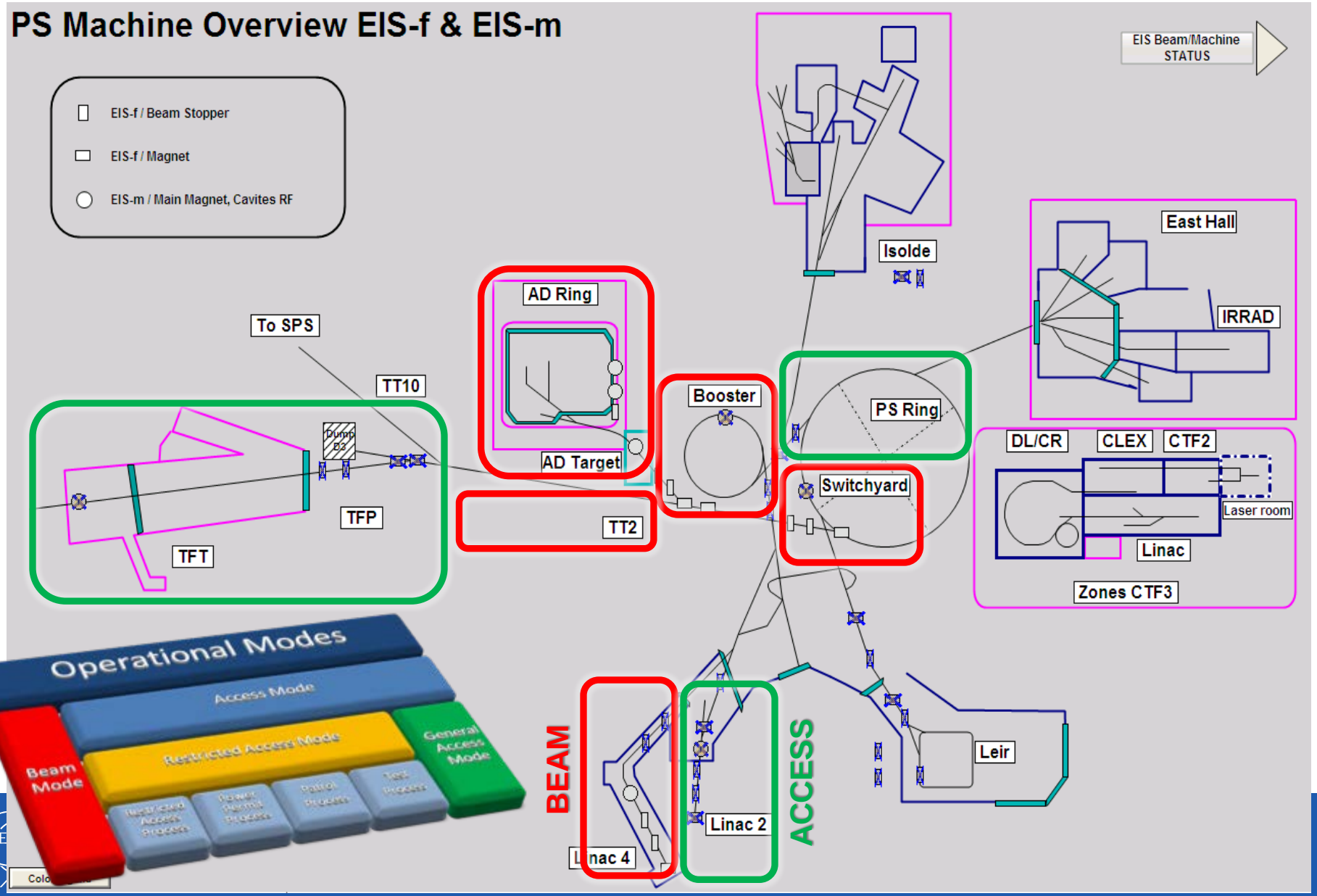
PS-PPS Project Scope



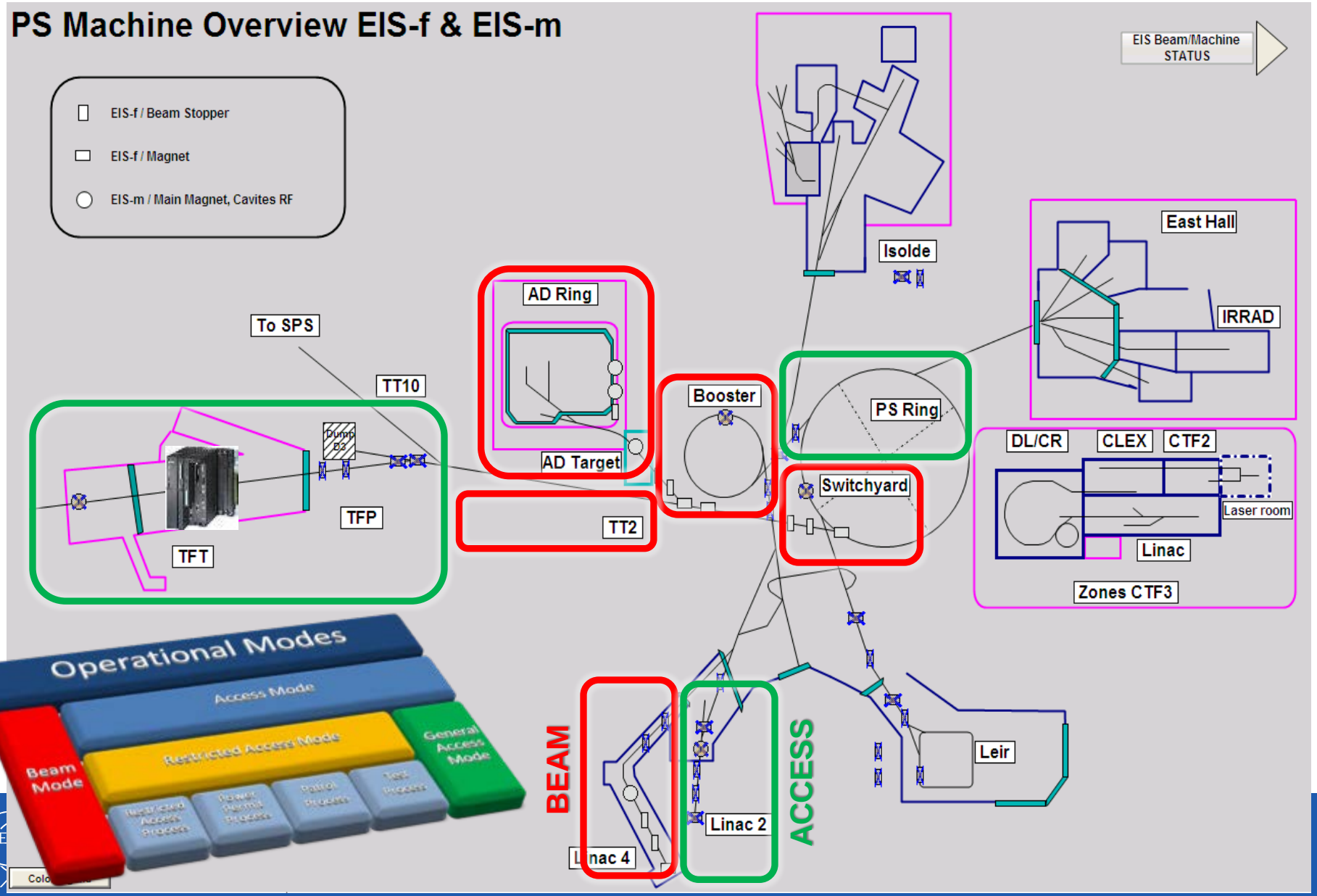
PS-PPS Project Scope



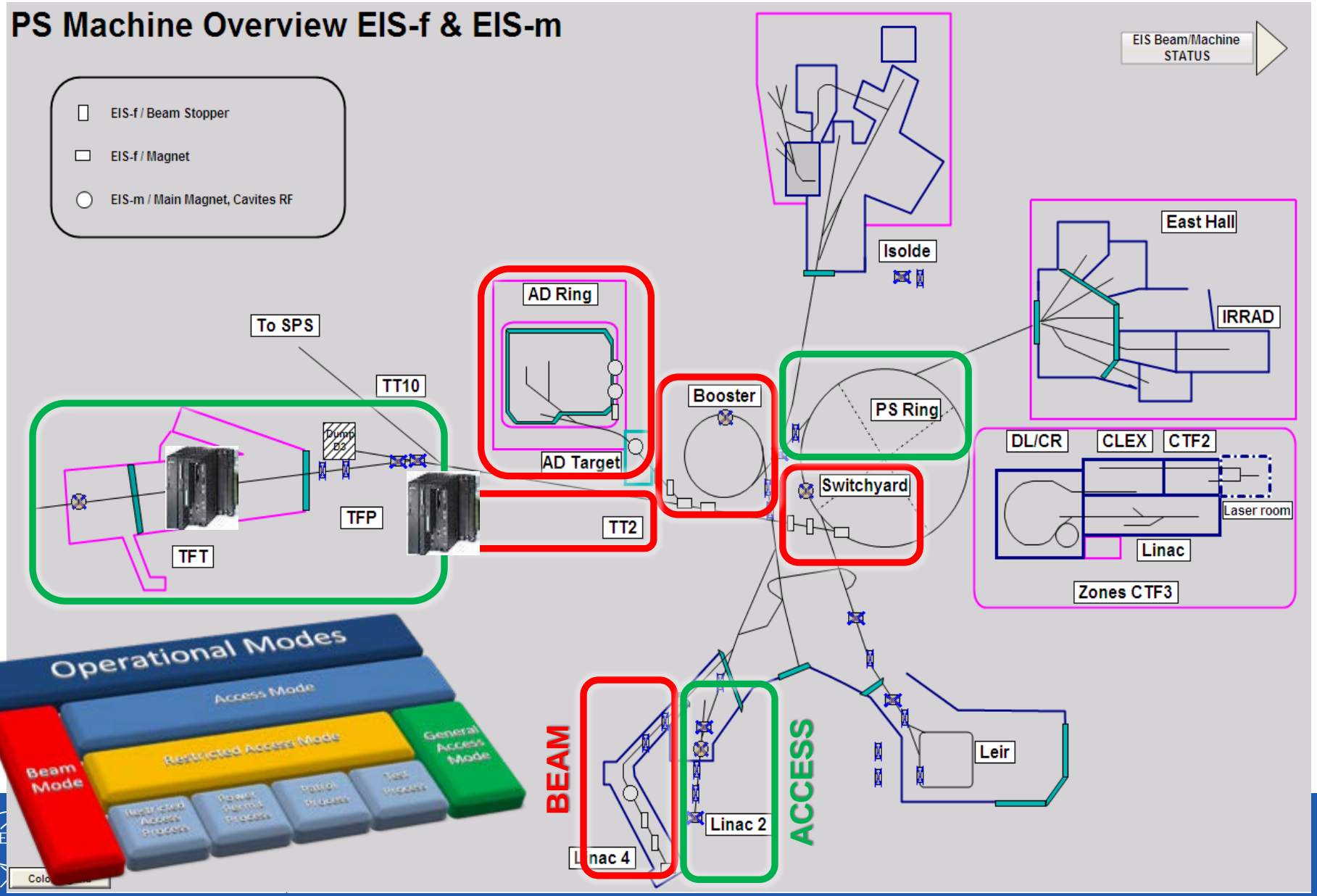
PS-PPS Project Scope



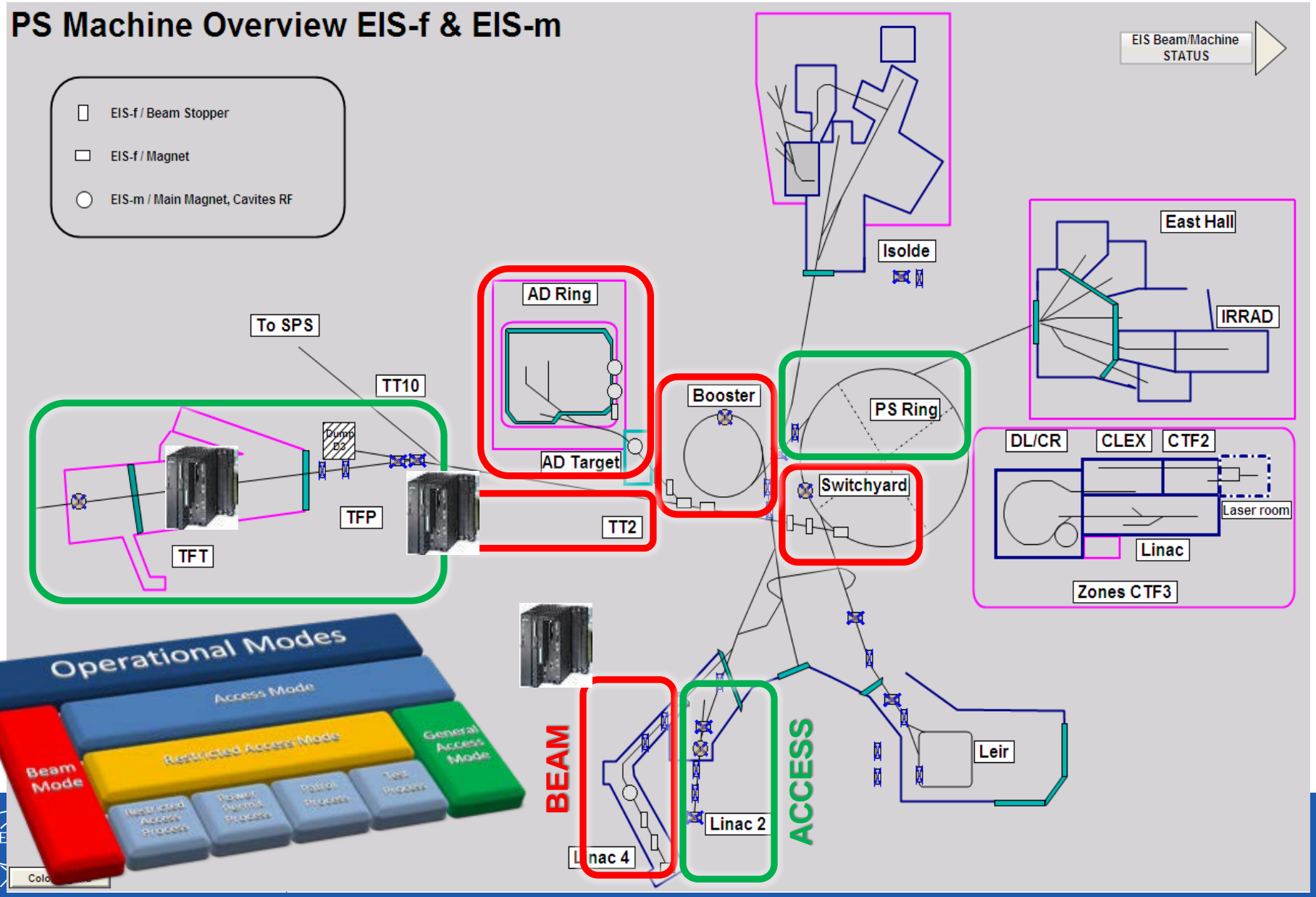
PS-PPS Project Scope



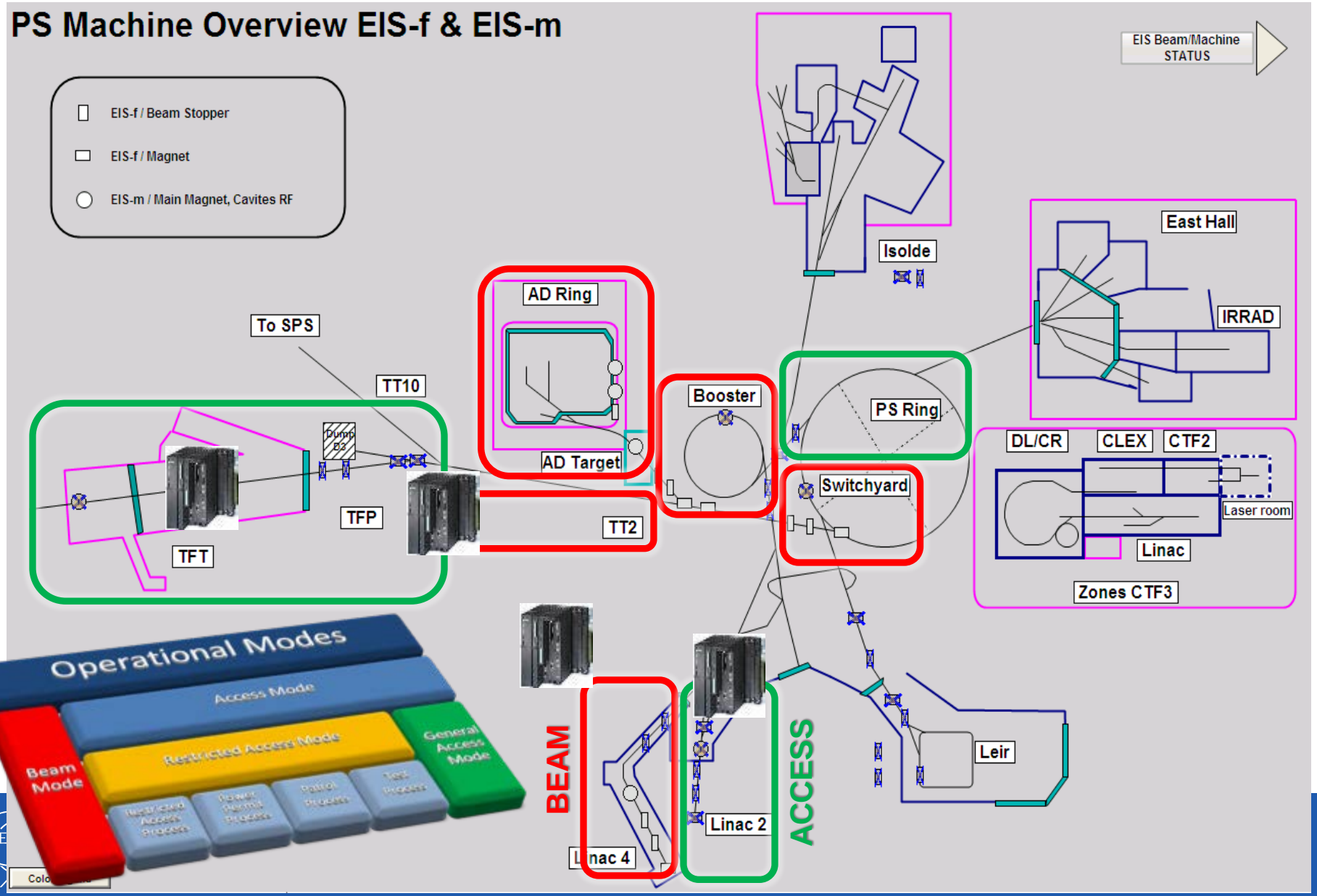
PS-PPS Project Scope



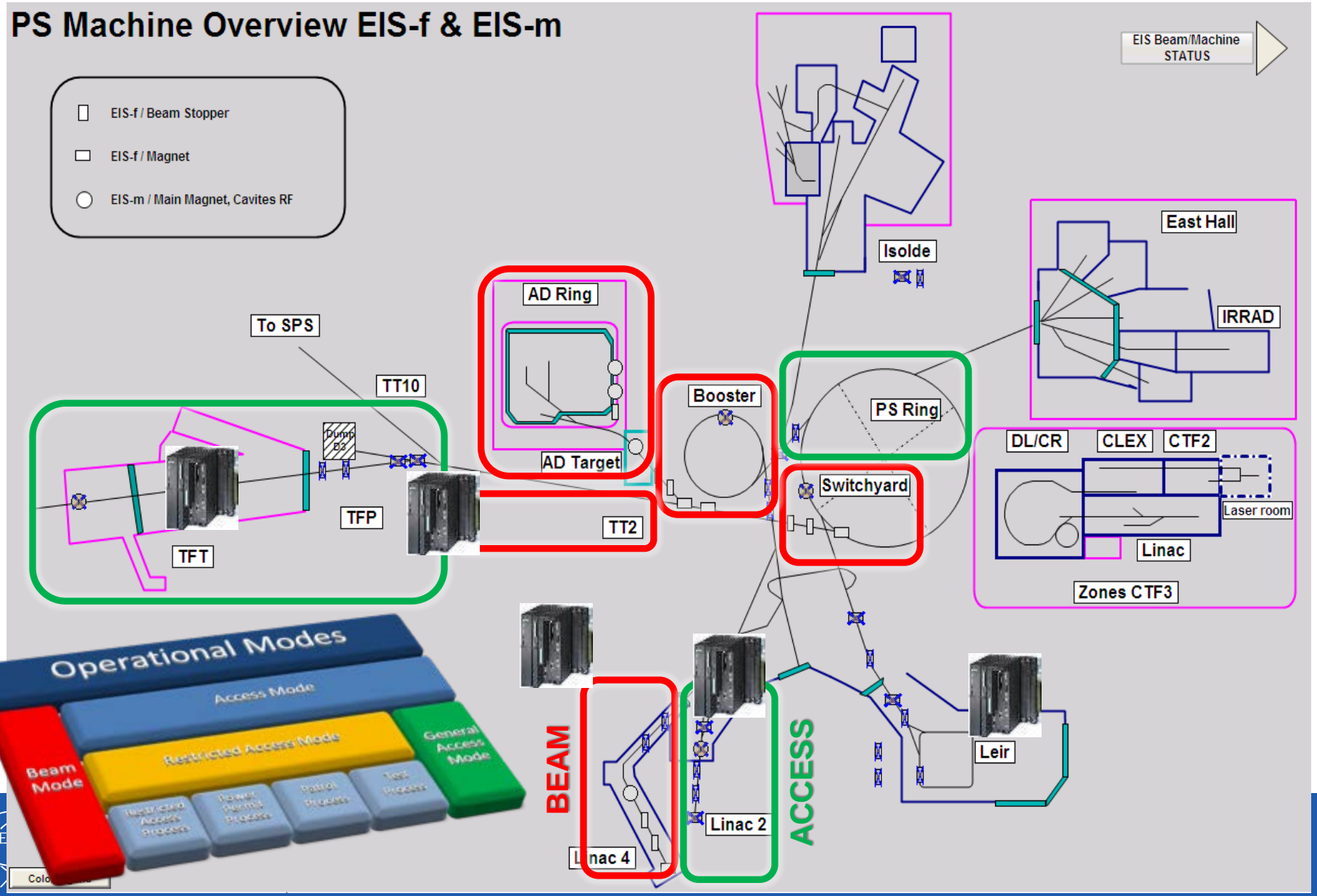
PS-PPS Project Scope



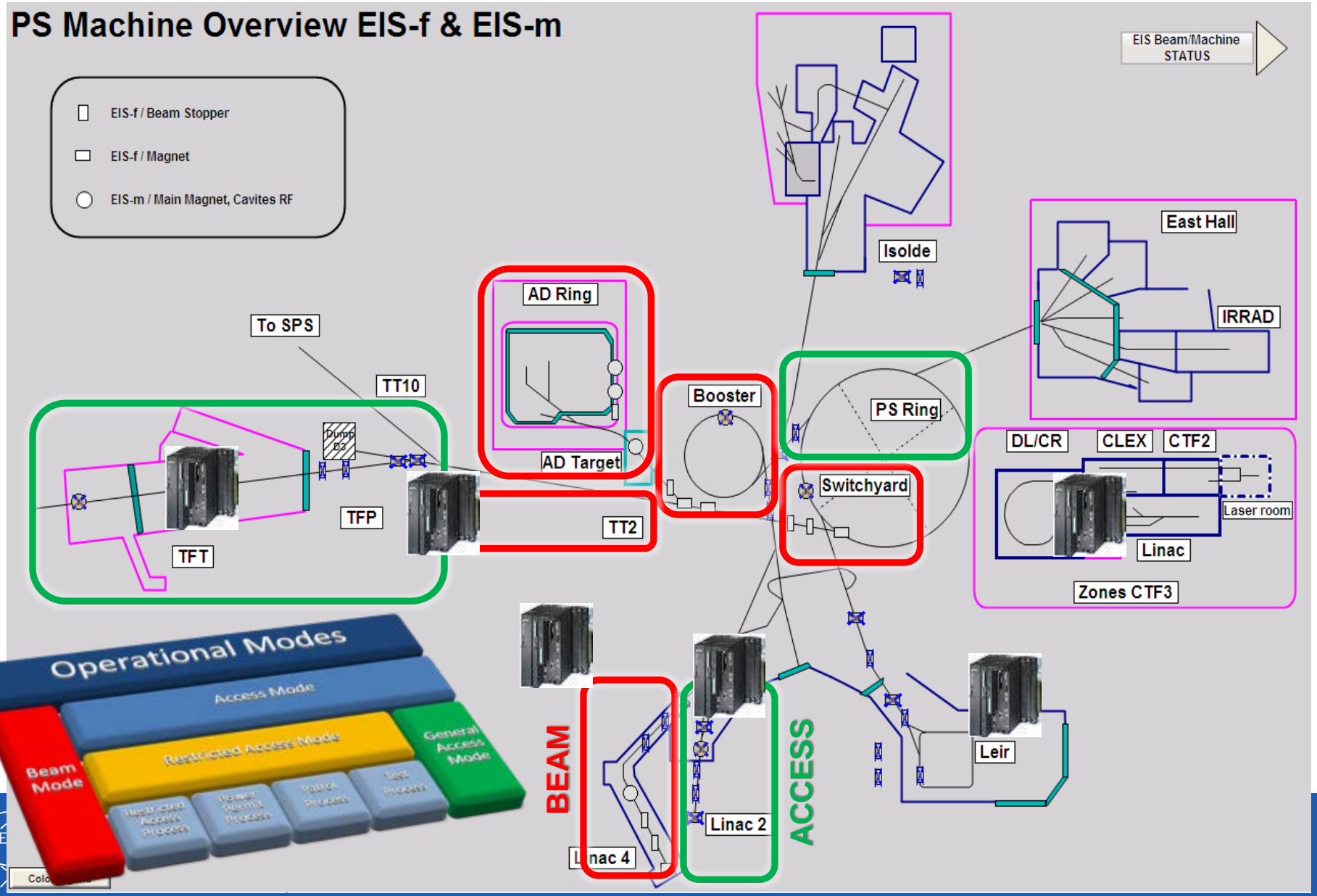
PS-PPS Project Scope



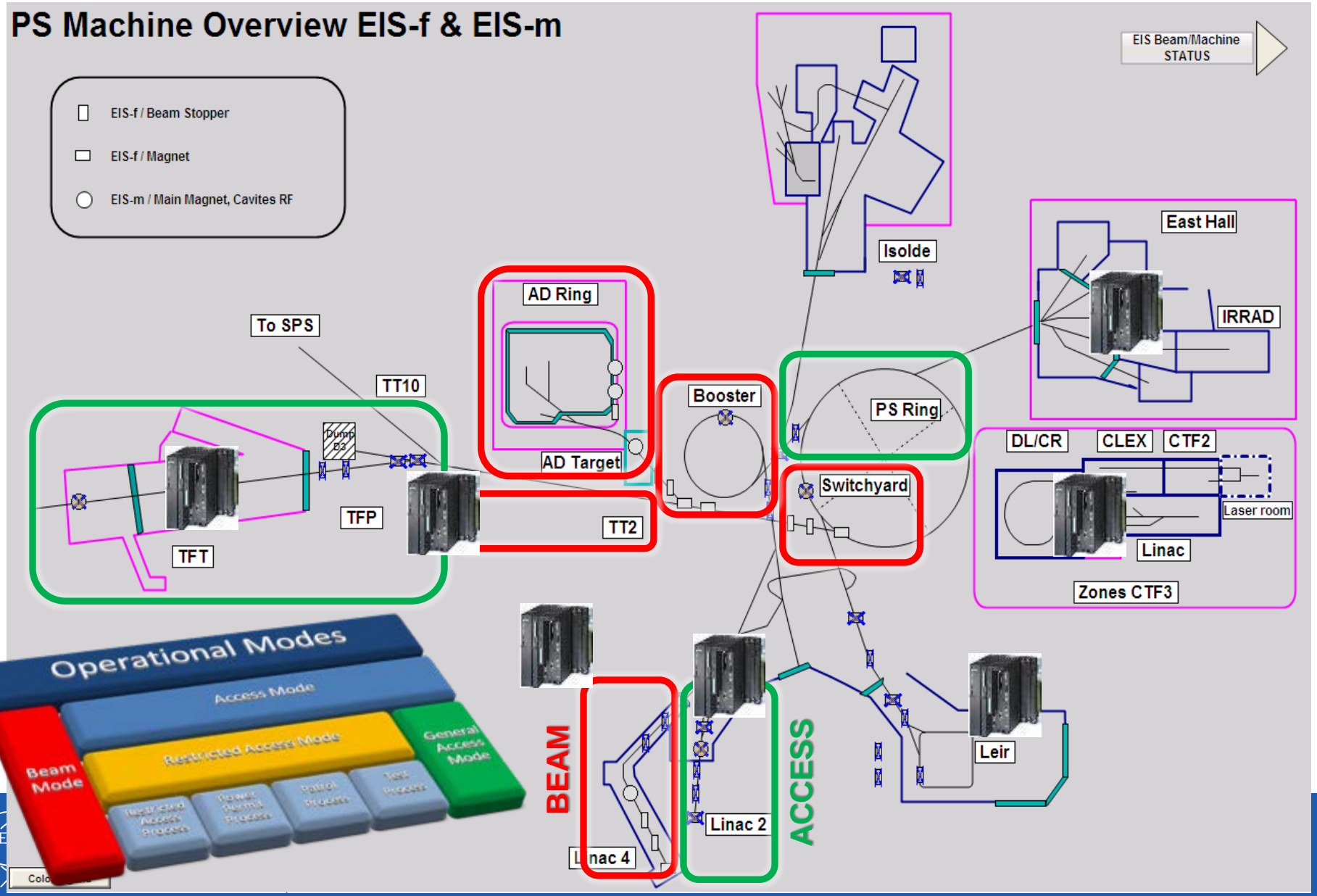
PS-PPS Project Scope



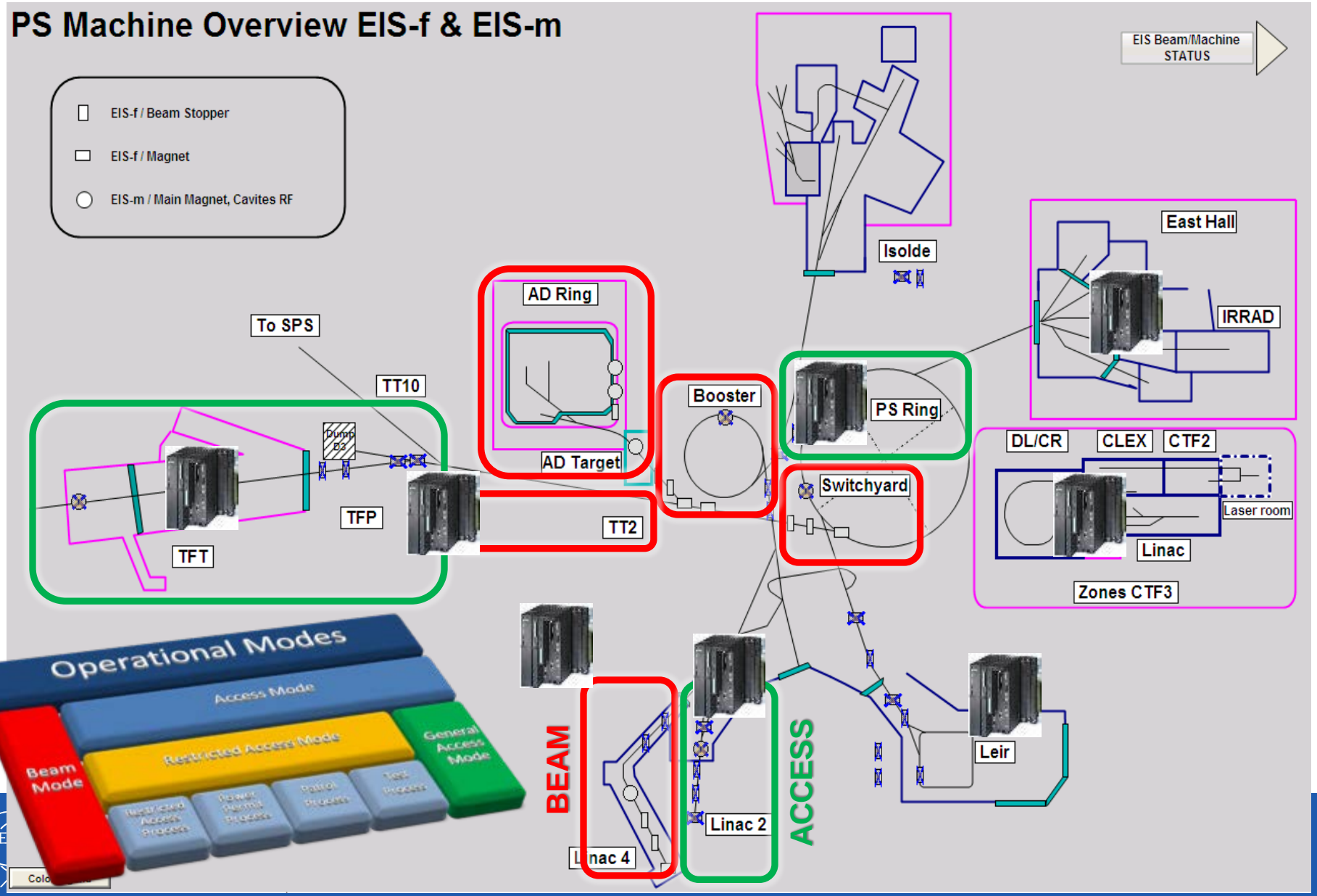
PS-PPS Project Scope



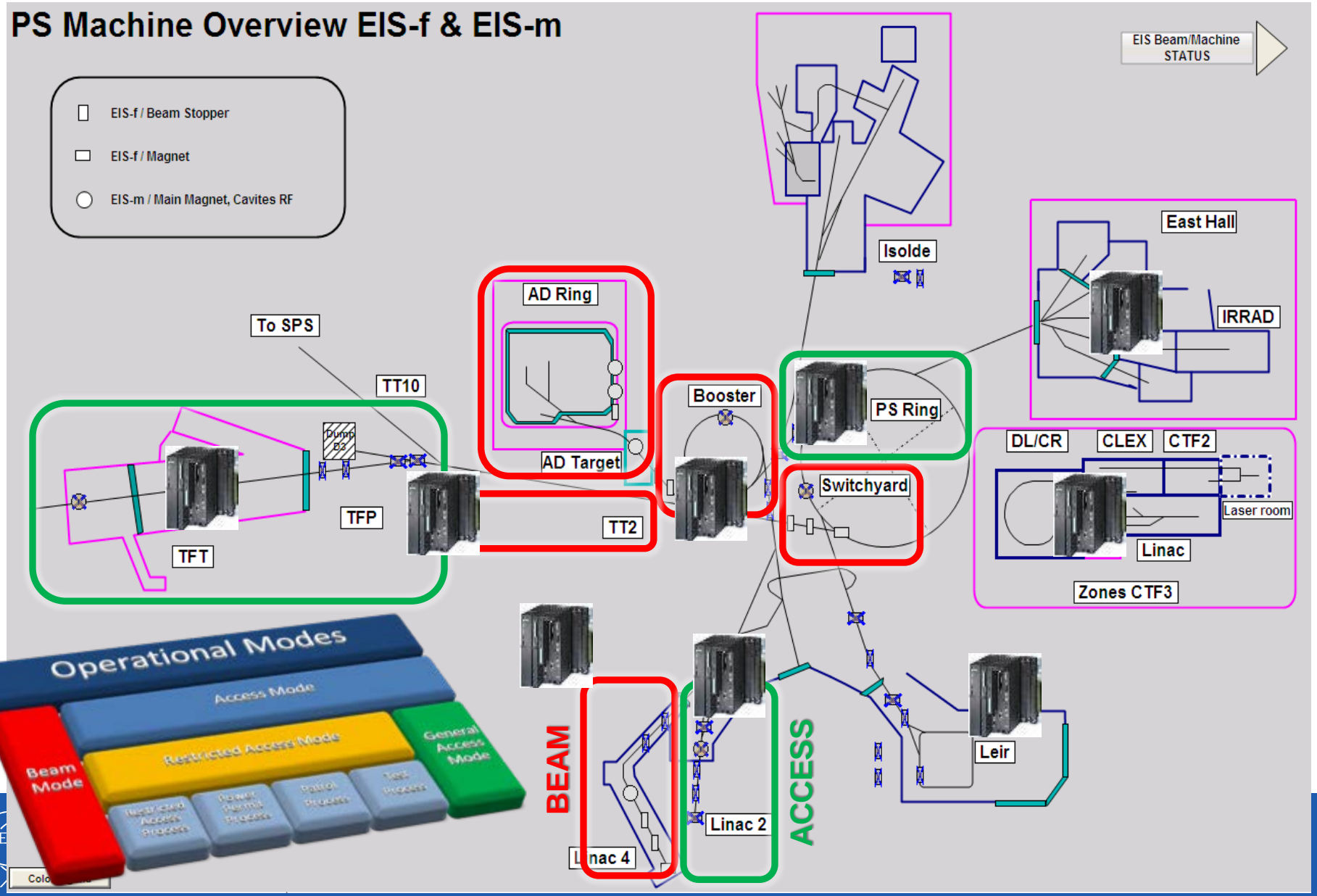
PS-PPS Project Scope



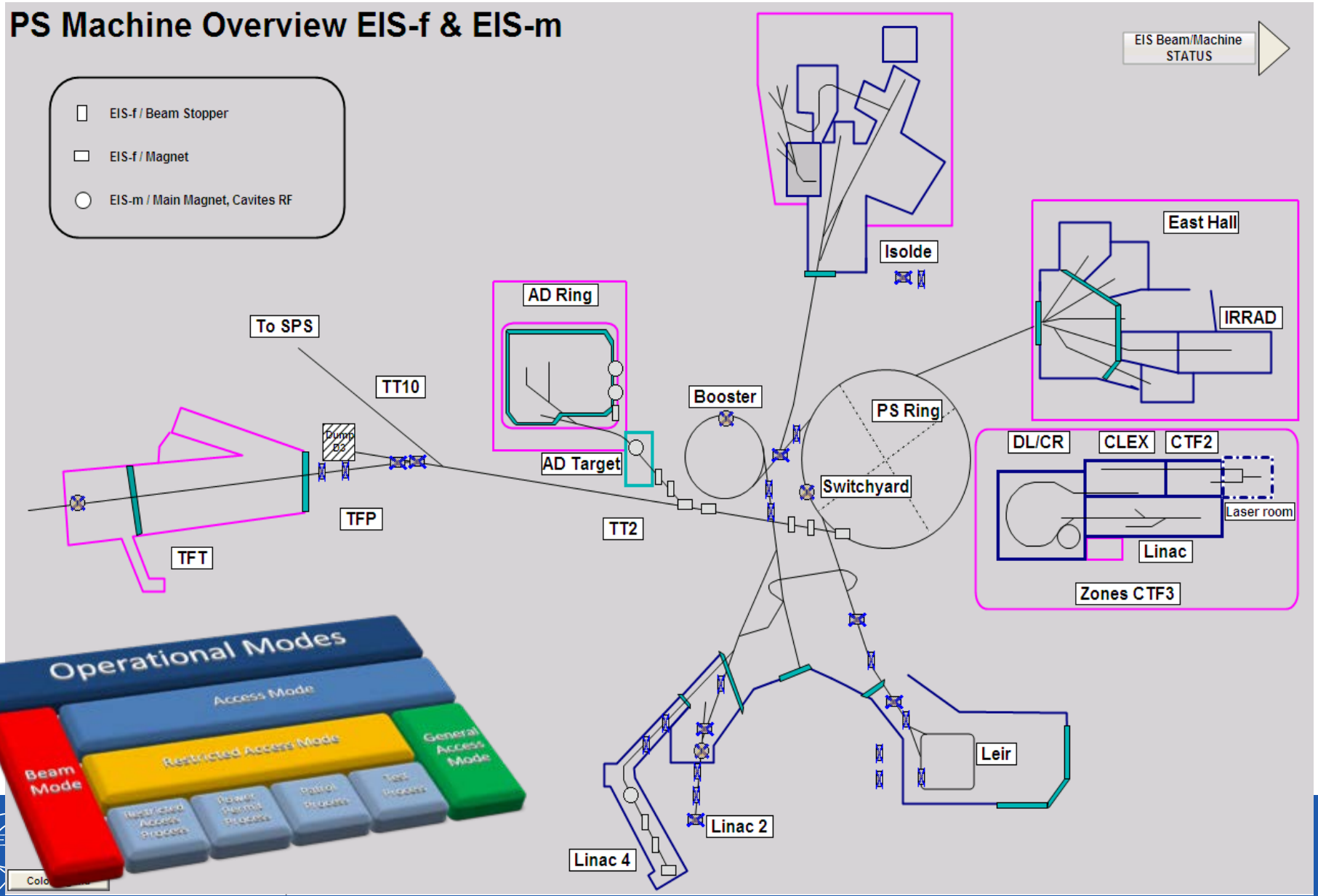
PS-PPS Project Scope



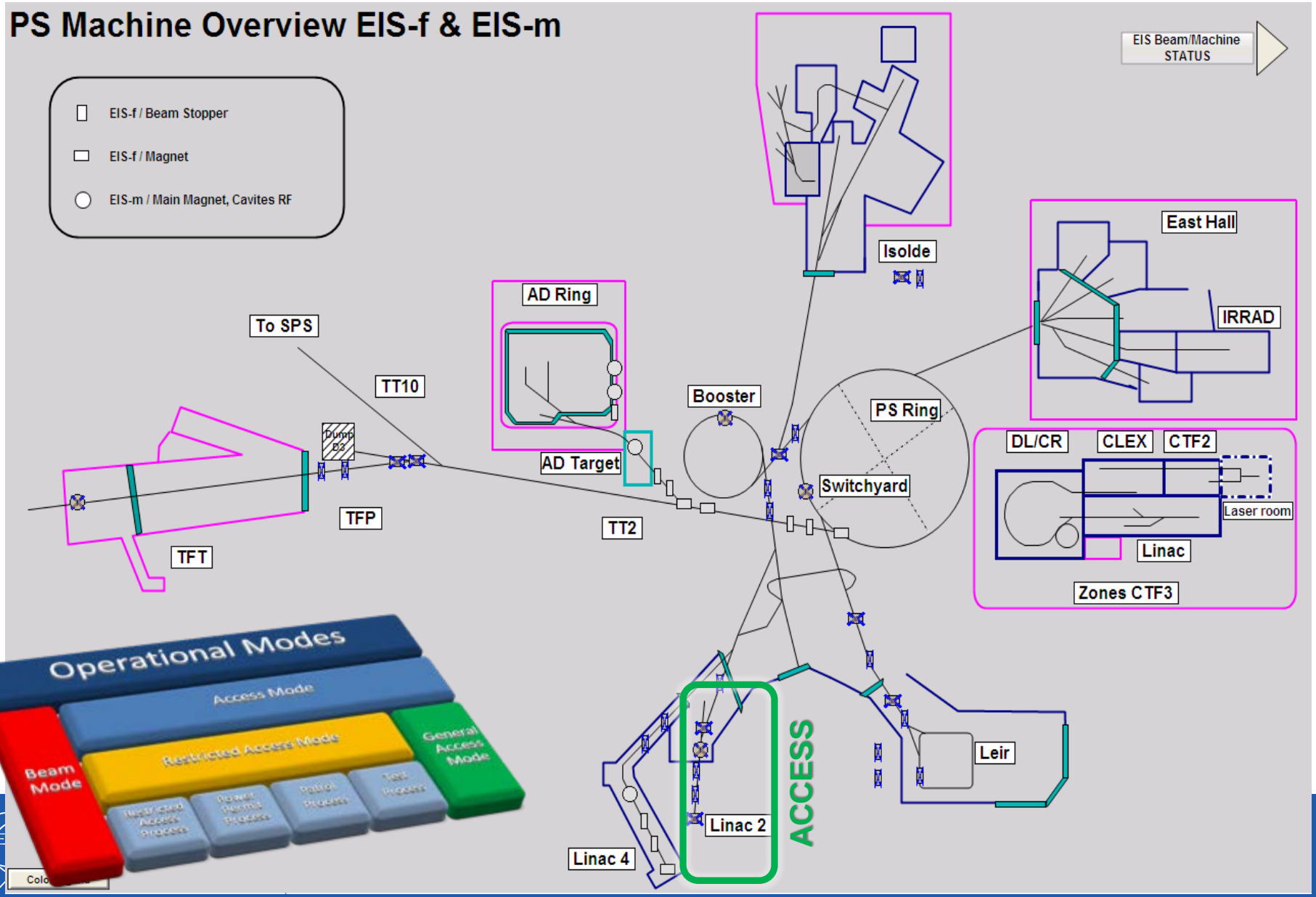
PS-PPS Project Scope



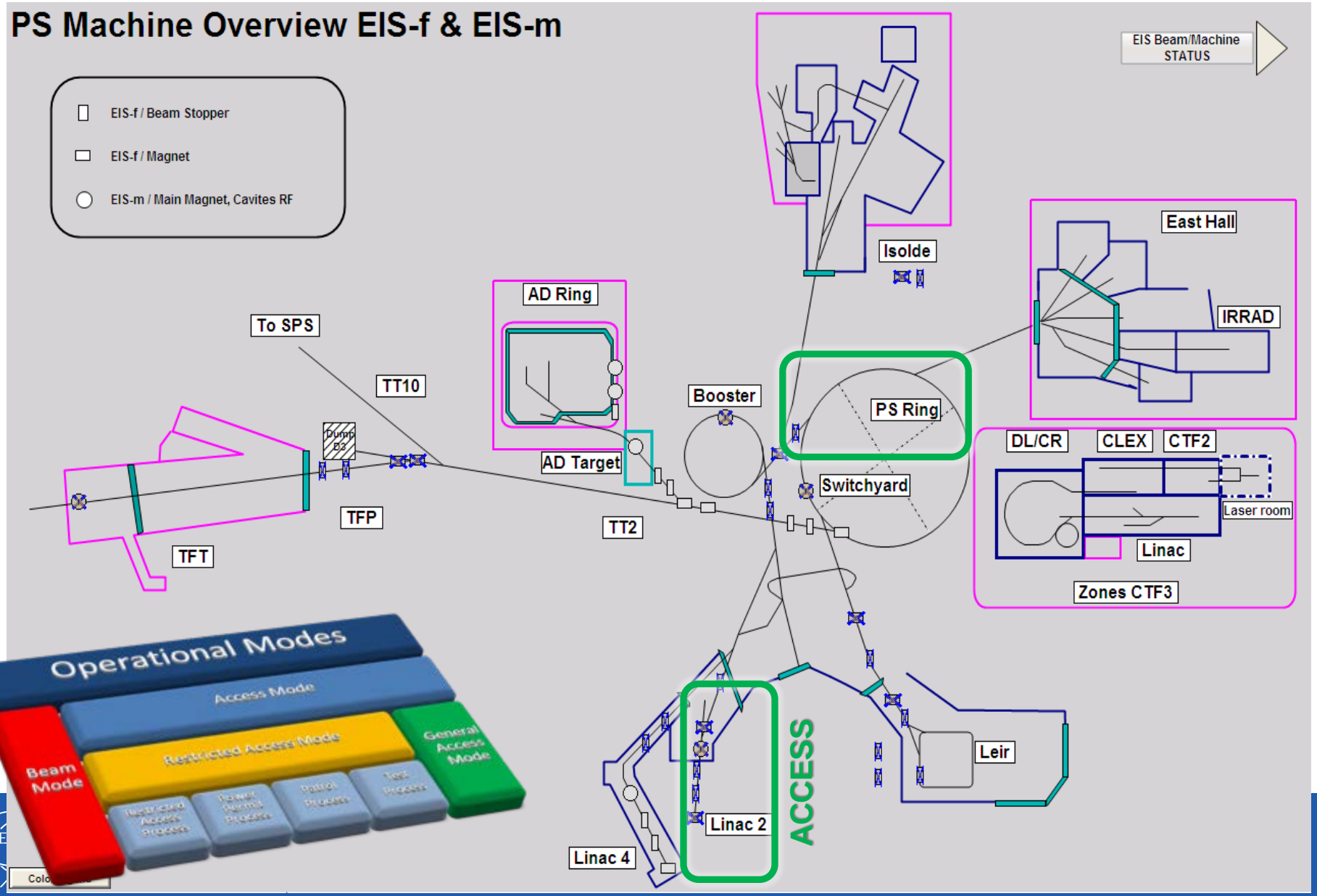
PS-PPS Project Scope



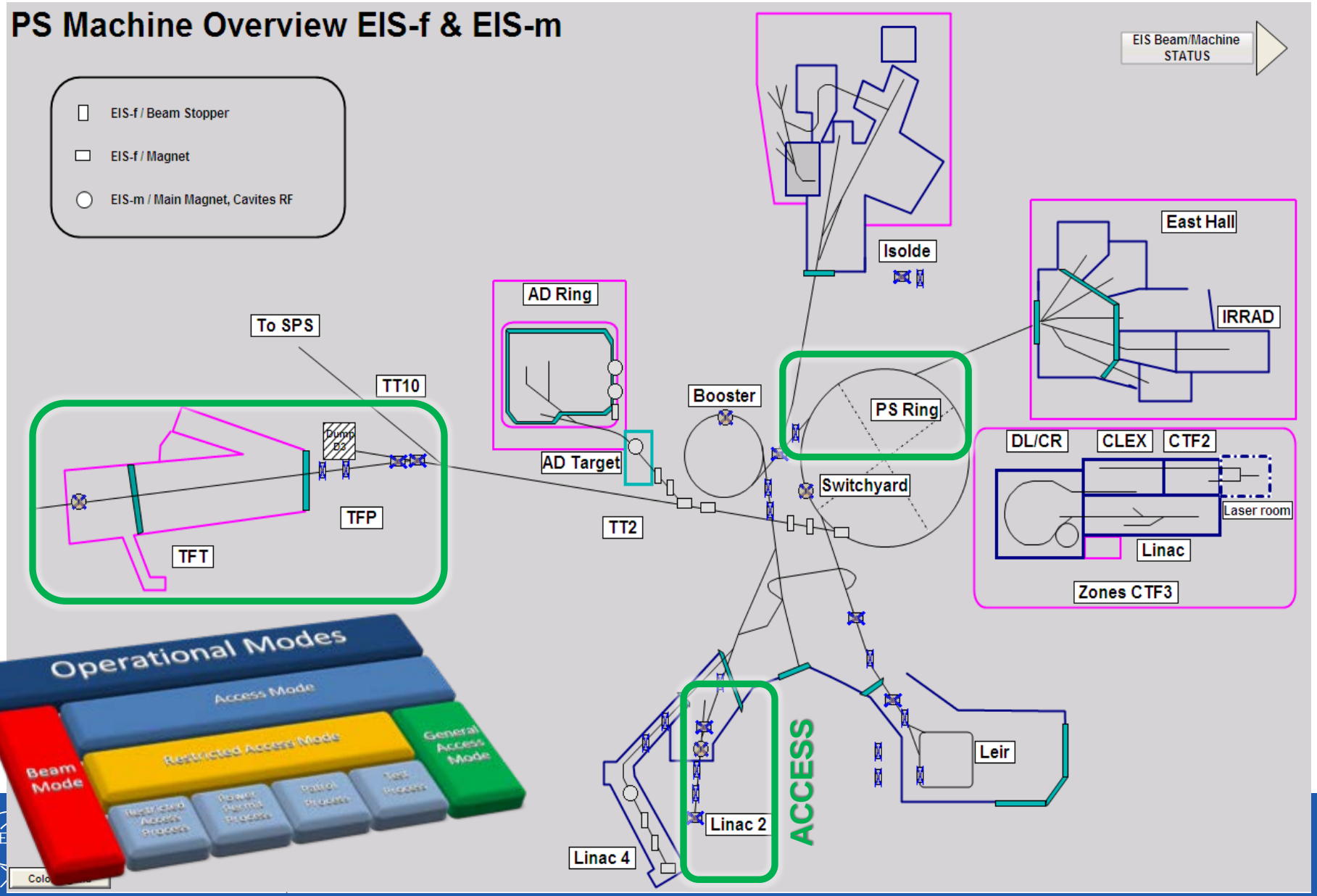
PS-PPS Project Scope



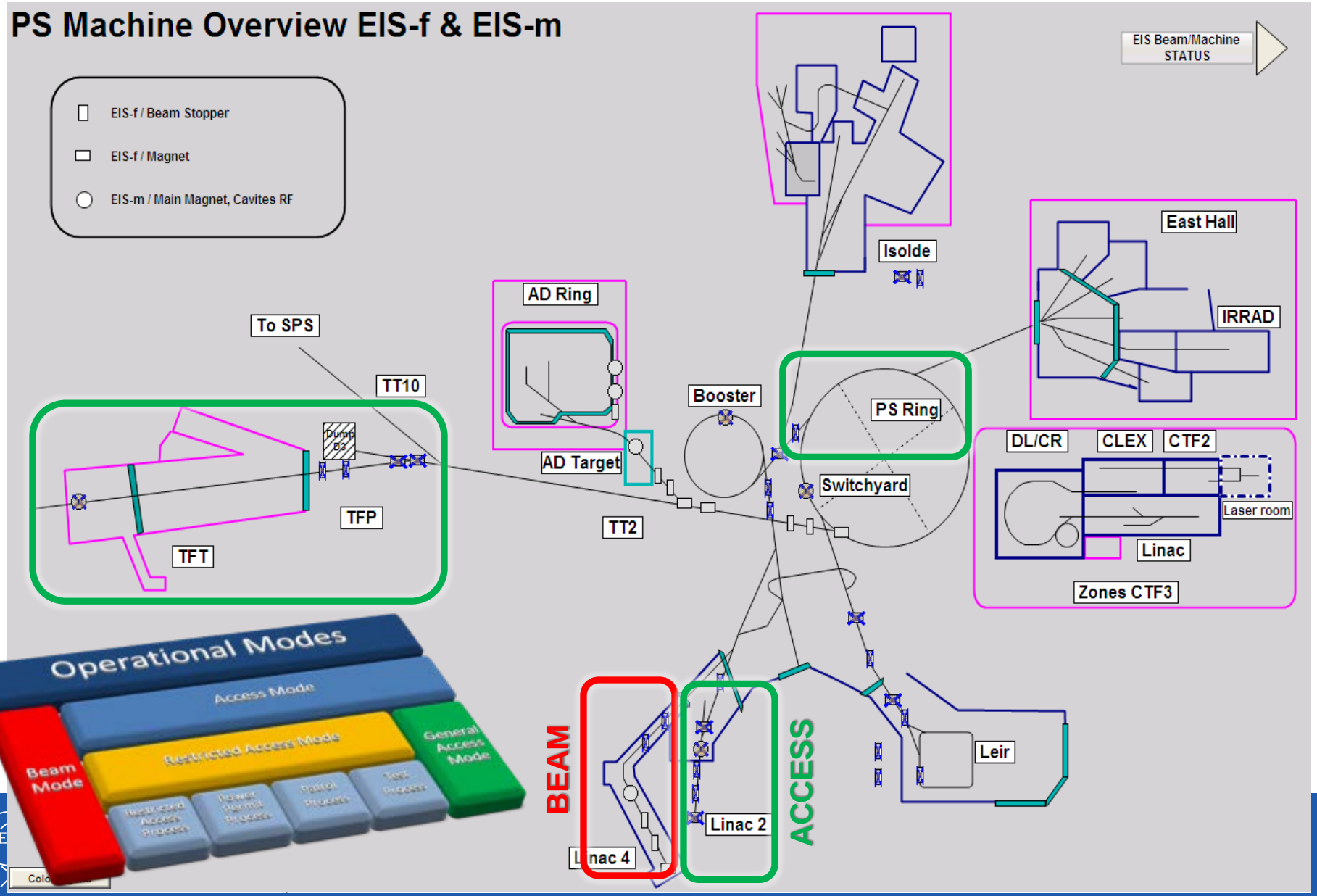
PS-PPS Project Scope



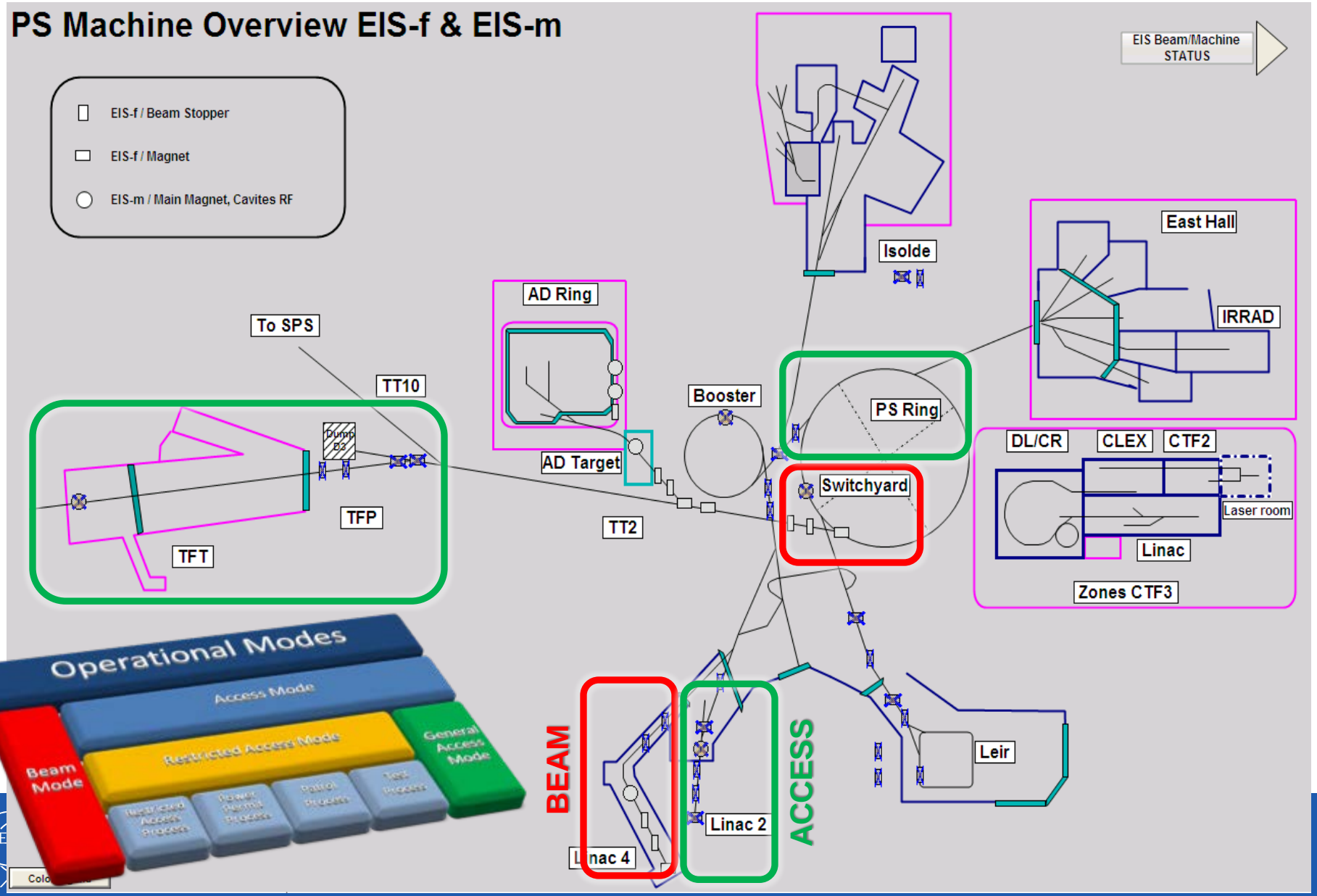
PS-PPS Project Scope



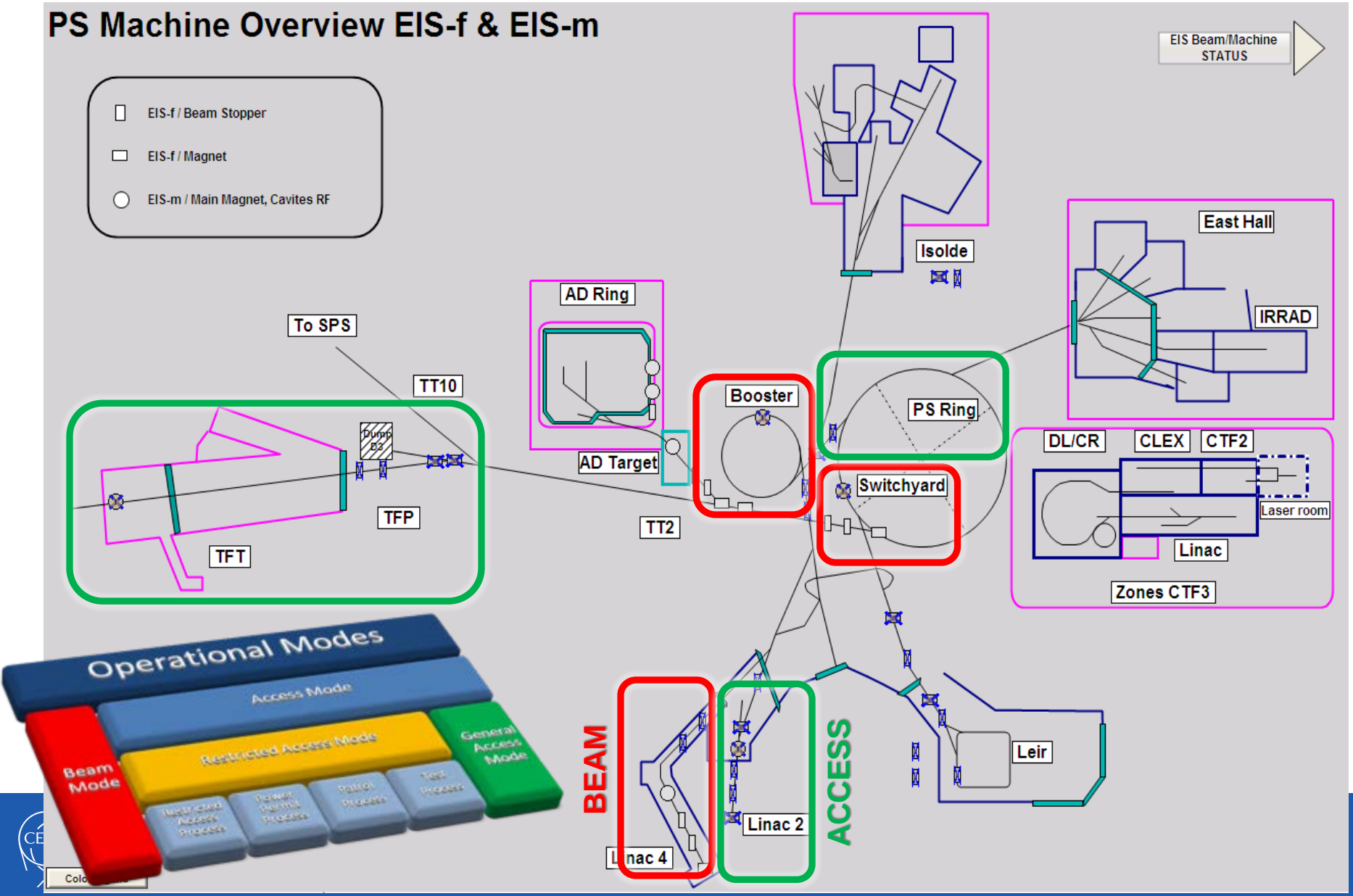
PS-PPS Project Scope



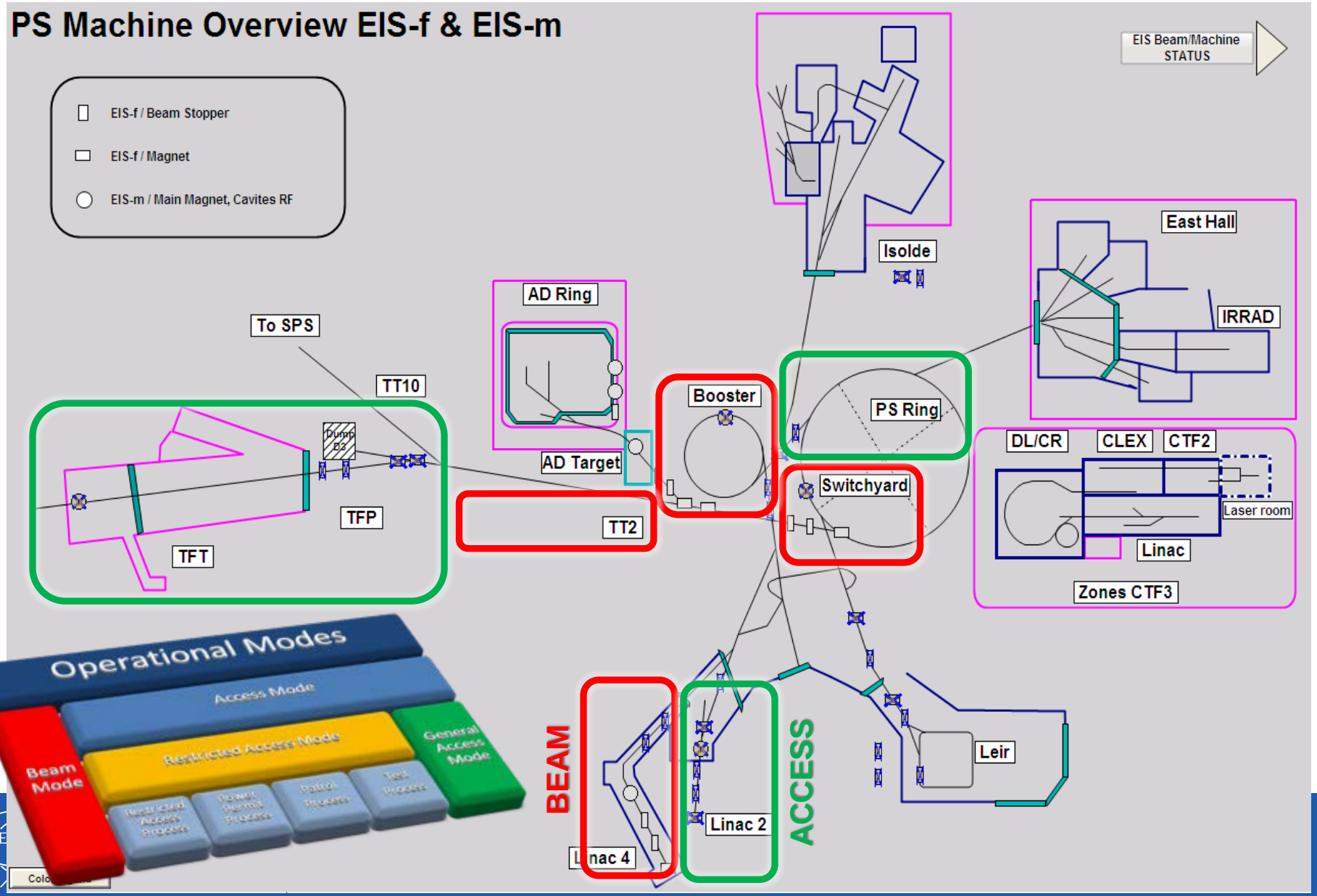
PS-PPS Project Scope



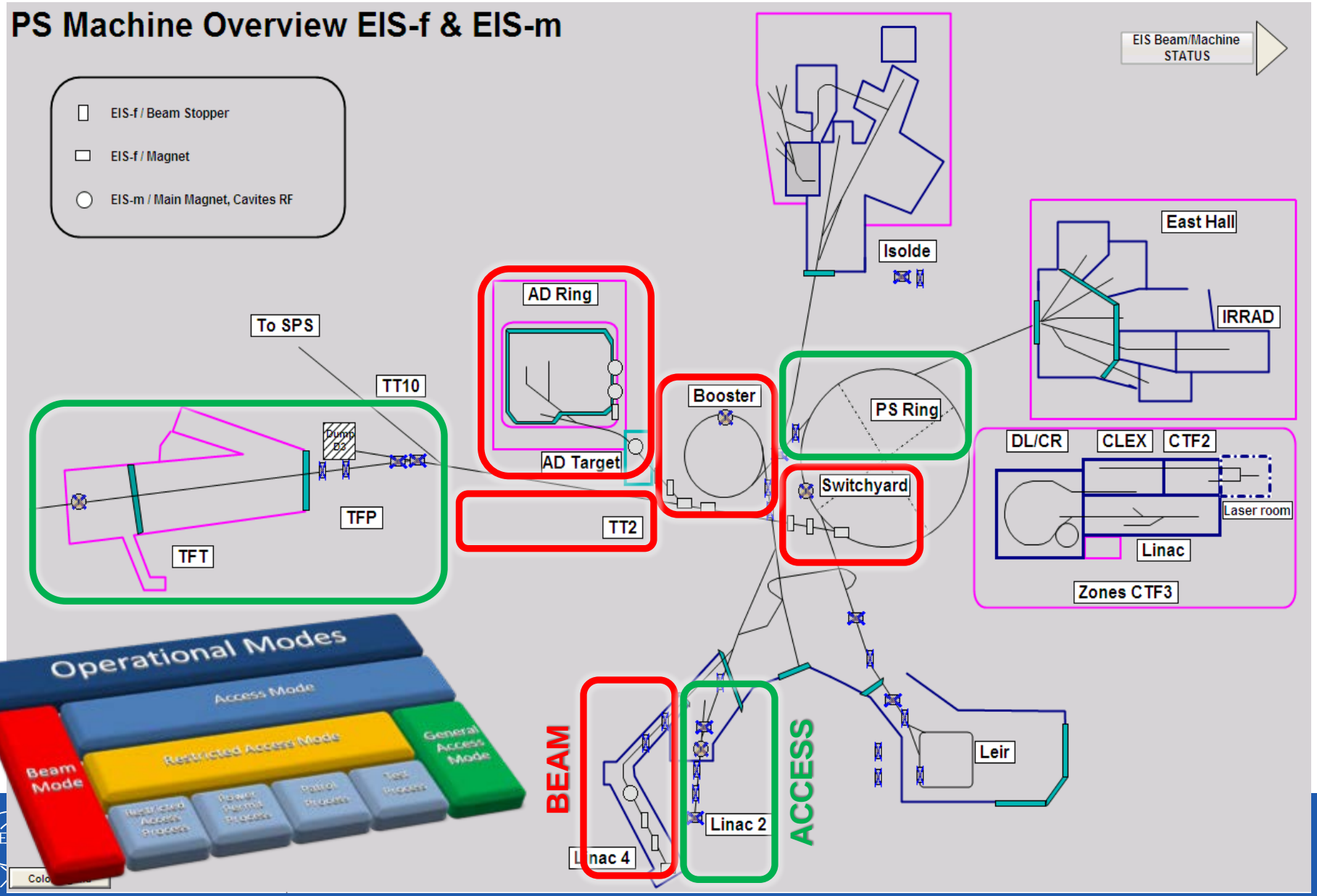
PS-PPS Project Scope



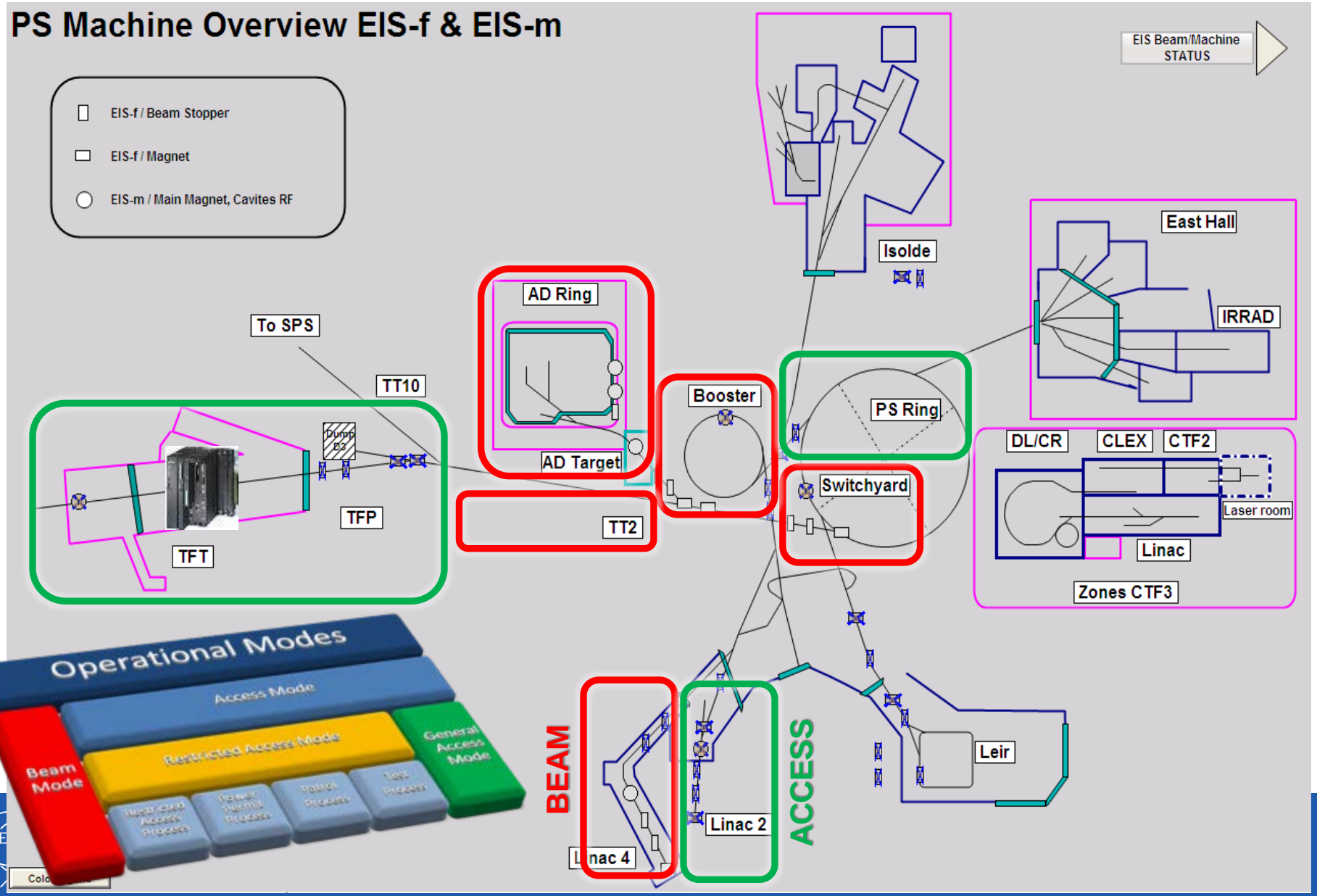
PS-PPS Project Scope



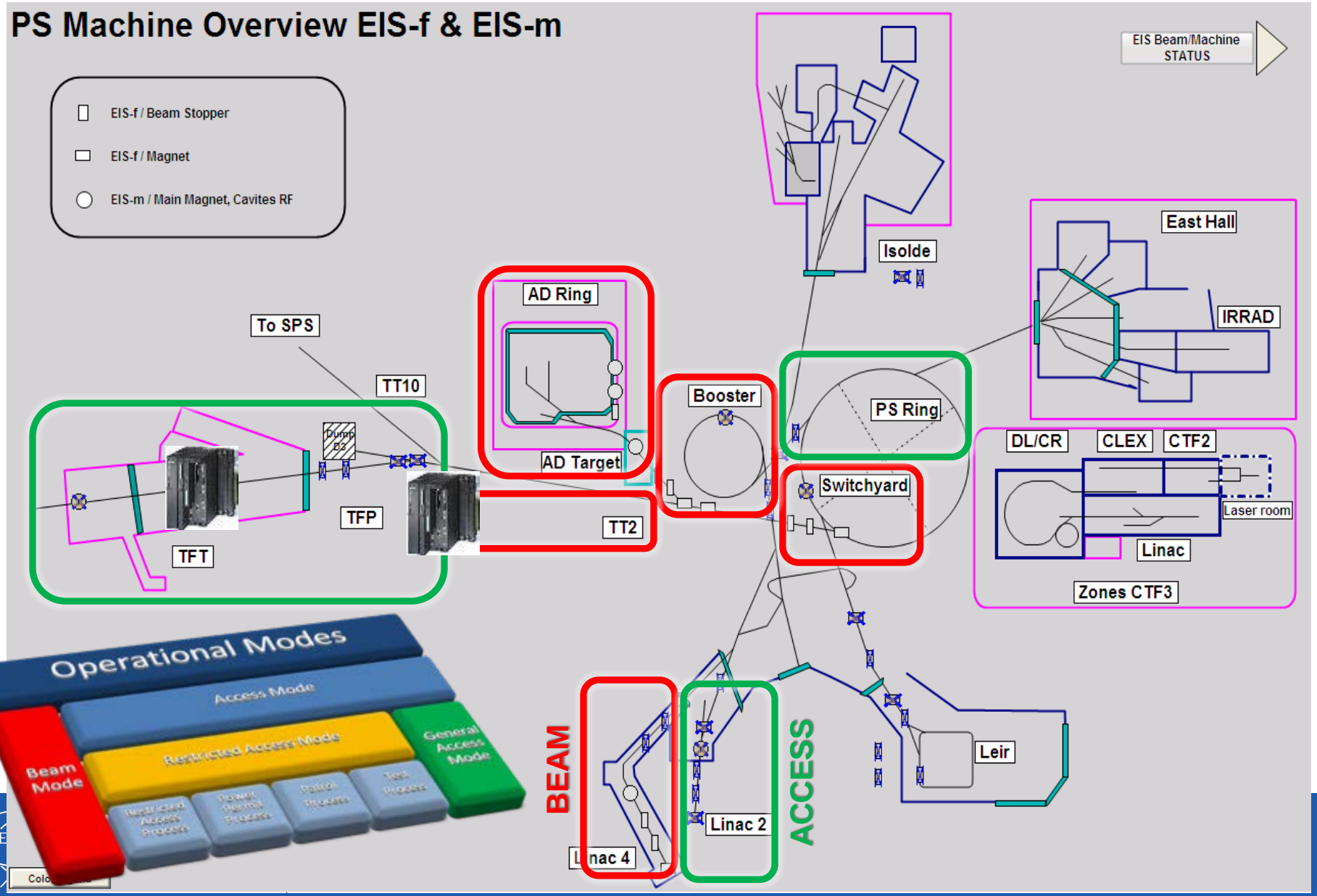
PS-PPS Project Scope



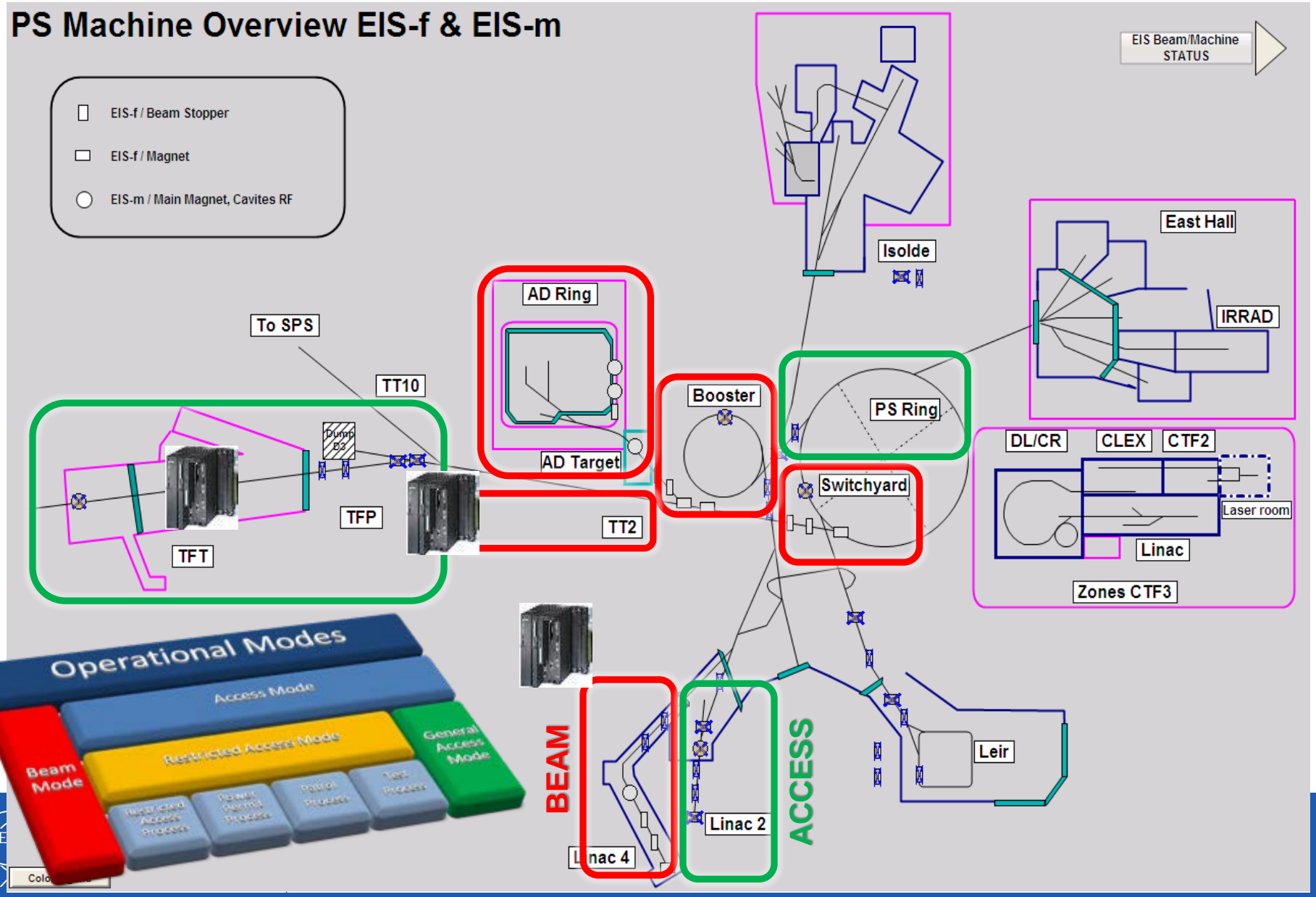
PS-PPS Project Scope



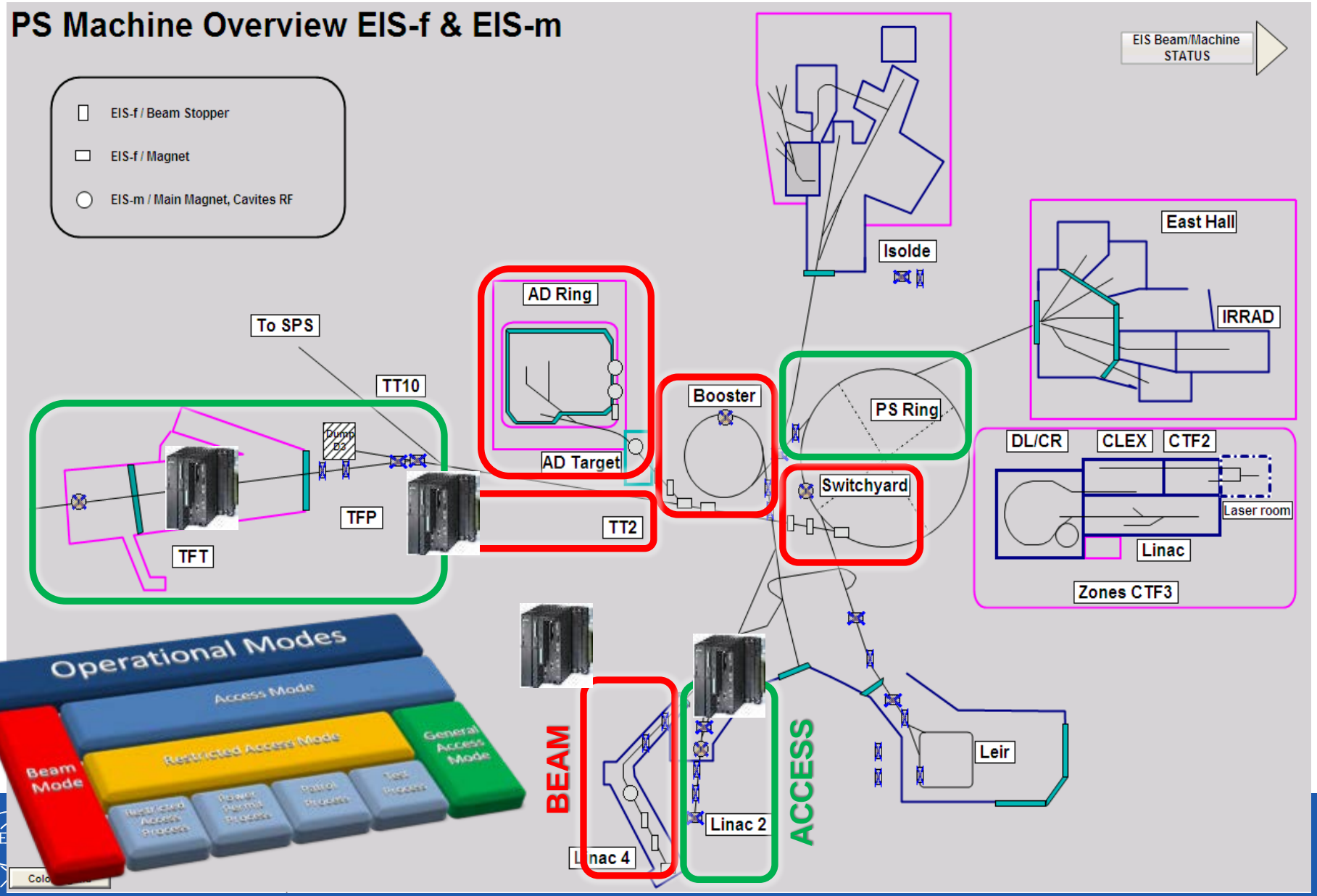
PS-PPS Project Scope



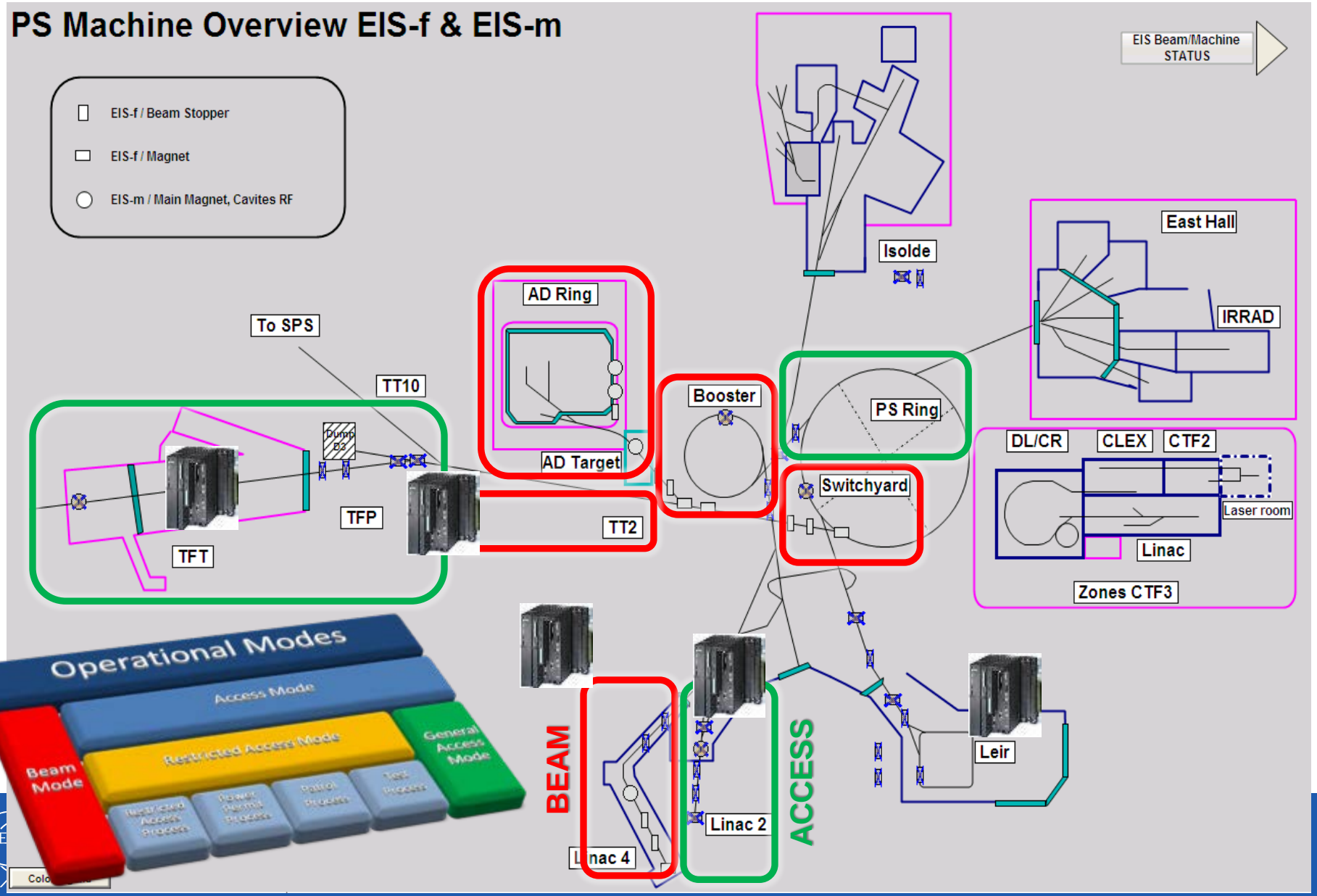
PS-PPS Project Scope



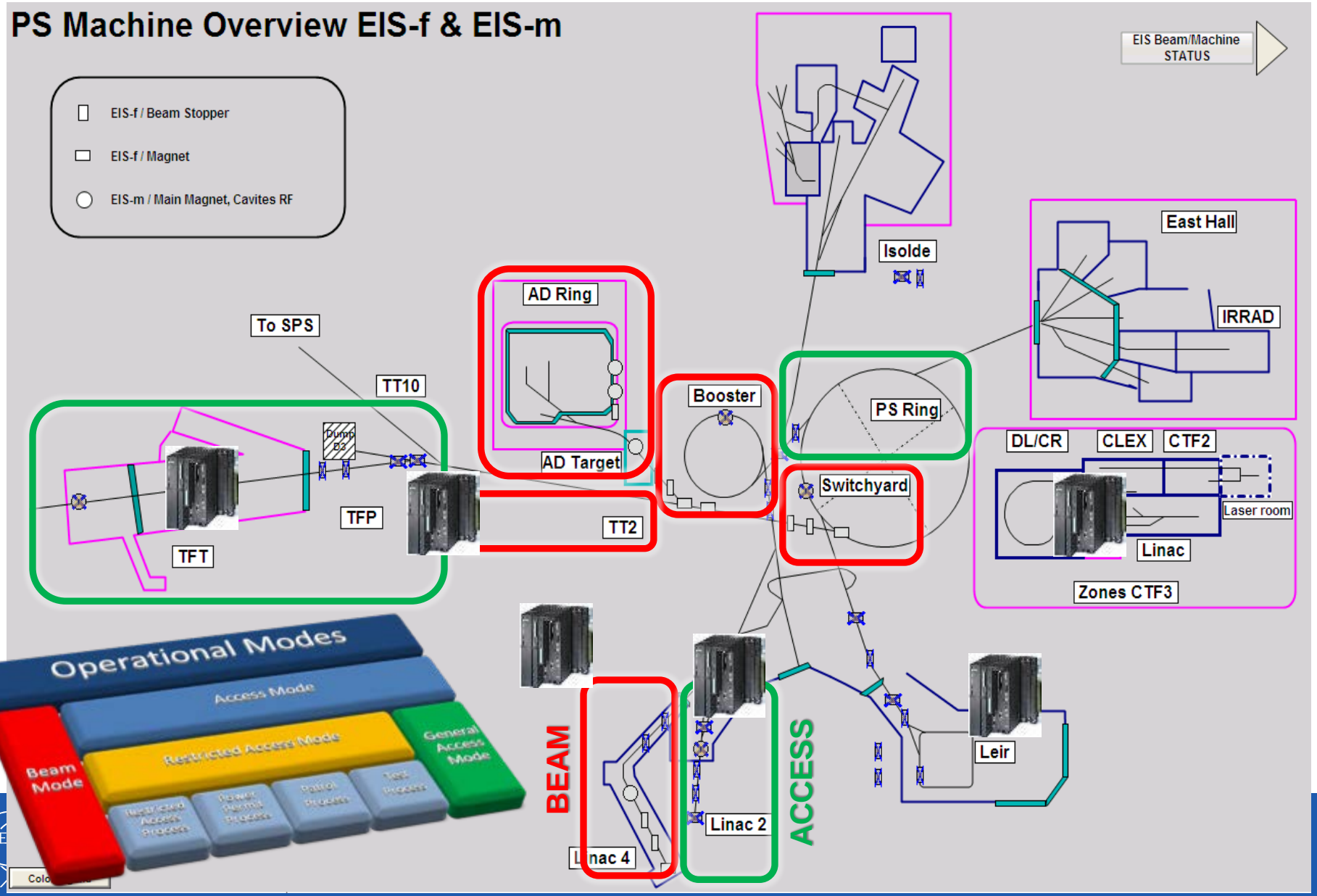
PS-PPS Project Scope



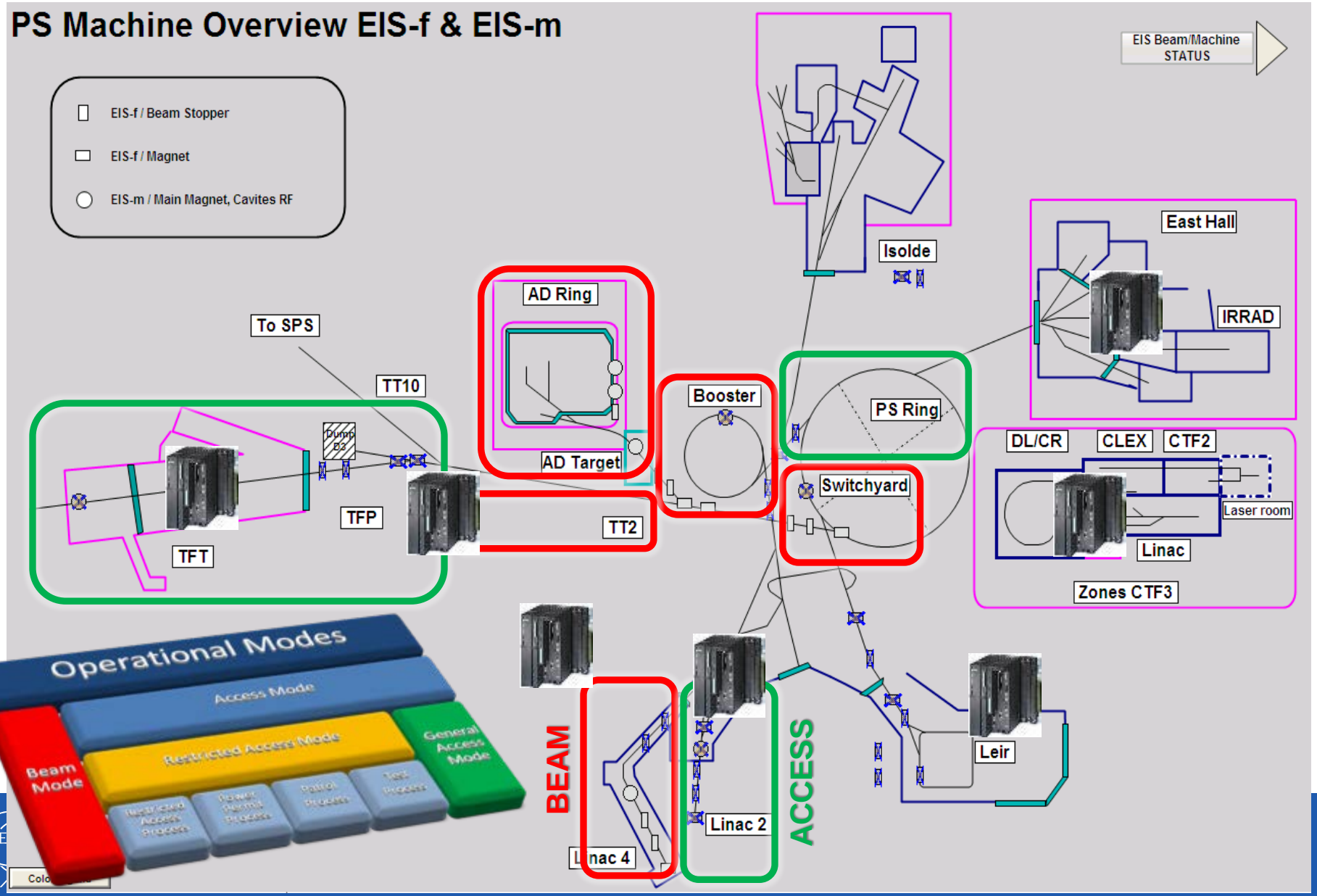
PS-PPS Project Scope



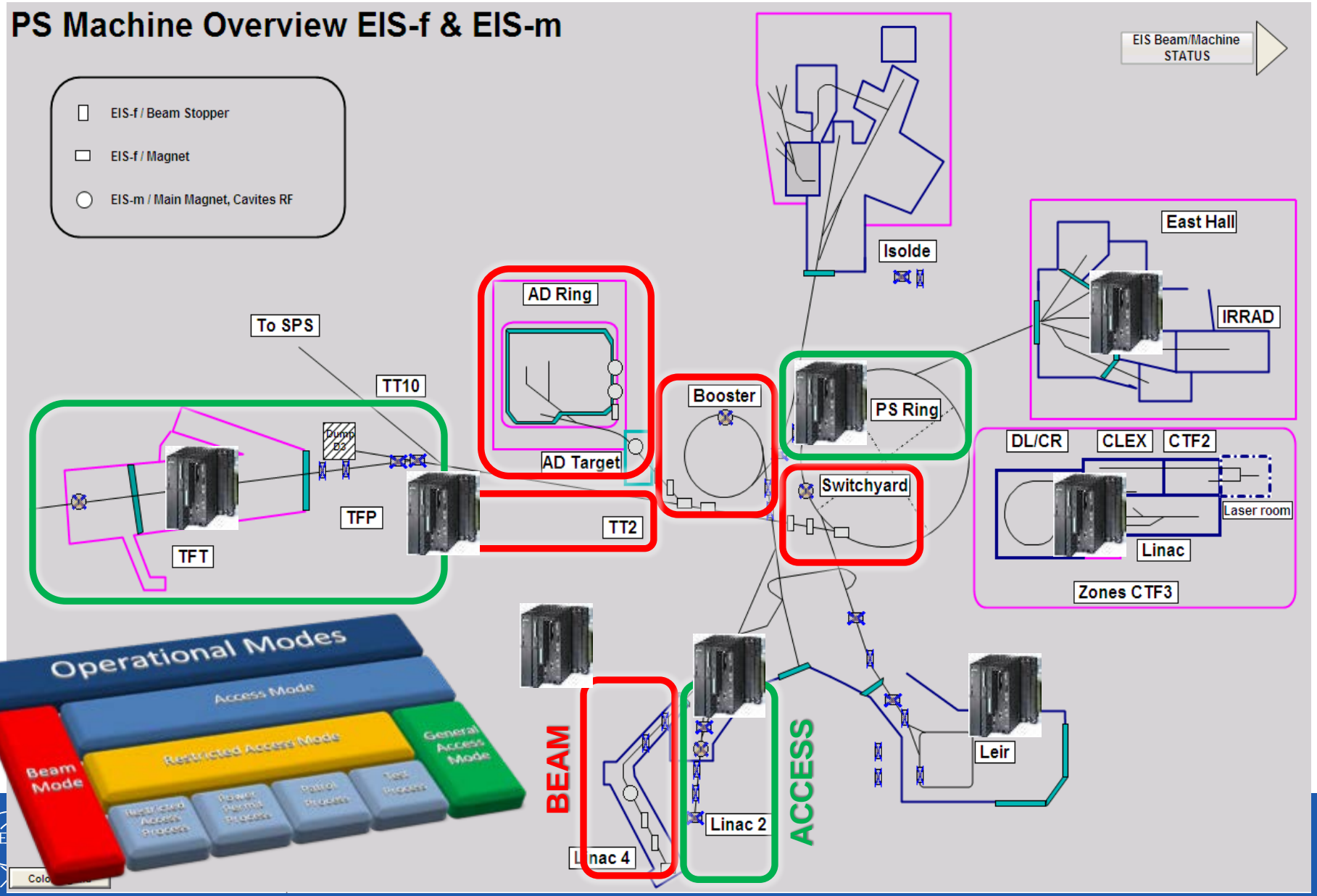
PS-PPS Project Scope



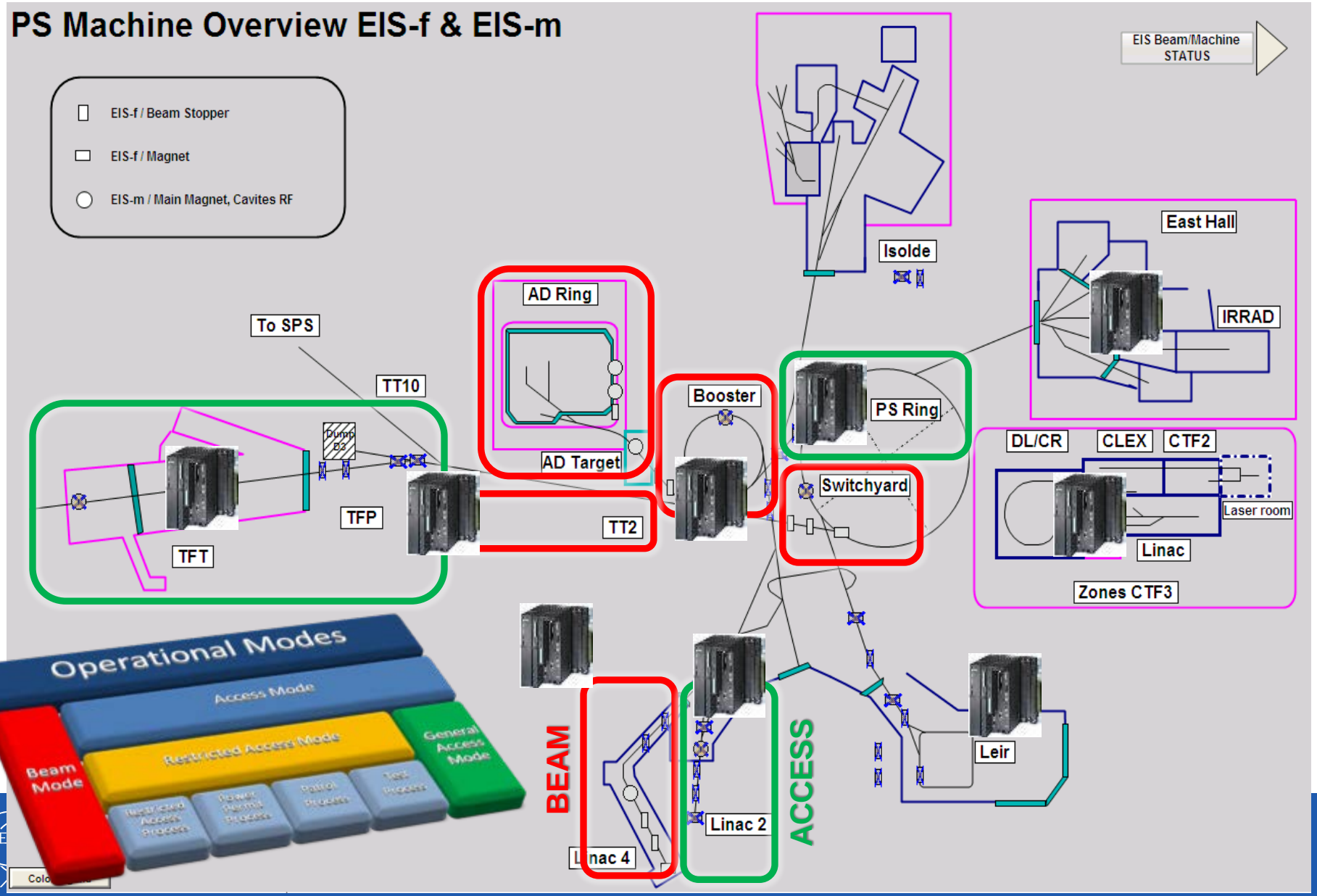
PS-PPS Project Scope



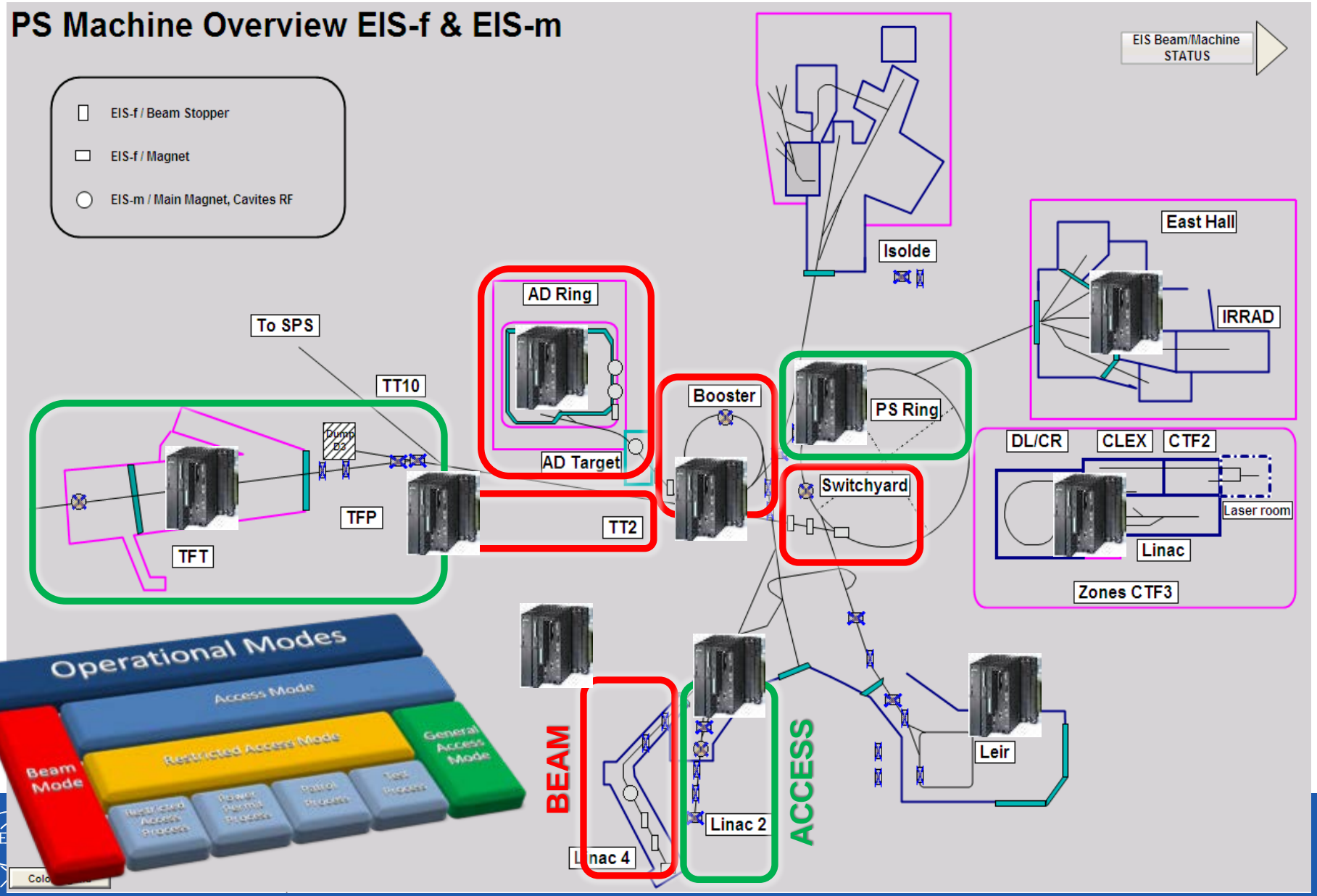
PS-PPS Project Scope



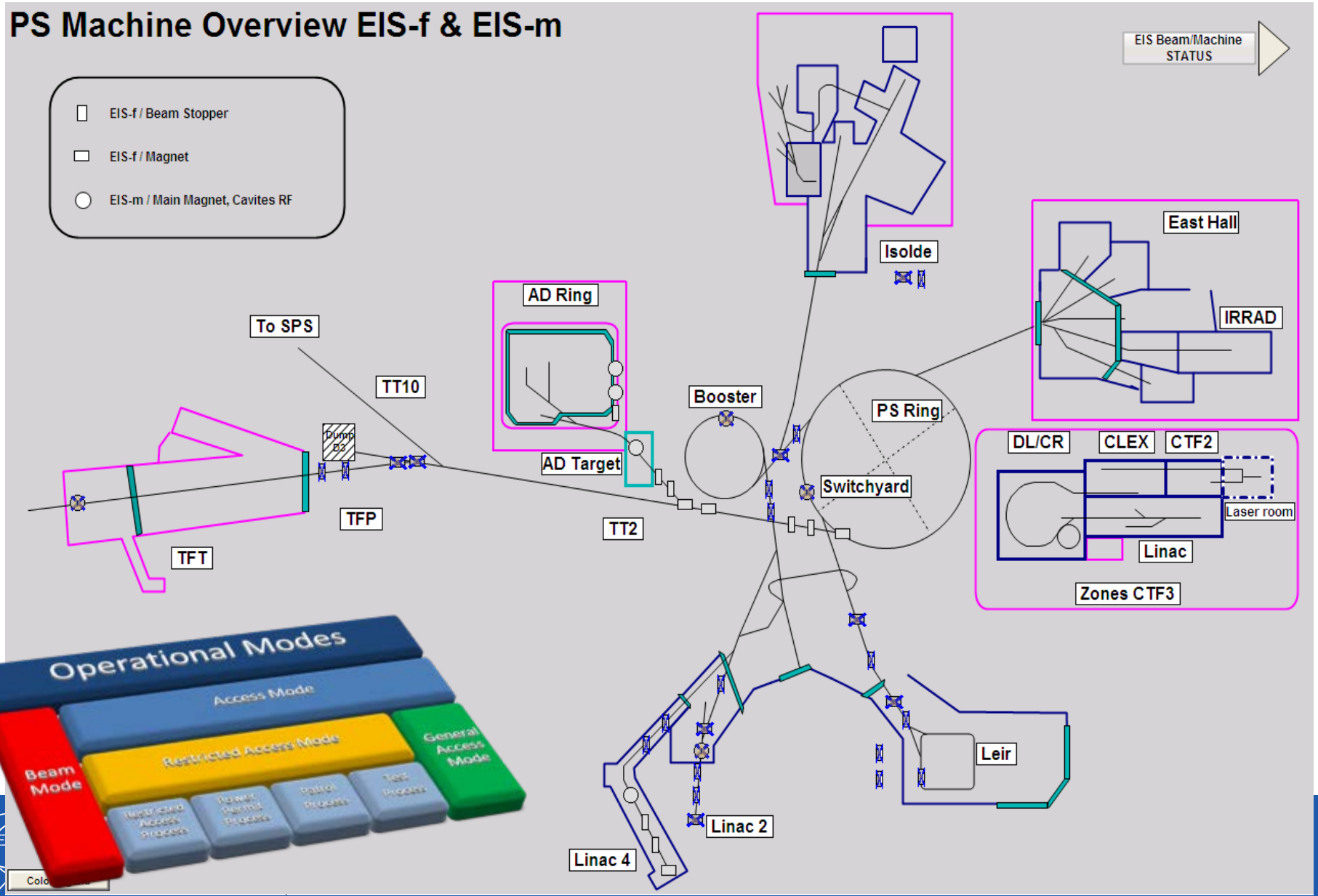
PS-PPS Project Scope



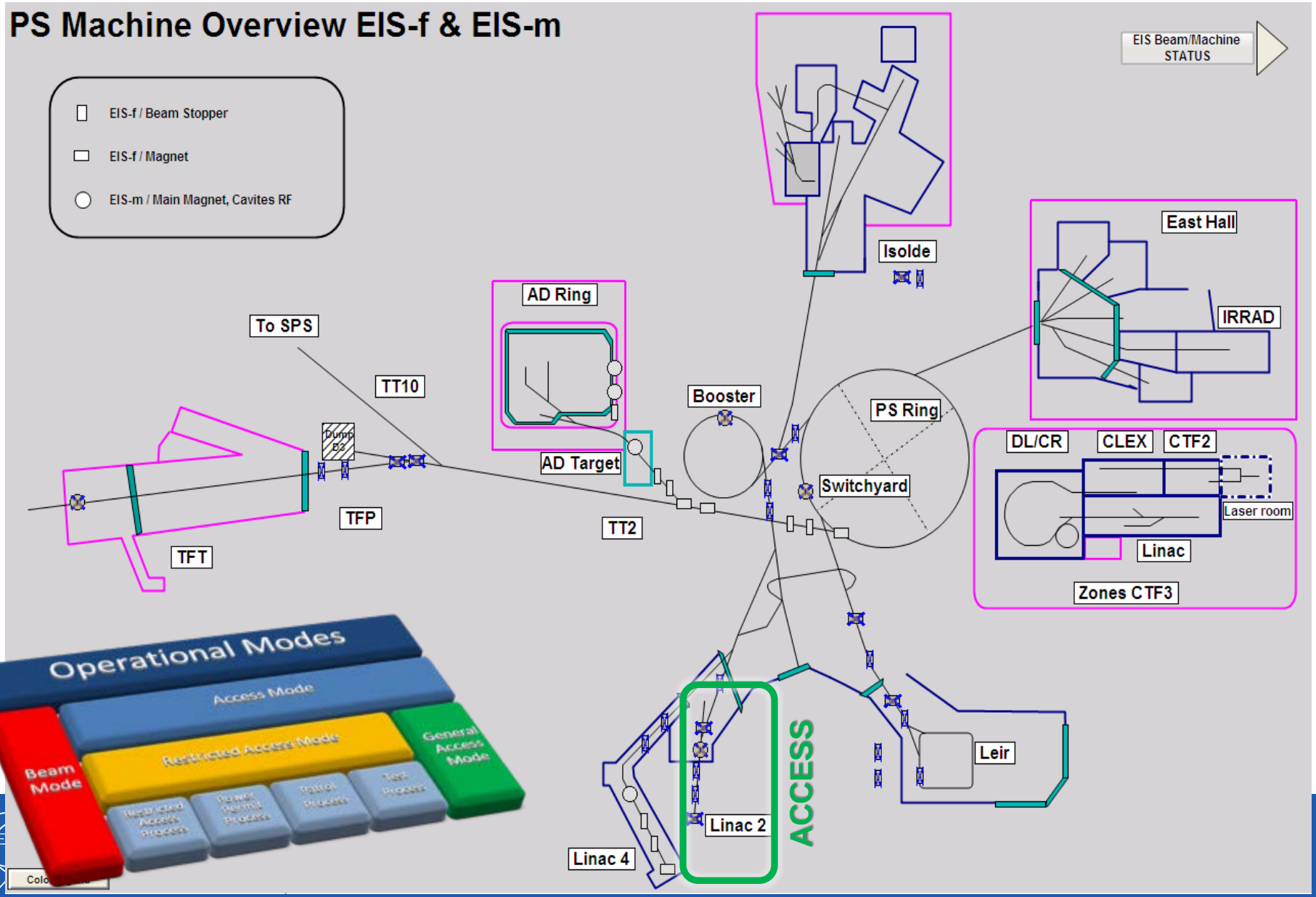
PS-PPS Project Scope



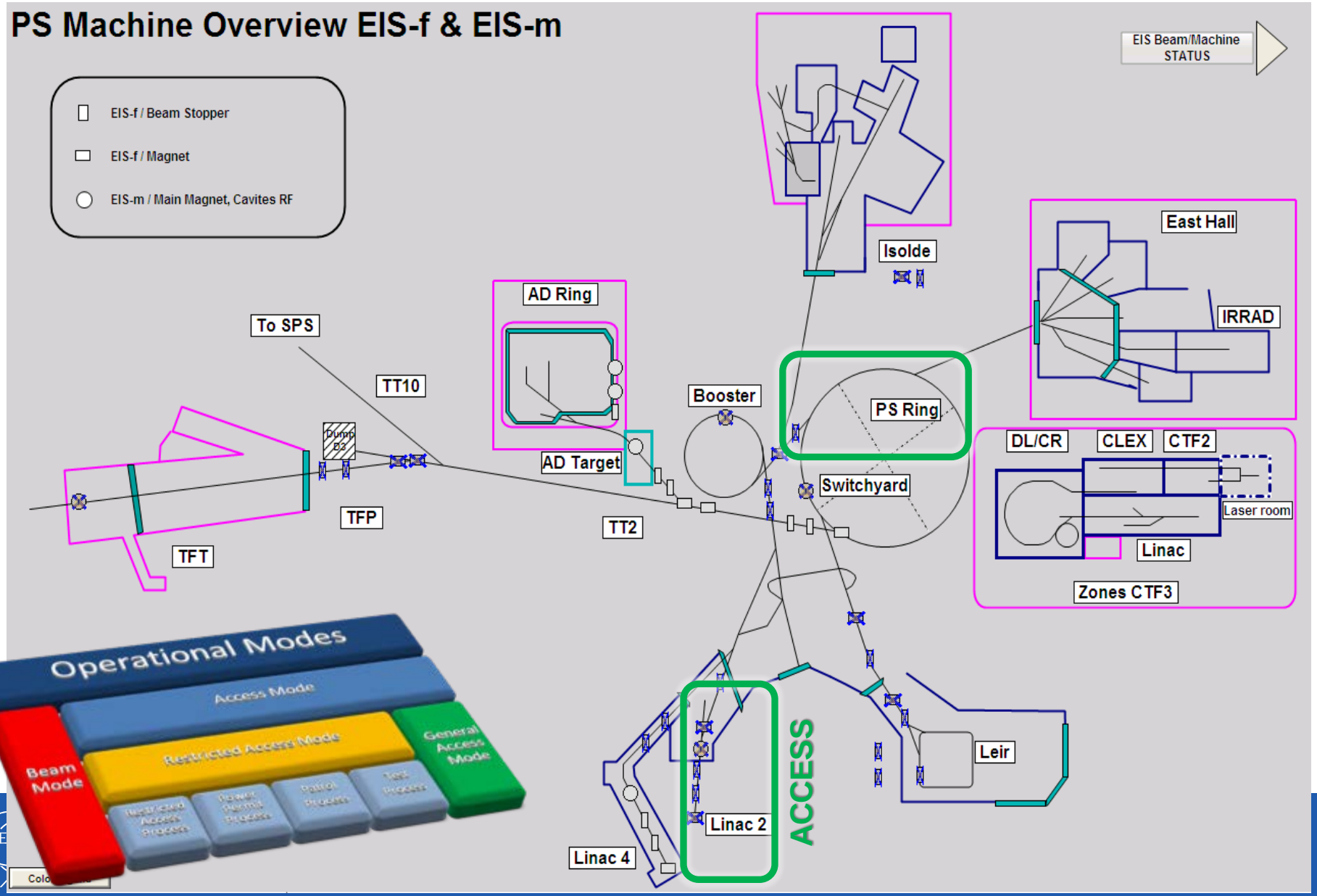
PS-PPS Project Scope



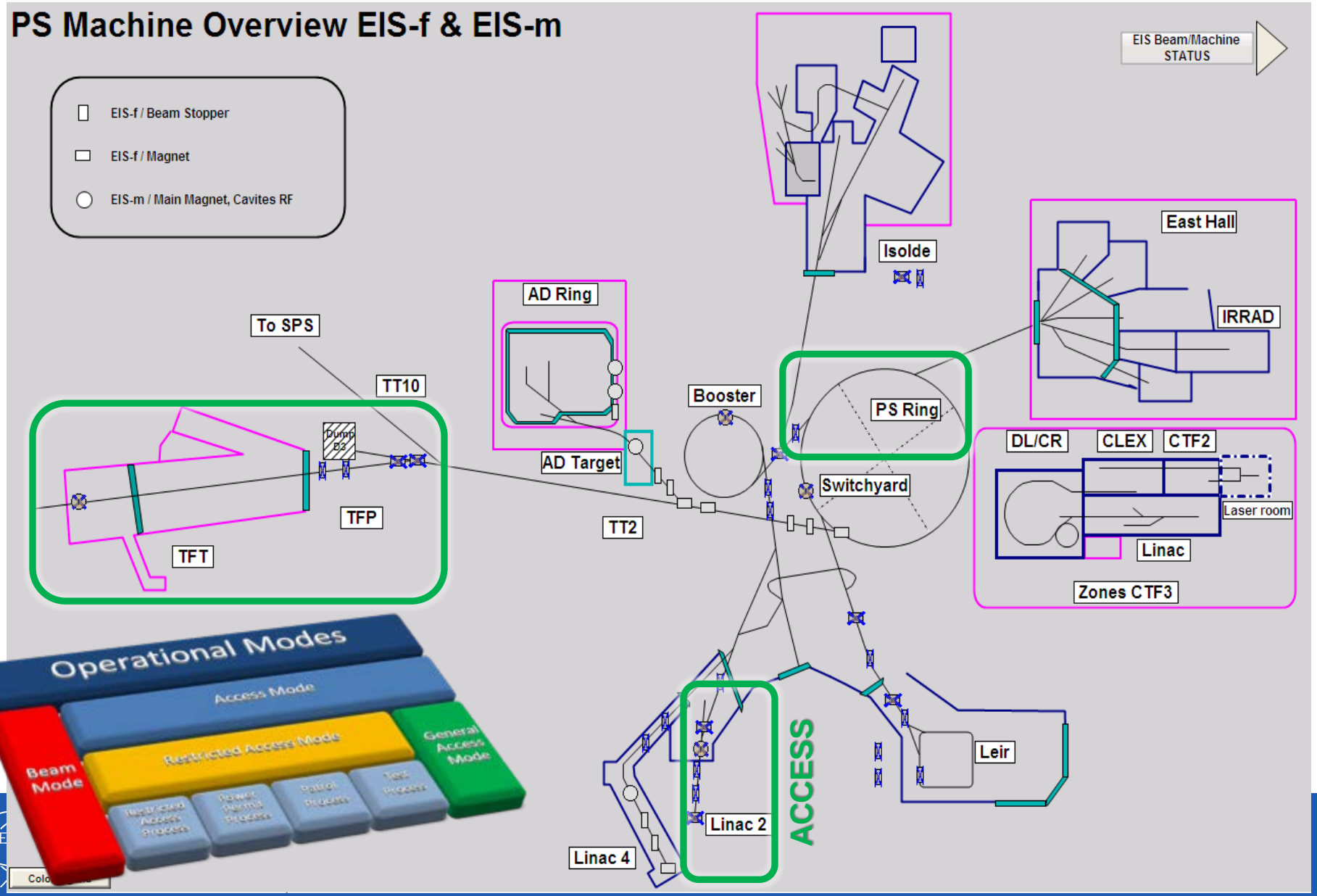
PS-PPS Project Scope



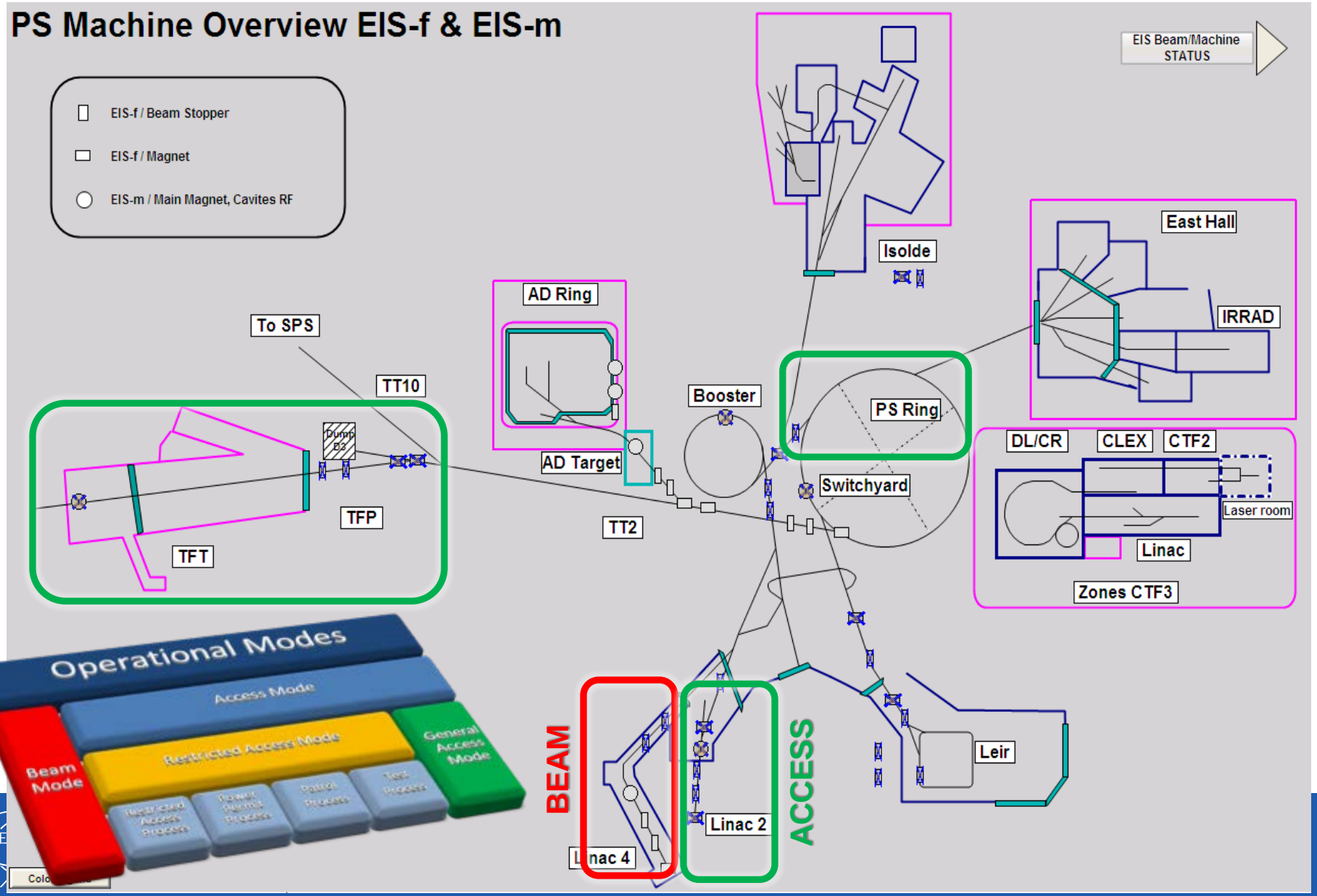
PS-PPS Project Scope



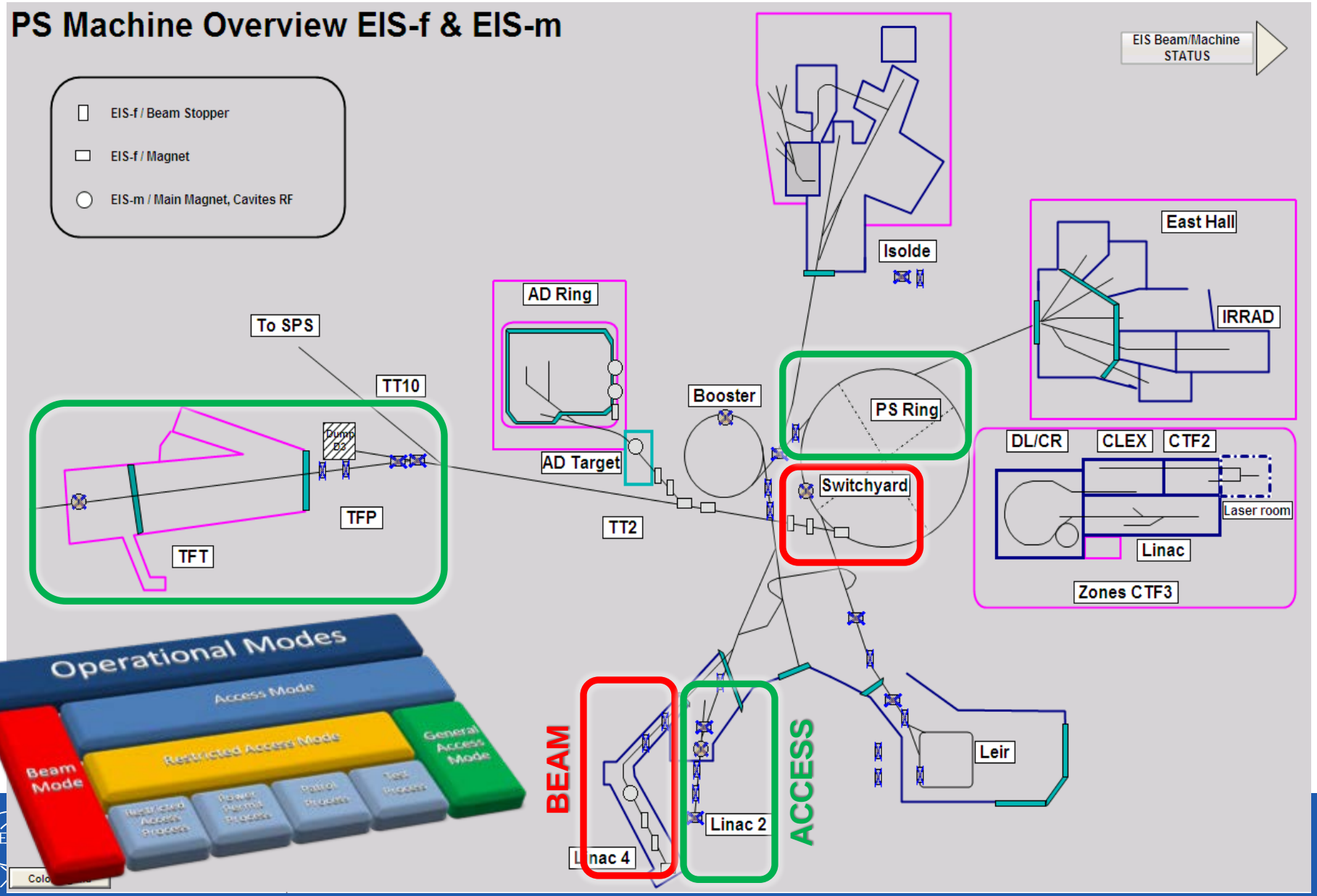
PS-PPS Project Scope



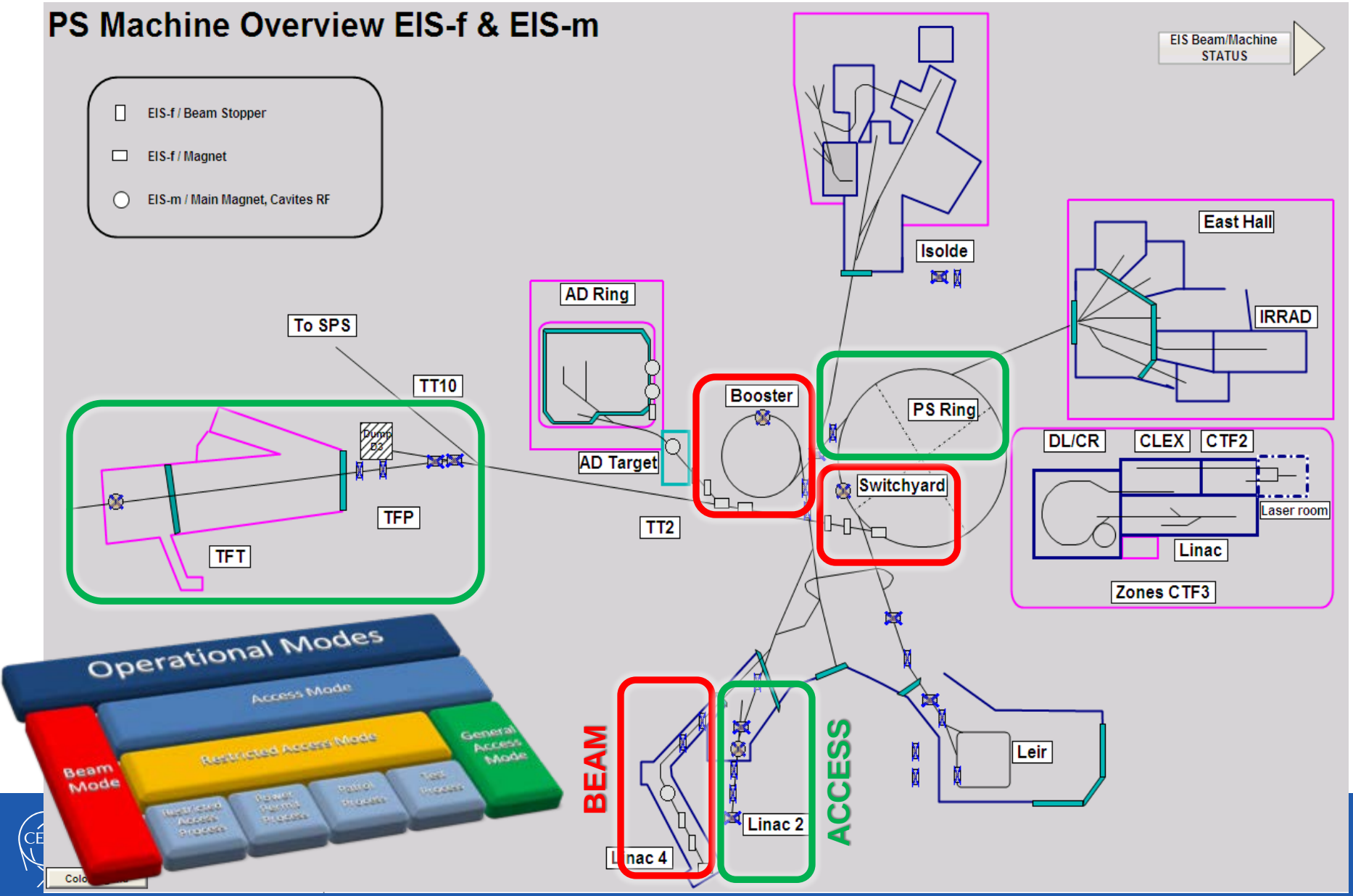
PS-PPS Project Scope



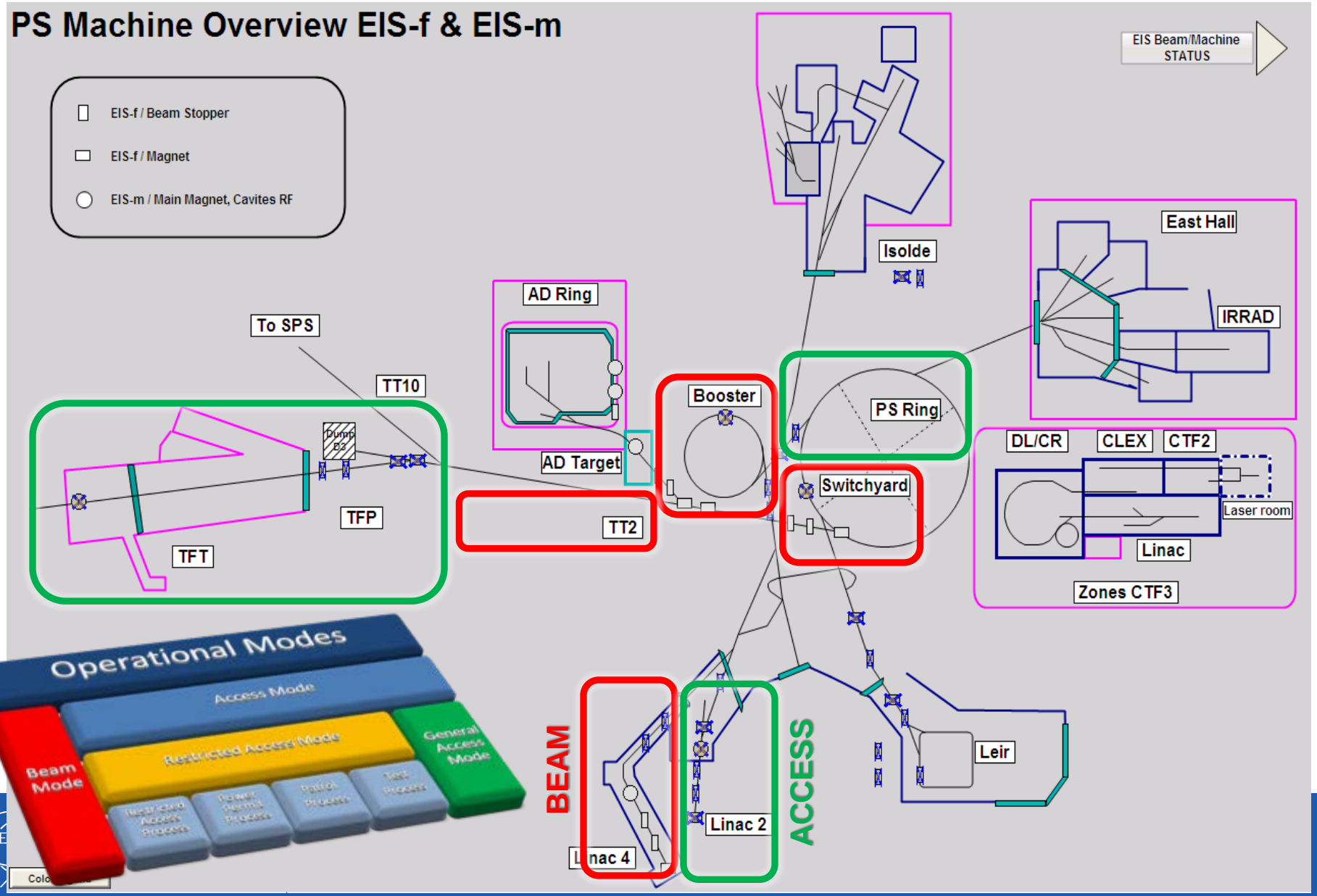
PS-PPS Project Scope



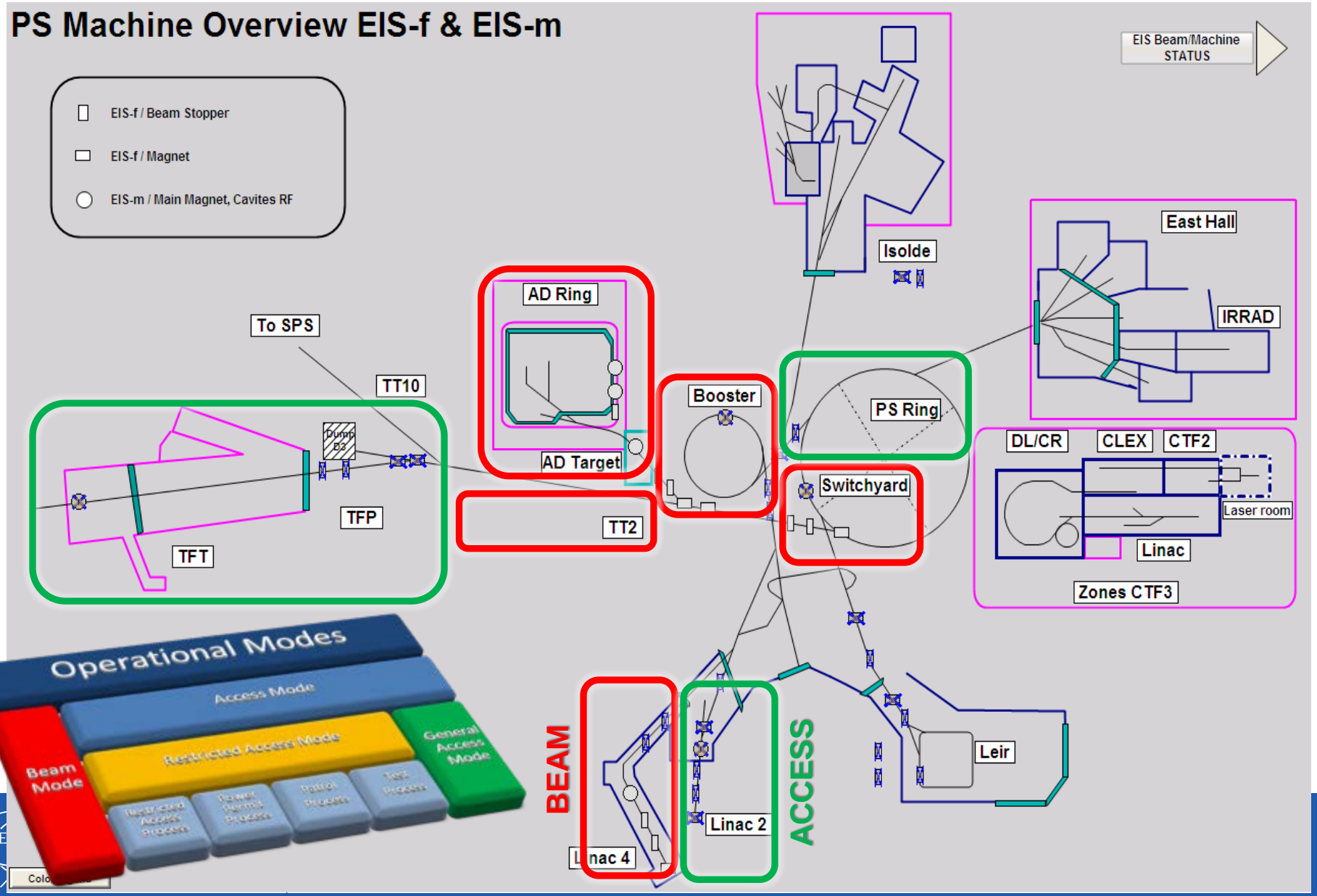
PS-PPS Project Scope



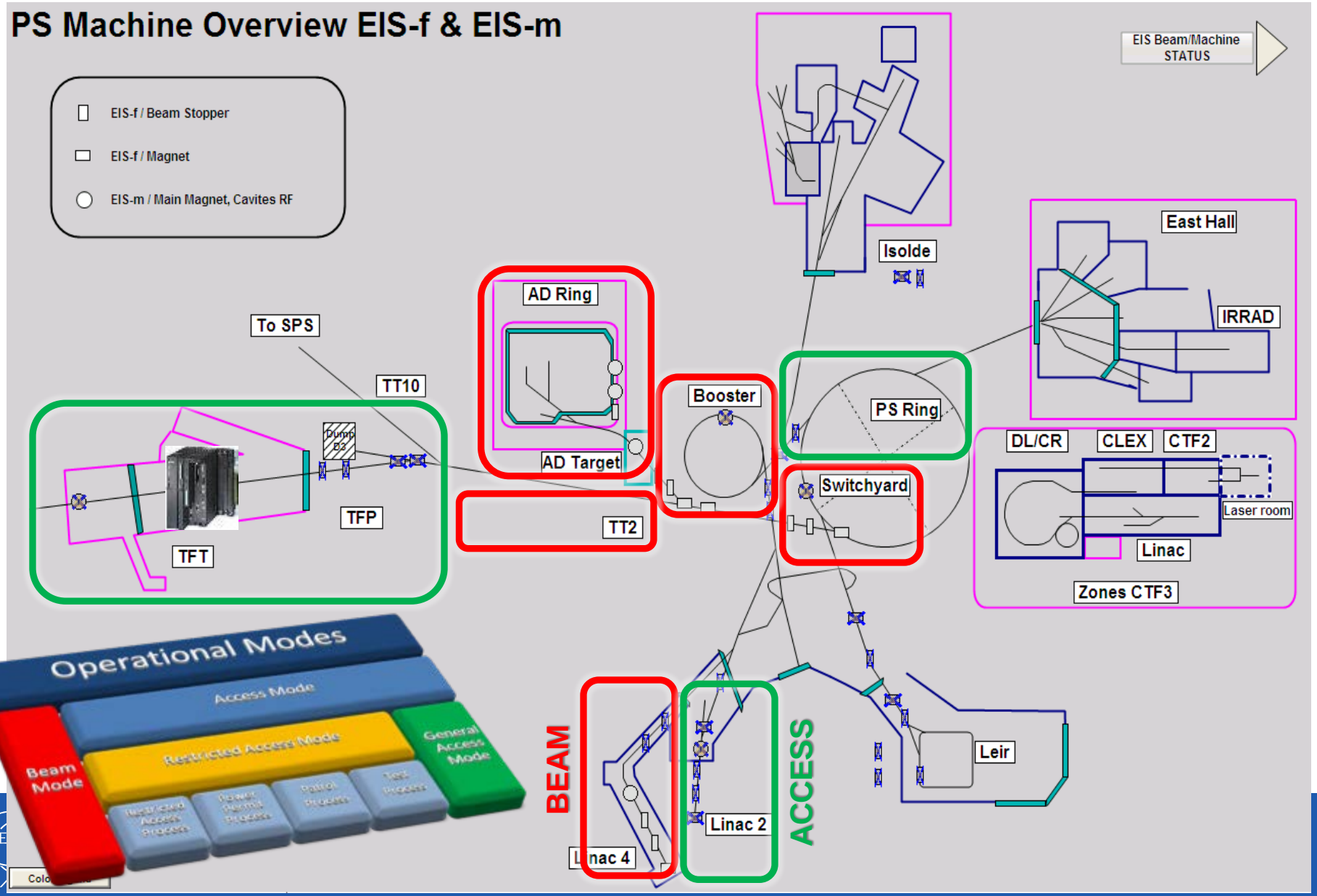
PS-PPS Project Scope



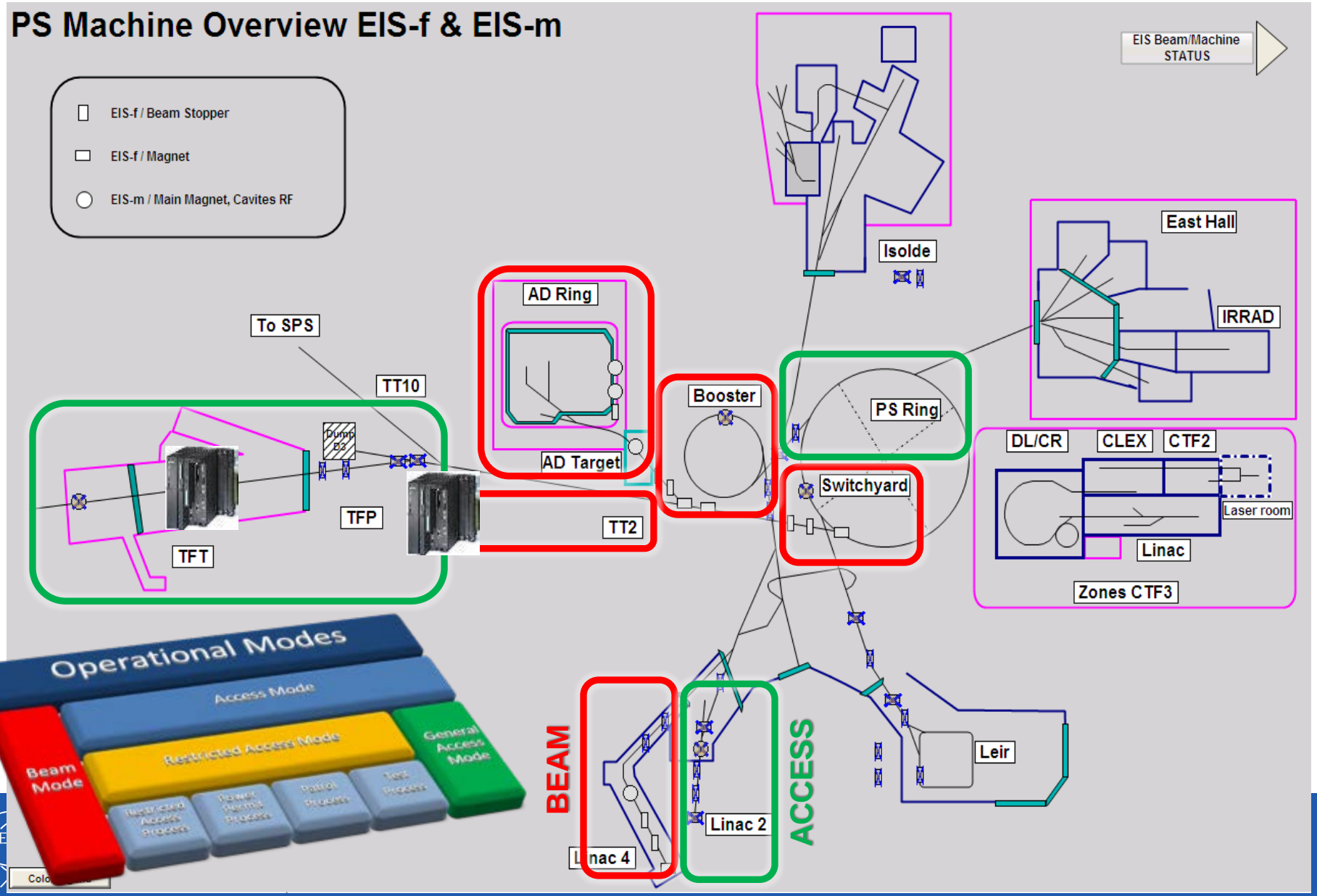
PS-PPS Project Scope



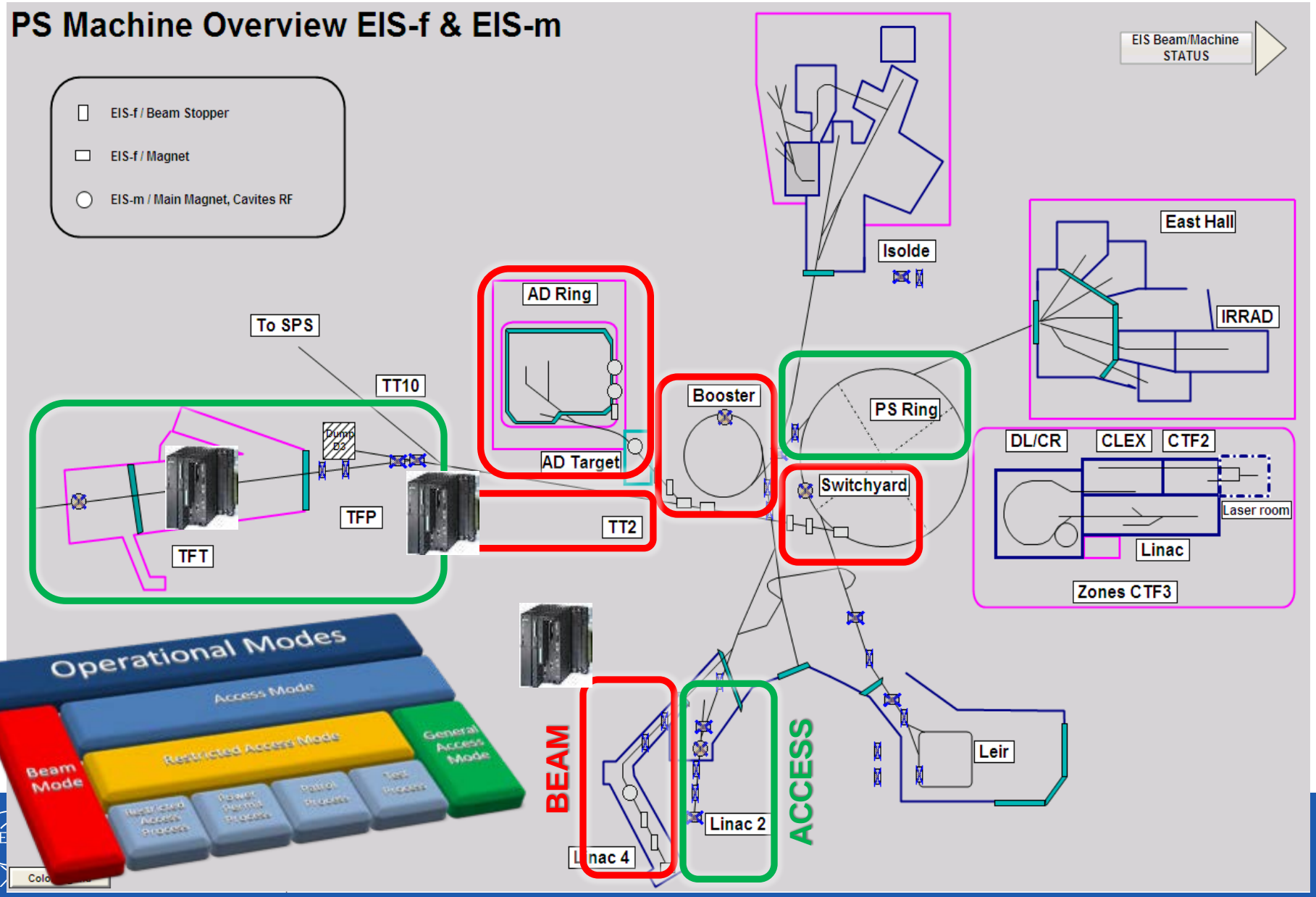
PS-PPS Project Scope



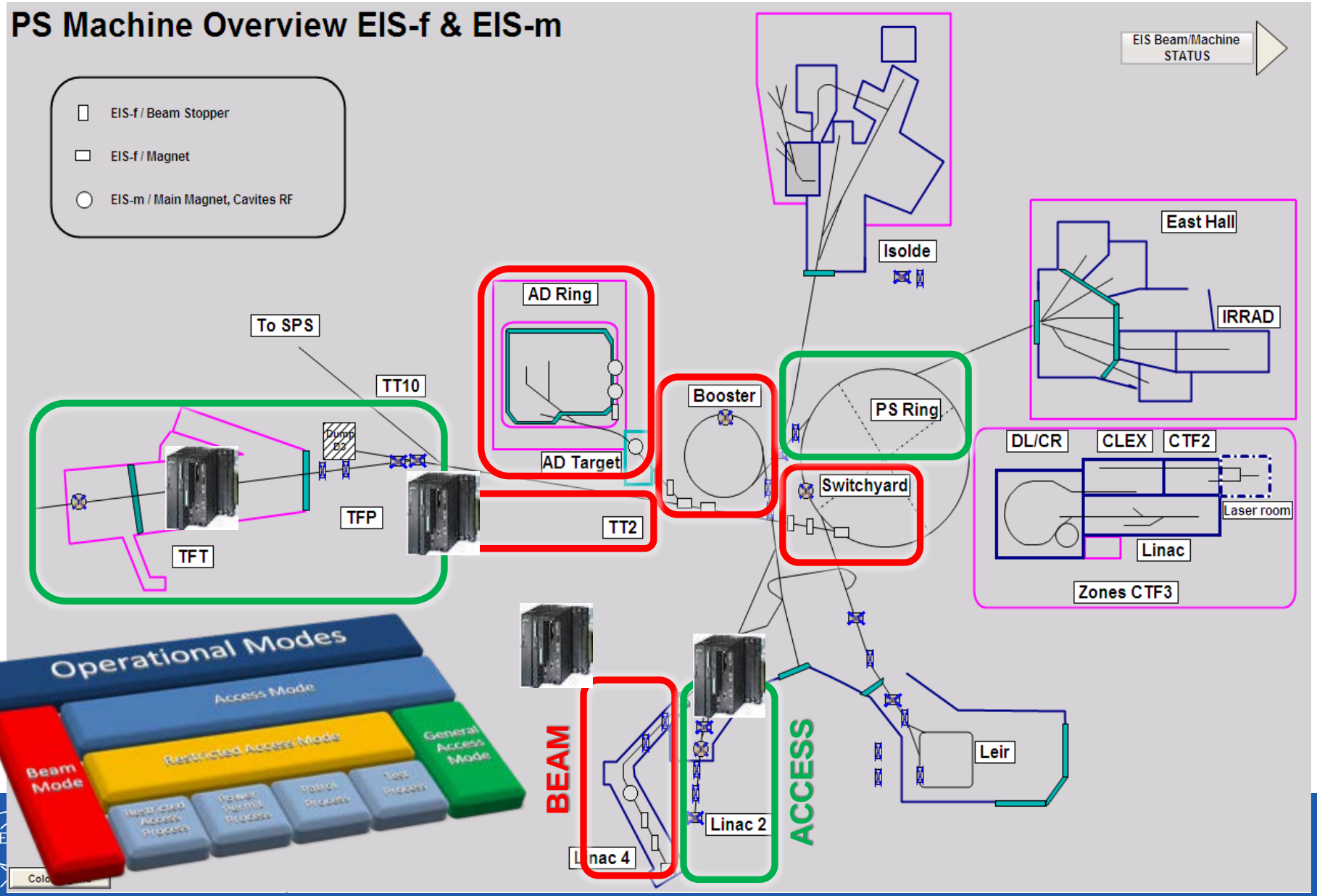
PS-PPS Project Scope



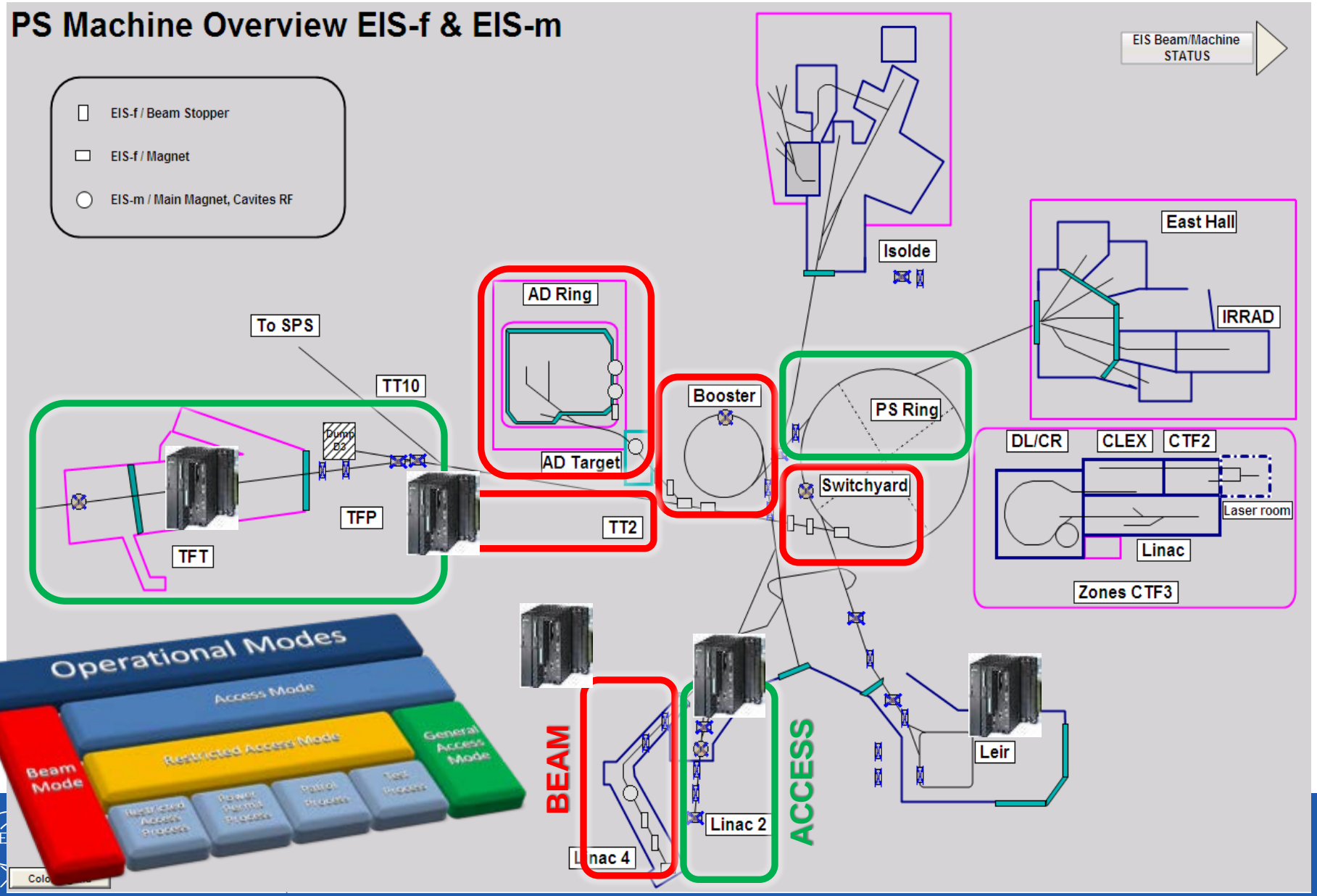
PS-PPS Project Scope



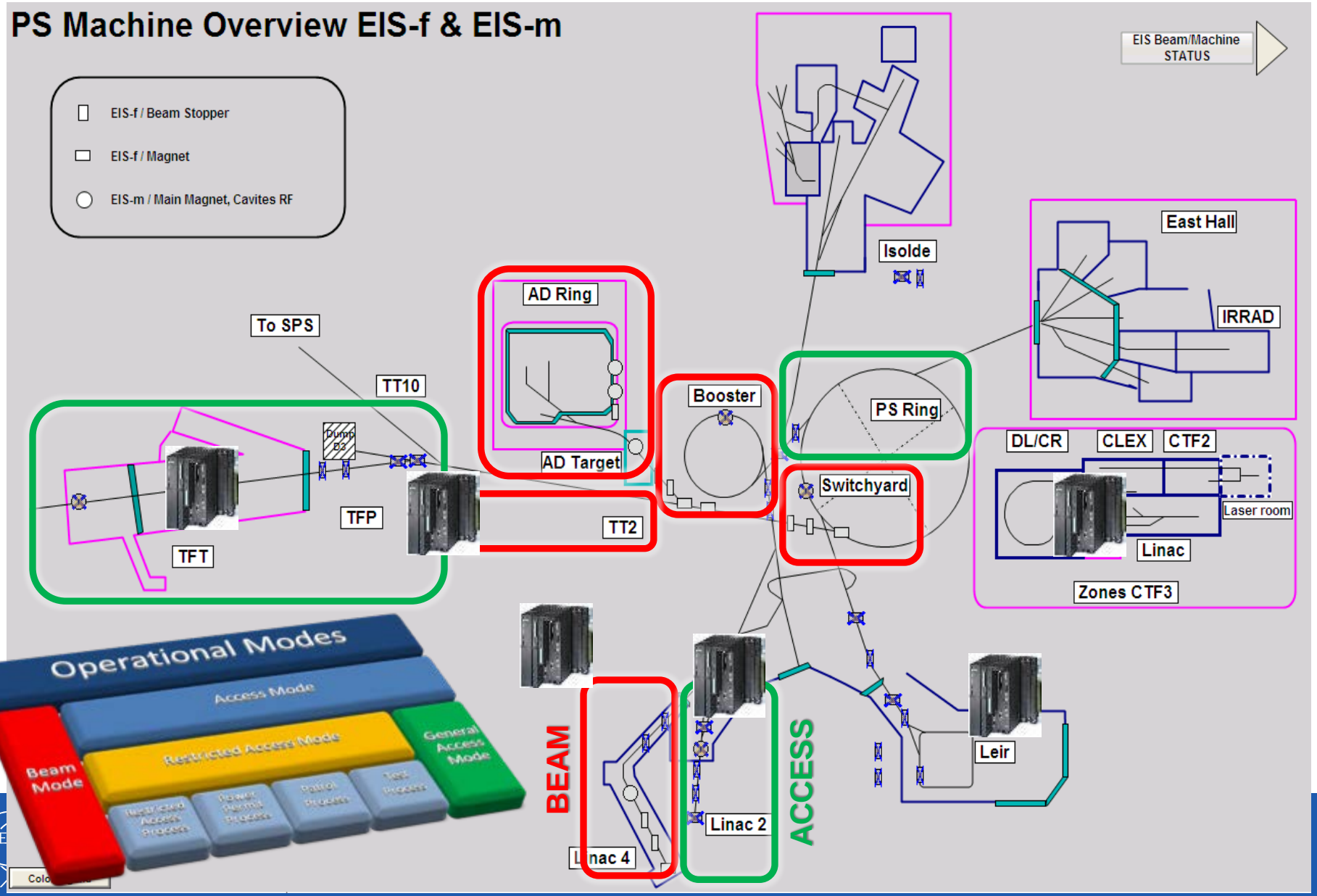
PS-PPS Project Scope



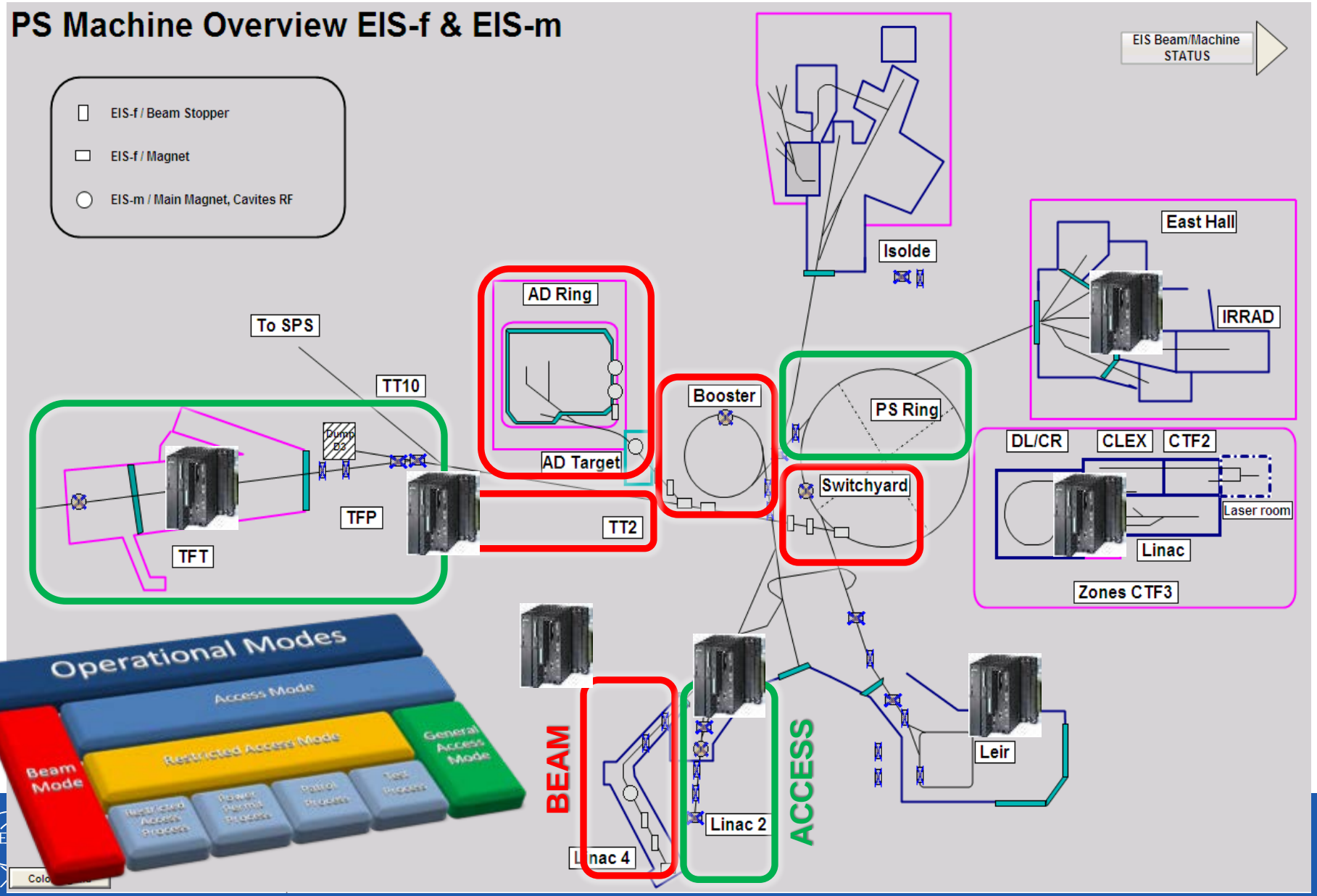
PS-PPS Project Scope



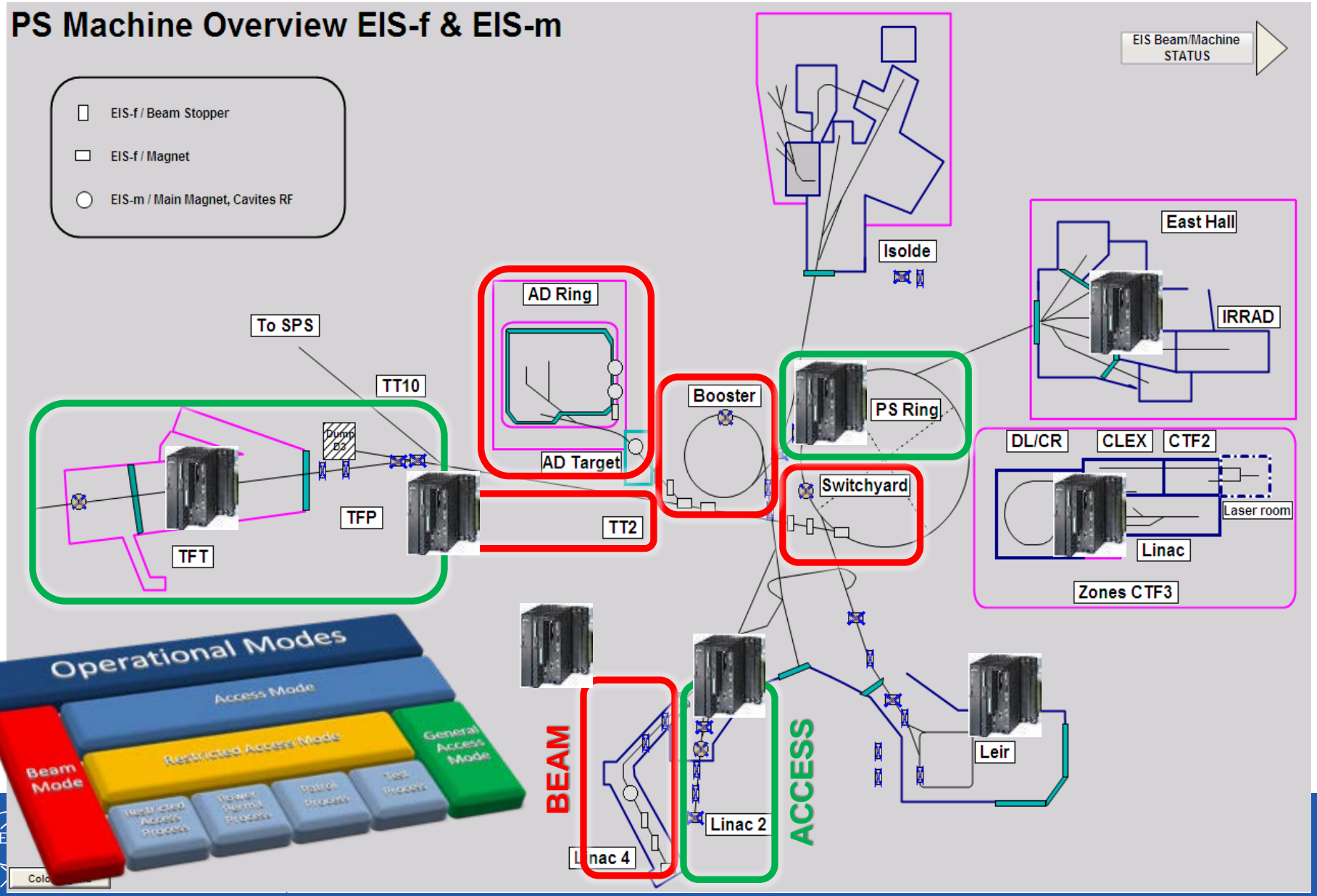
PS-PPS Project Scope



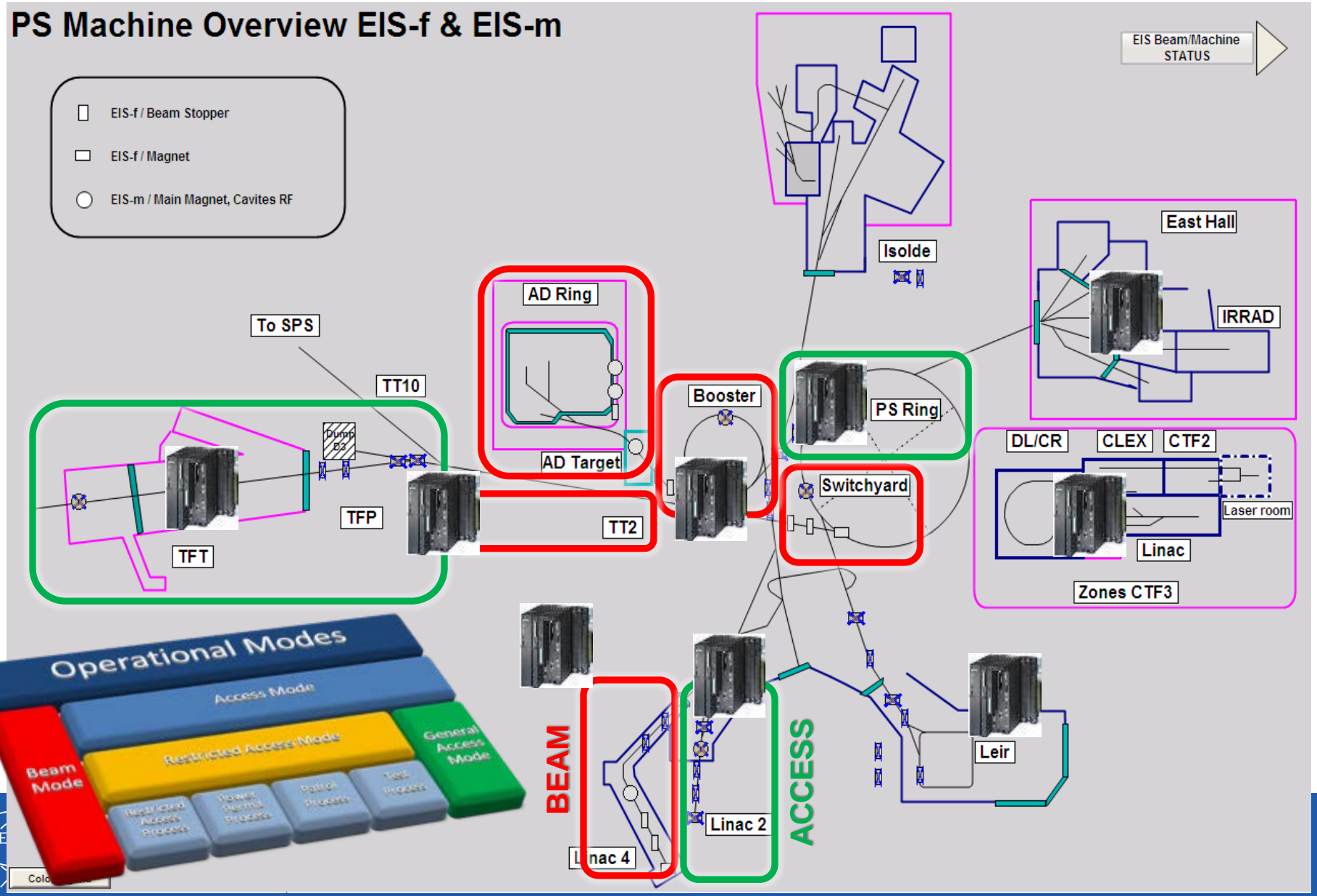
PS-PPS Project Scope



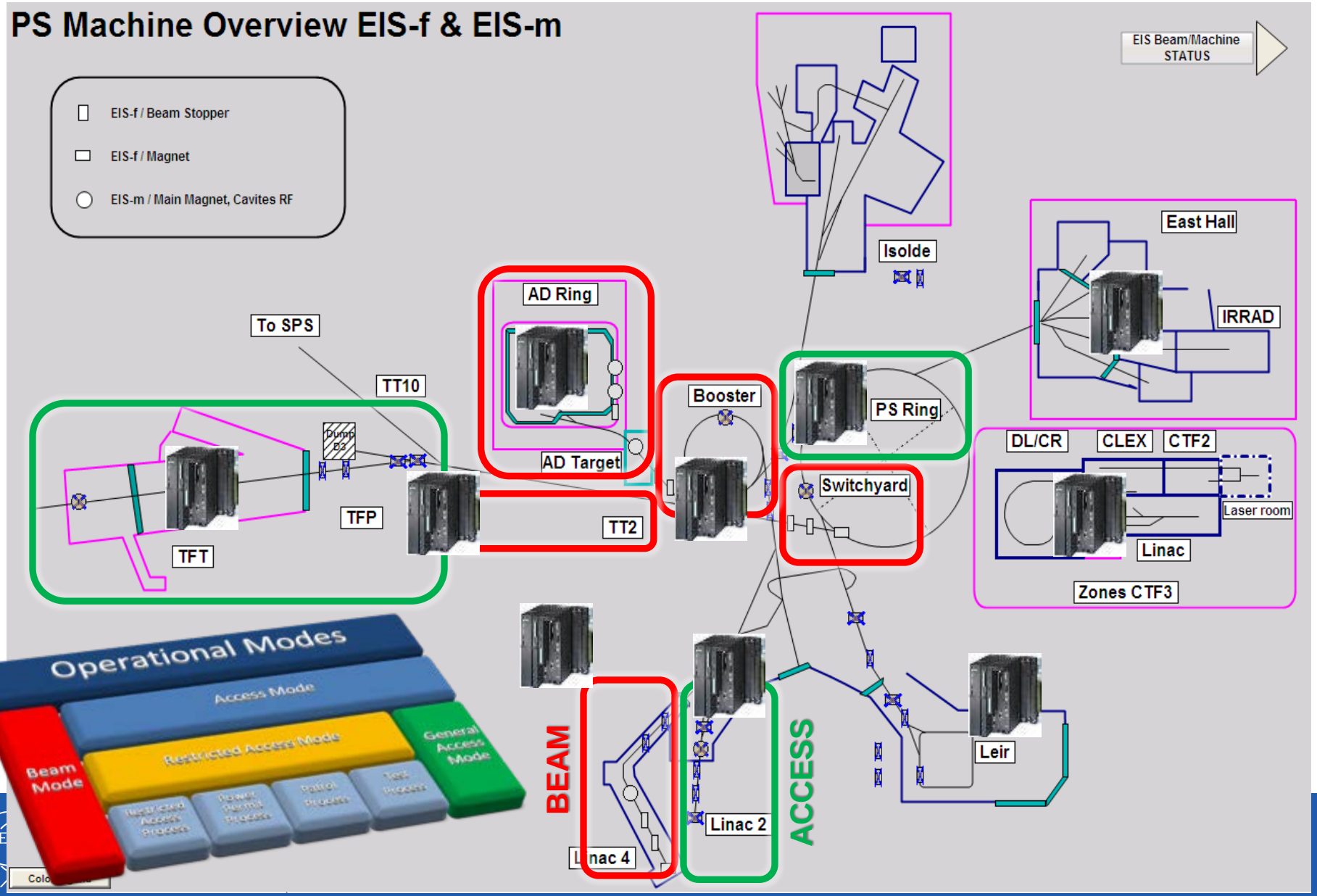
PS-PPS Project Scope



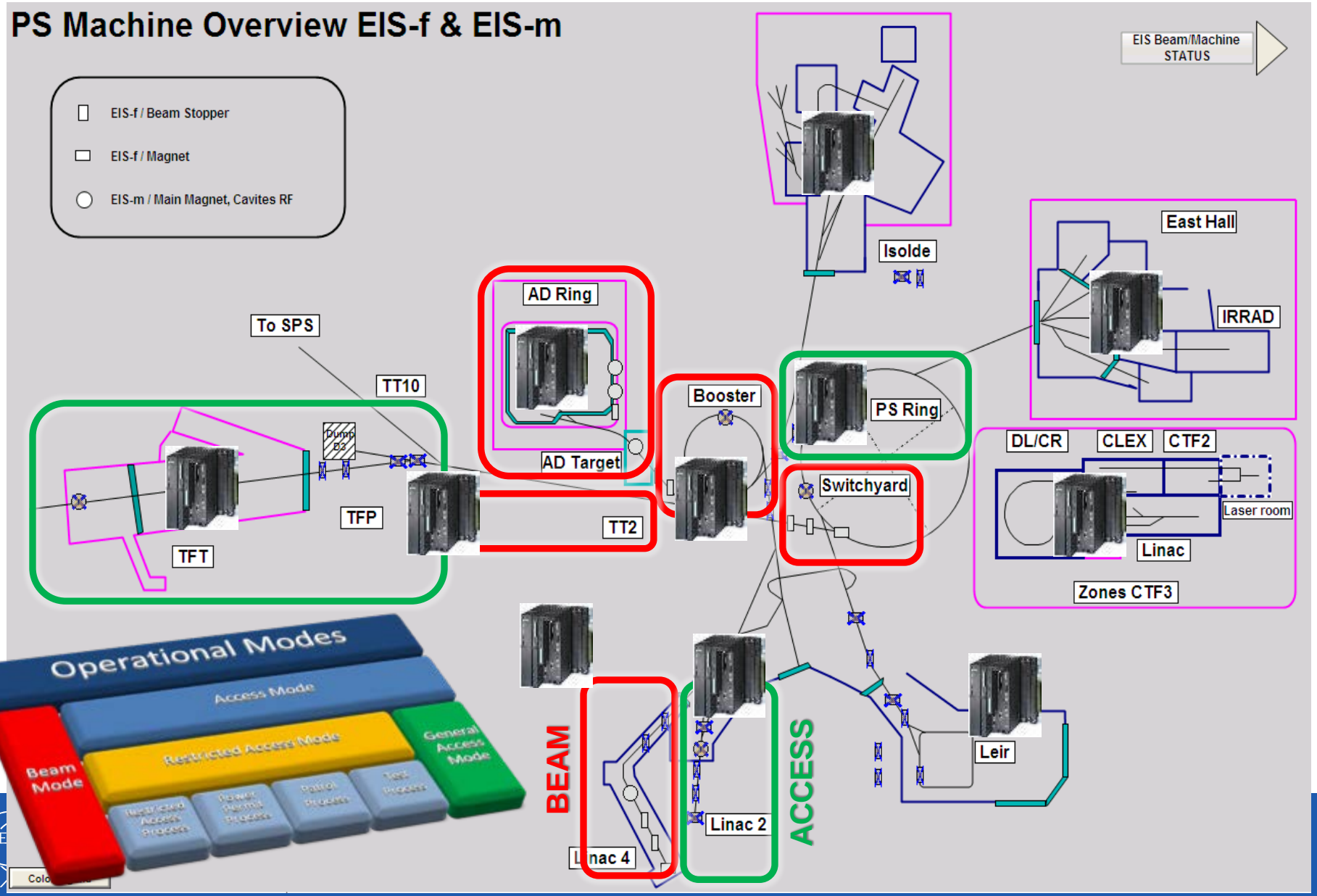
PS-PPS Project Scope



PS-PPS Project Scope



PS-PPS Project Scope



Safety Test Bench Conception

Safety

- Validate Safety Software of each zone controller.
- Validate safety communication between zone controllers (min. 3).

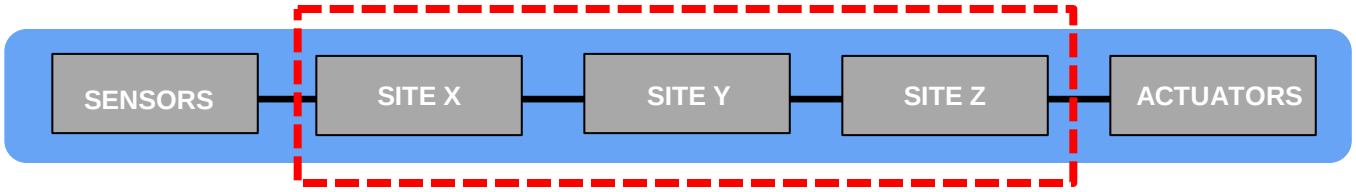
Operation

- Validate all operational synoptic.
- Integrate real access devices (PAD/MAD) within the simulated signals.

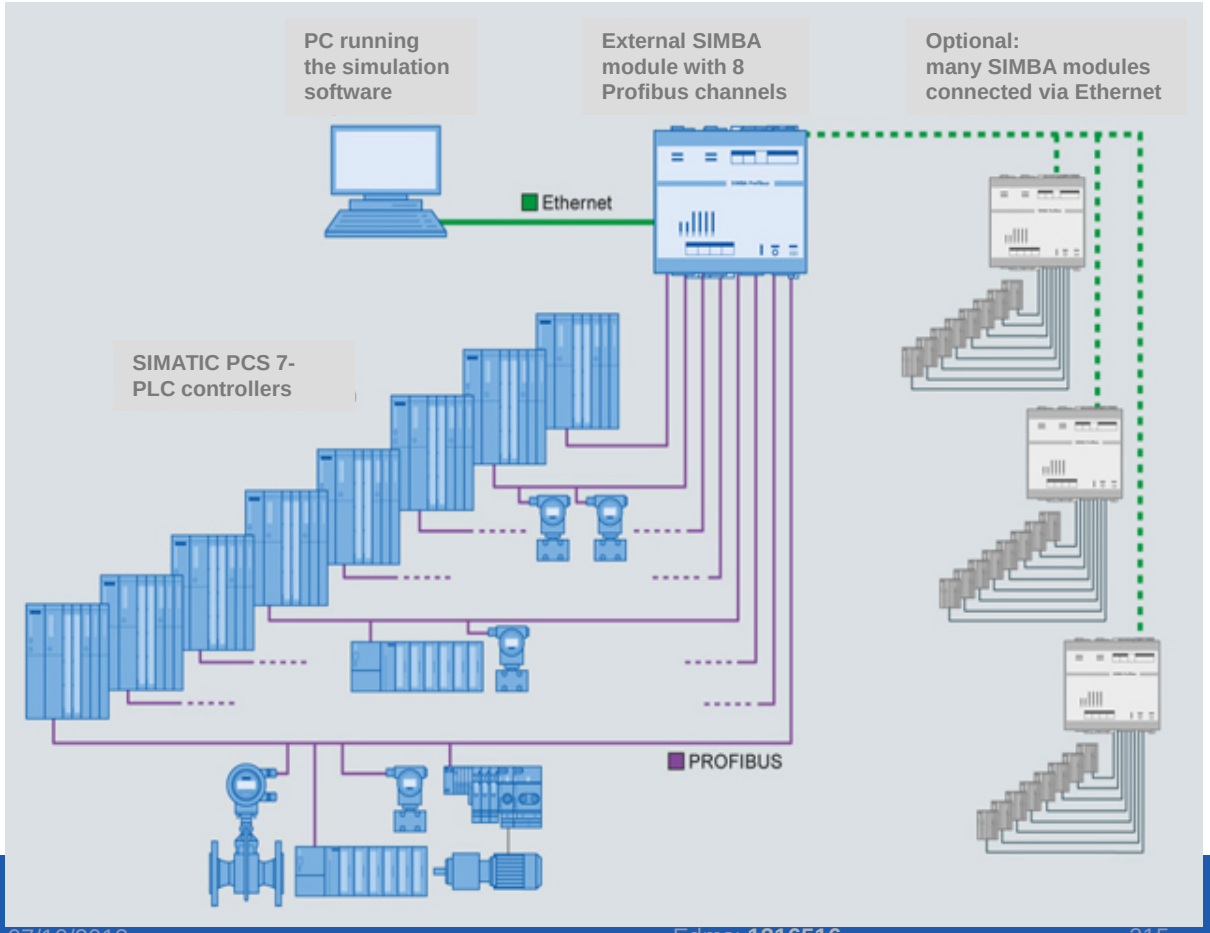
Usability

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

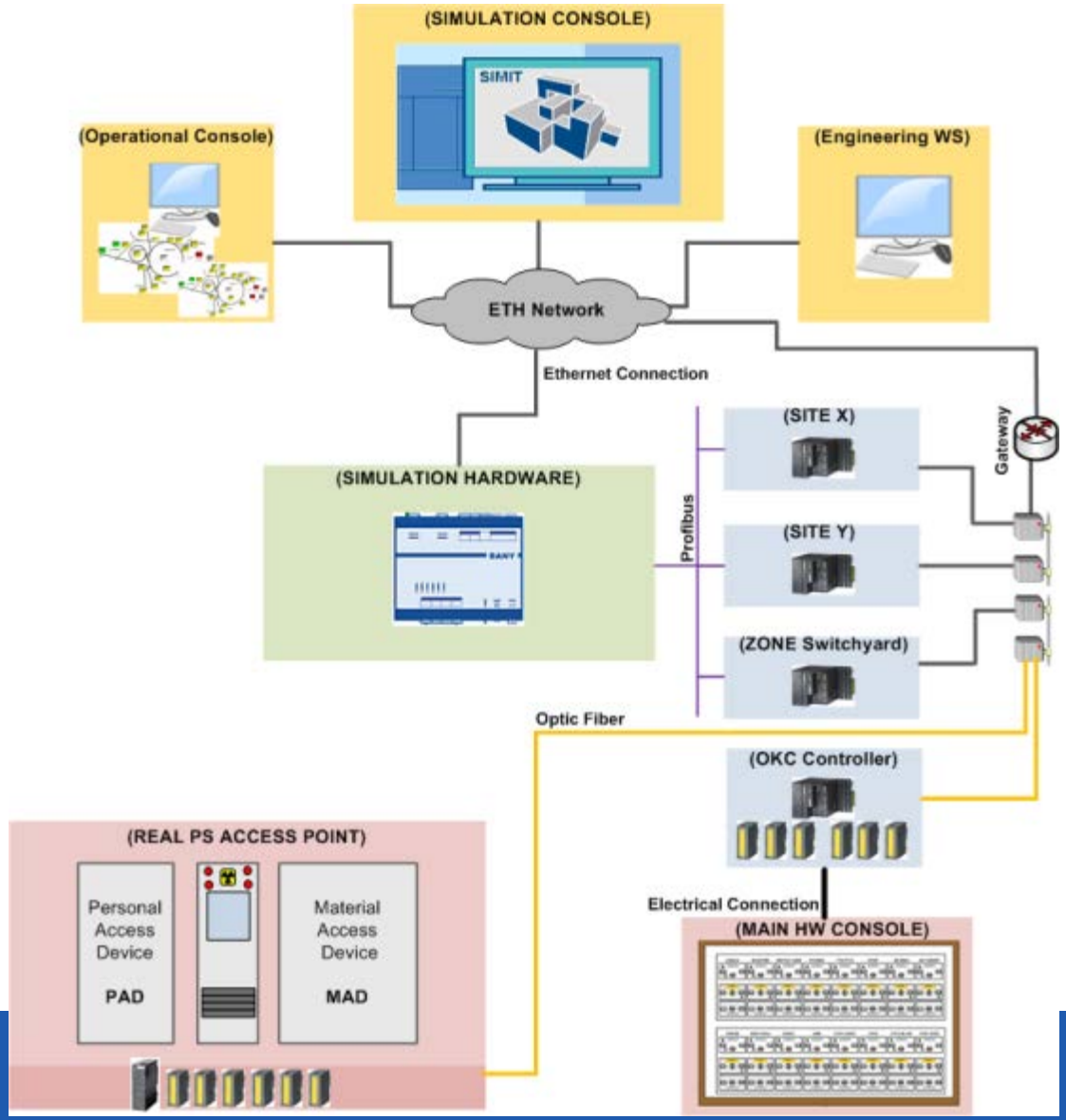
Safety Test Bench Conception



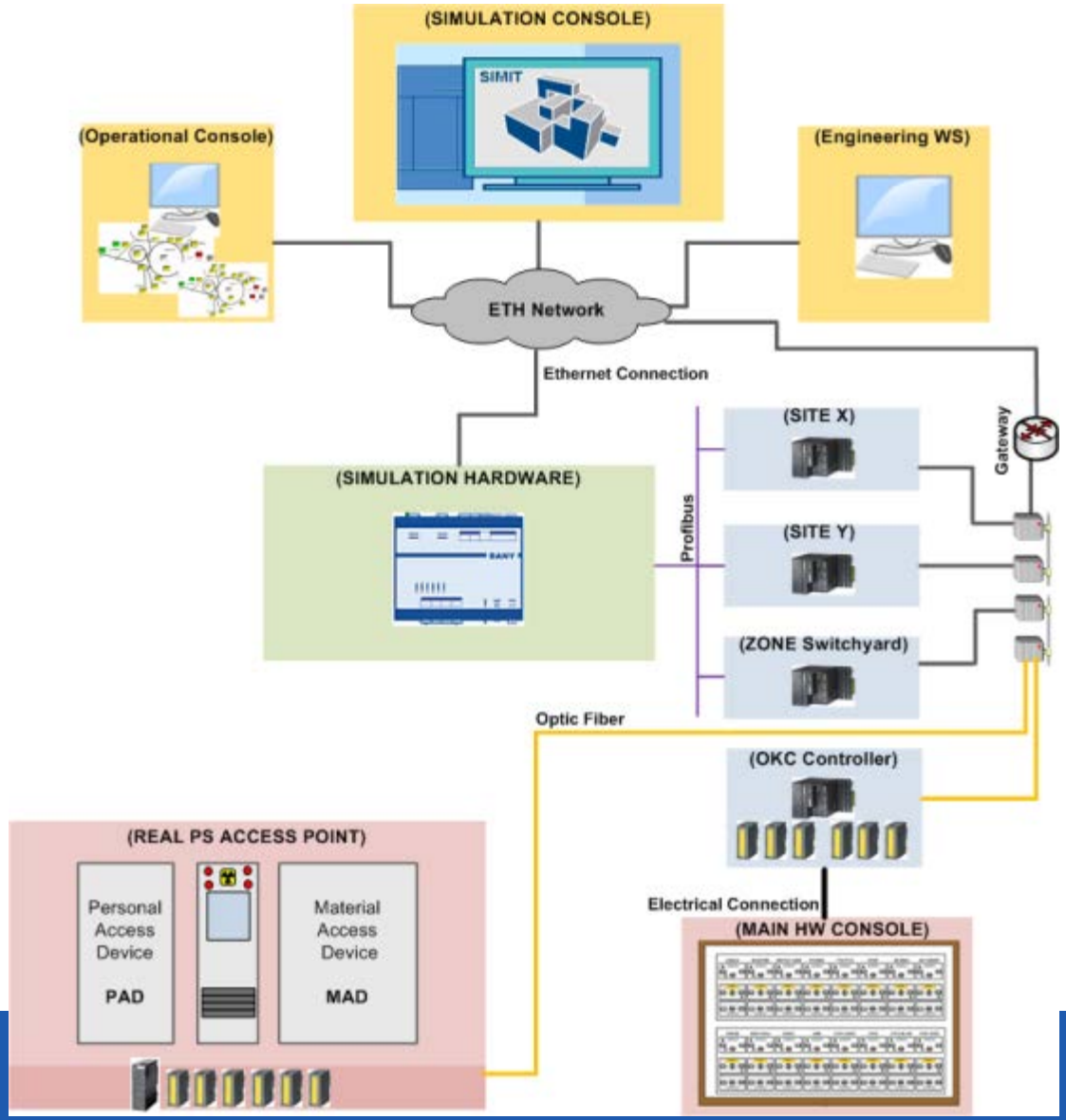
SIEMENS SIMBA Box



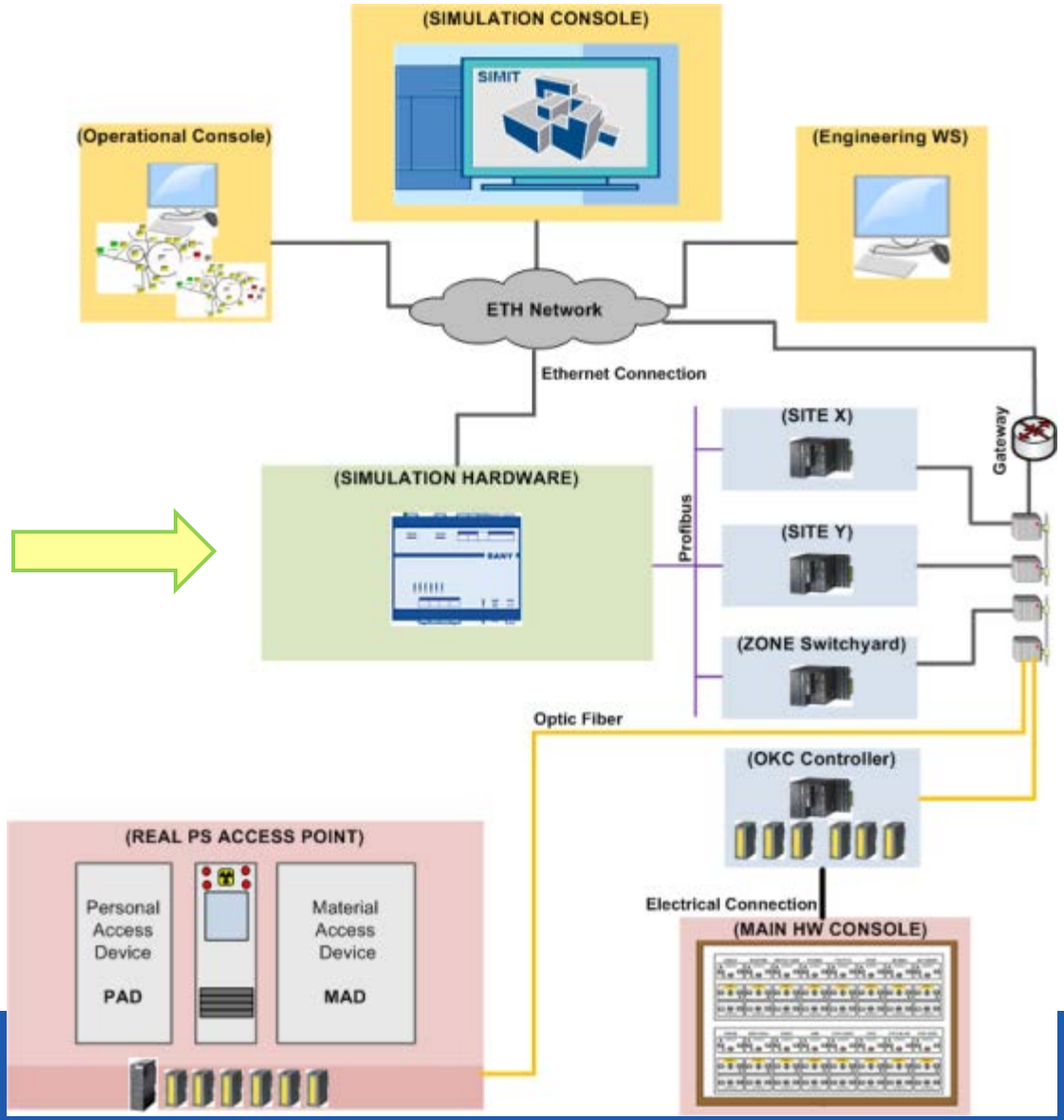
Safety Test Bench Conception



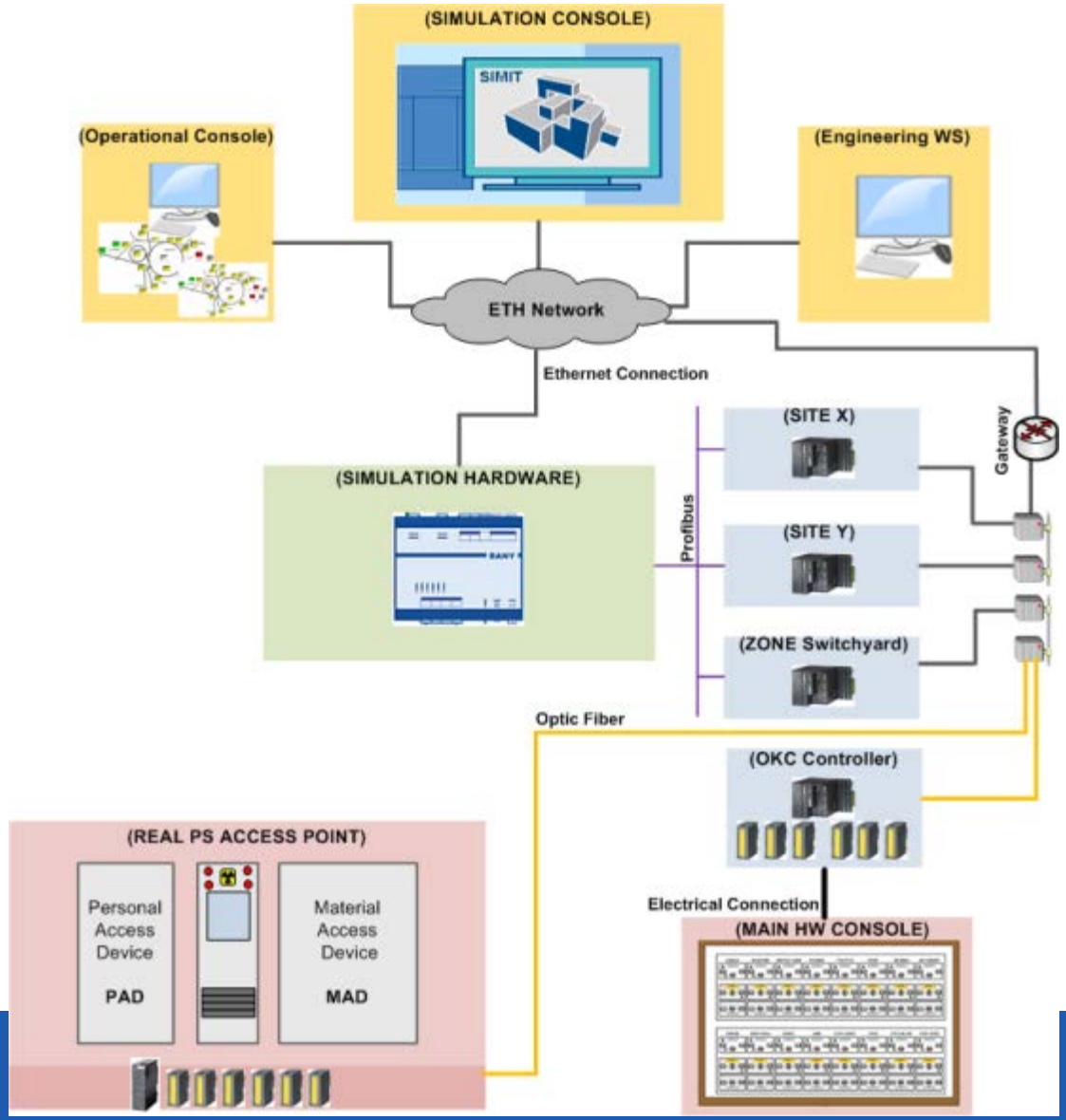
Safety Test Bench Conception



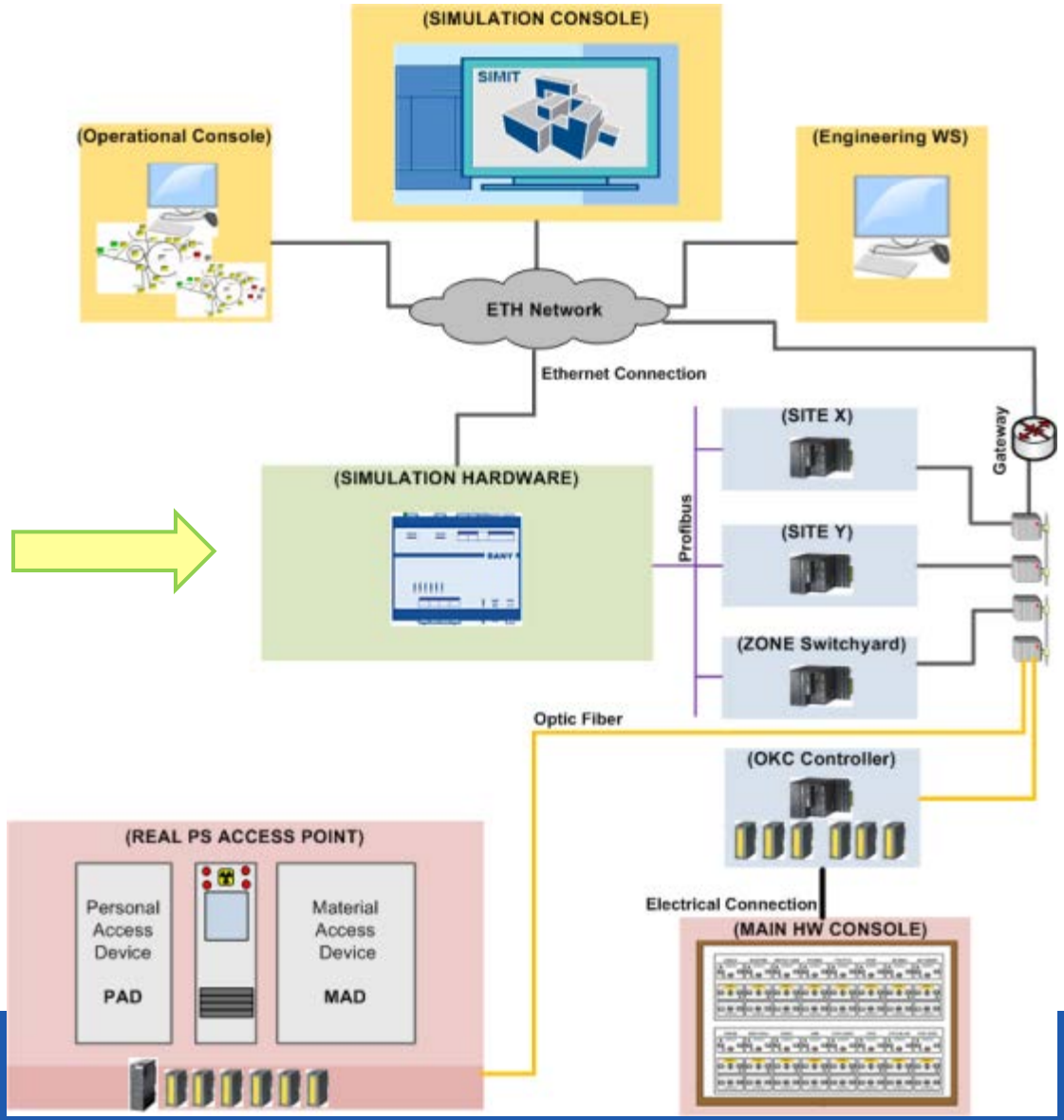
Safety Test Bench Conception



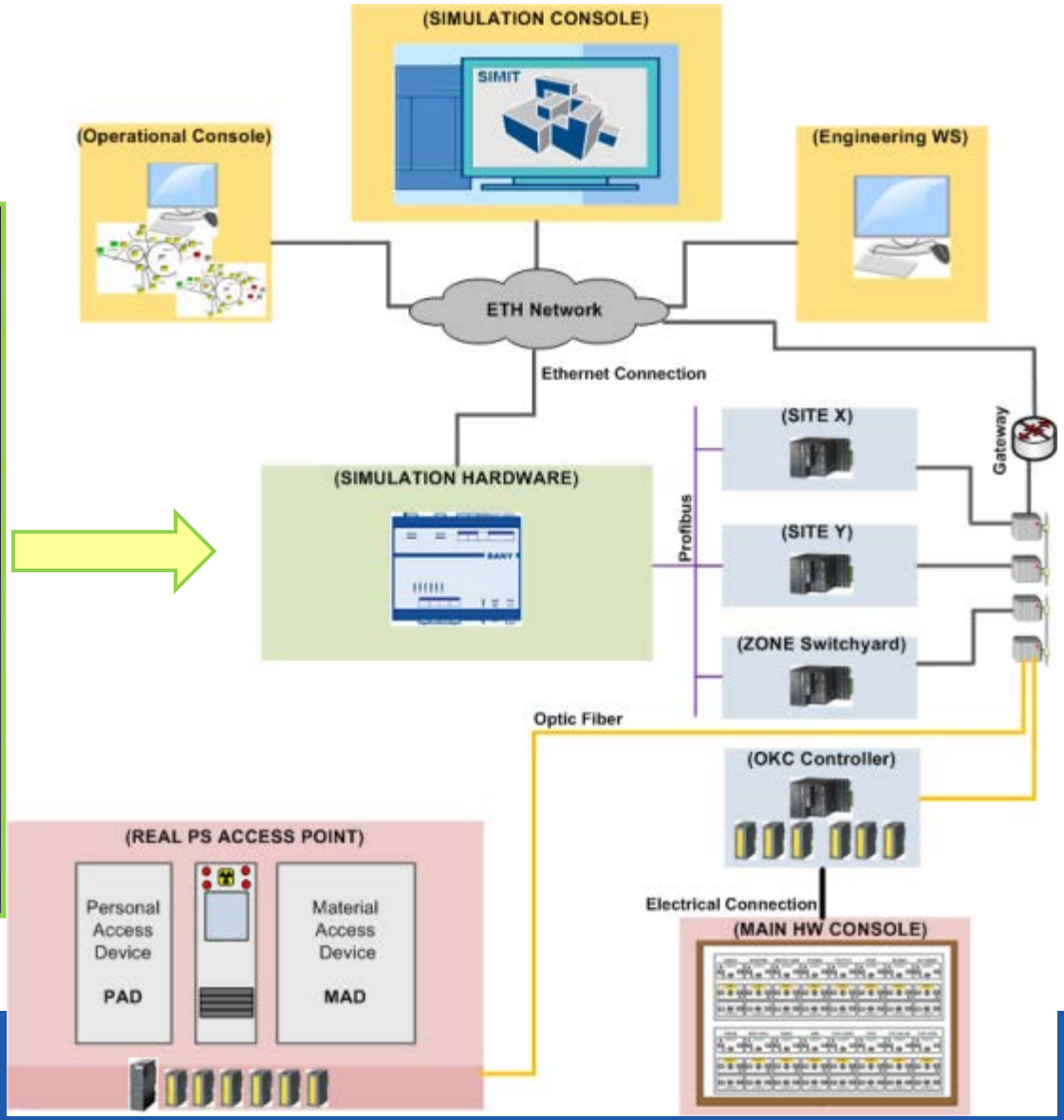
Safety Test Bench Conception



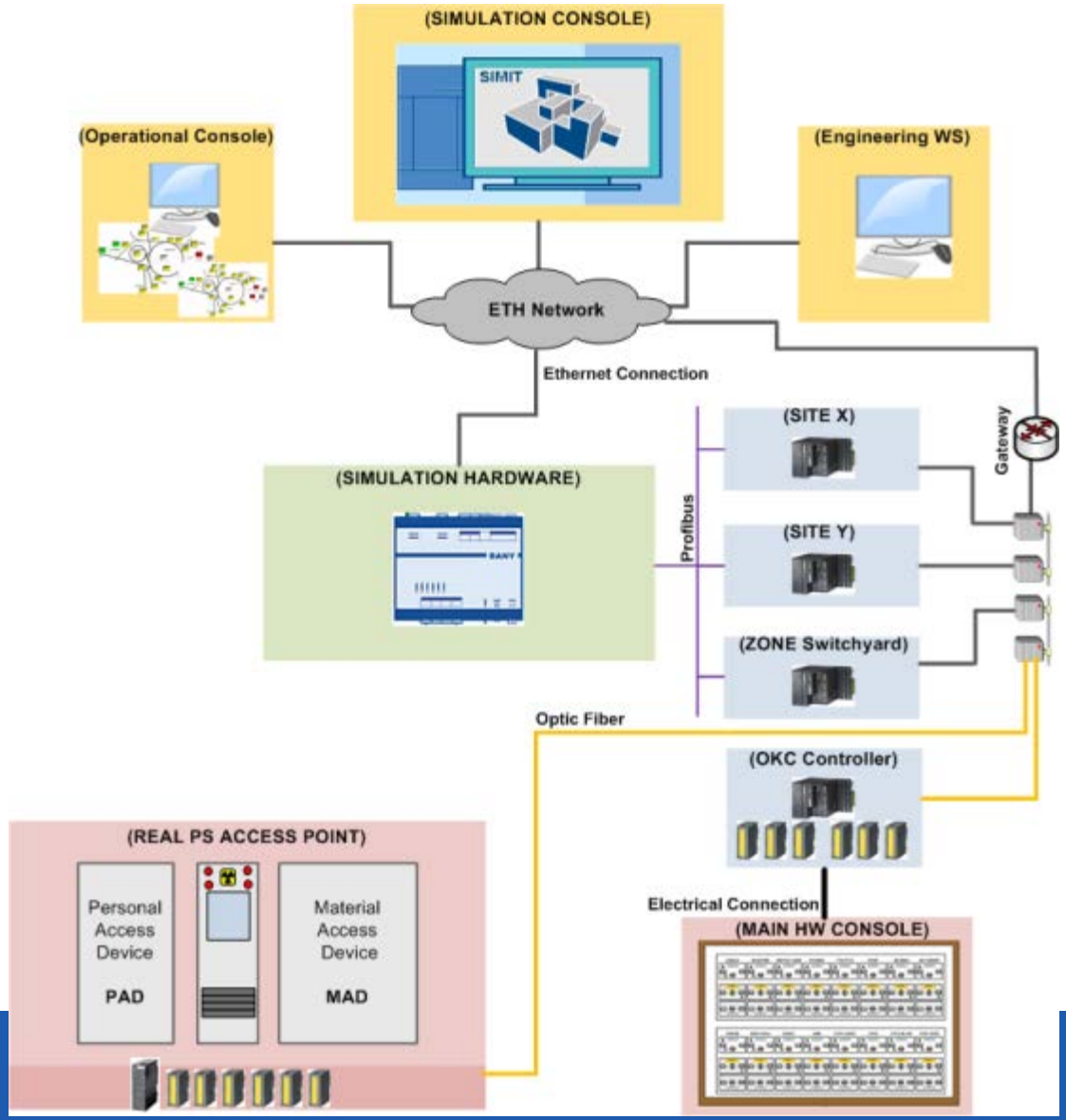
Safety Test Bench Conception



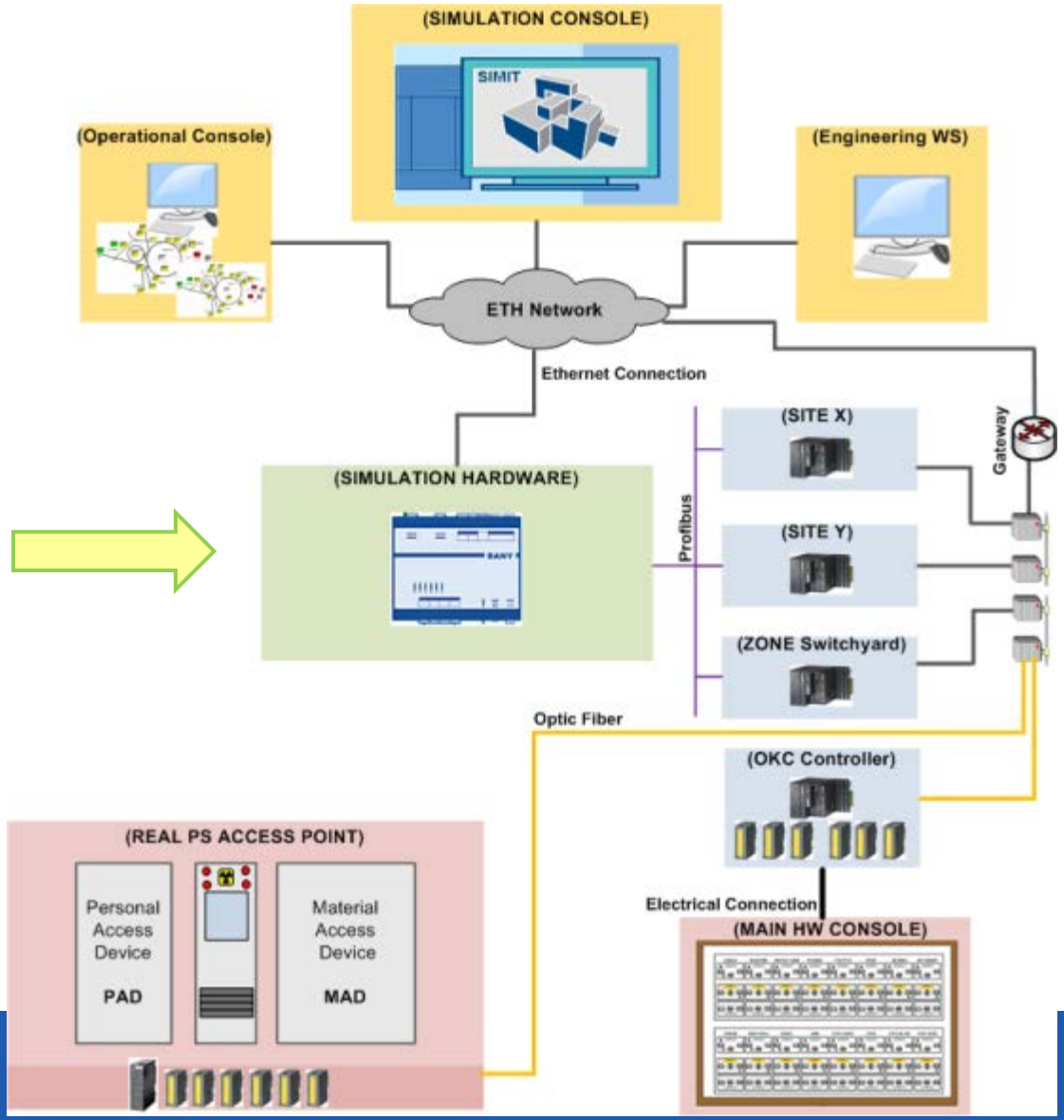
Safety Test Bench Conception



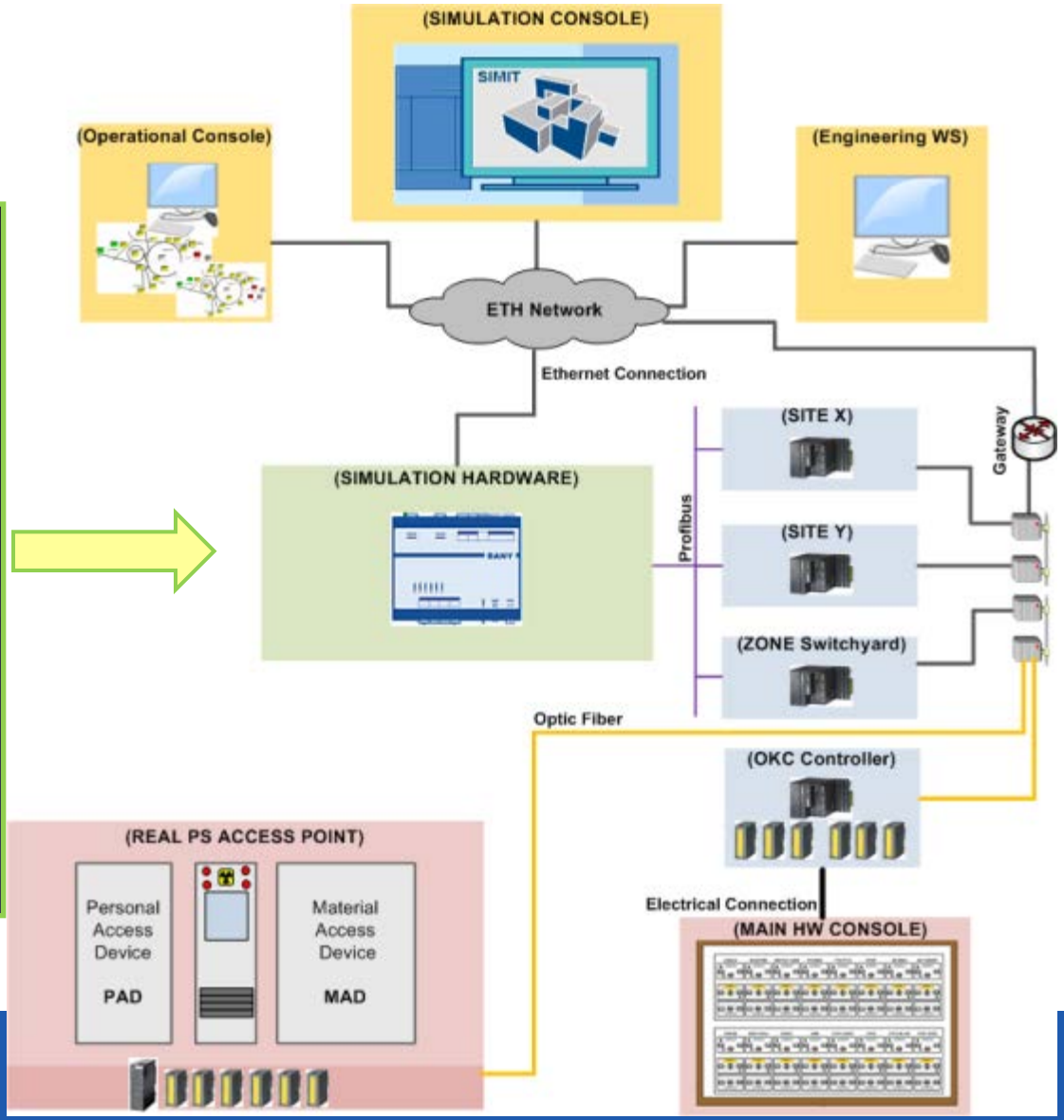
Safety Test Bench Conception



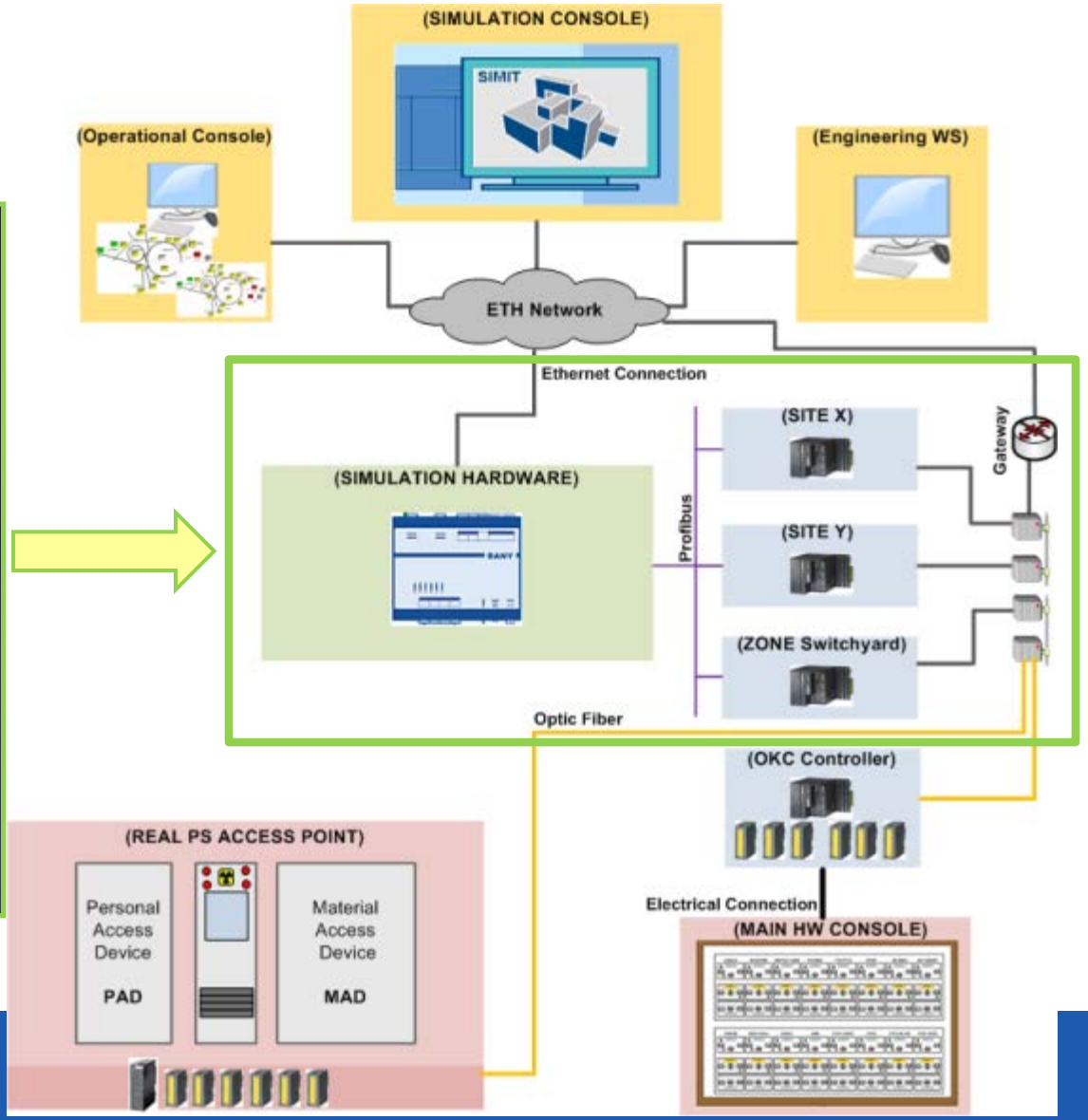
Safety Test Bench Conception



Safety Test Bench Conception



Safety Test Bench Conception



SIF – Formal Definition Language

SECTION 1: SIF 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*

SIF – Formal Definition Language

SECTION 2: SIF 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

SIF – Formal Definition Language

SECTION 3: SIF 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**

Safety Functions – Testing Problem

MAIN OBJECTIVE: *Validate efficiently all Safety Instrumented Functions in order to discover all major bugs related to safety before the final system deployment phase.*

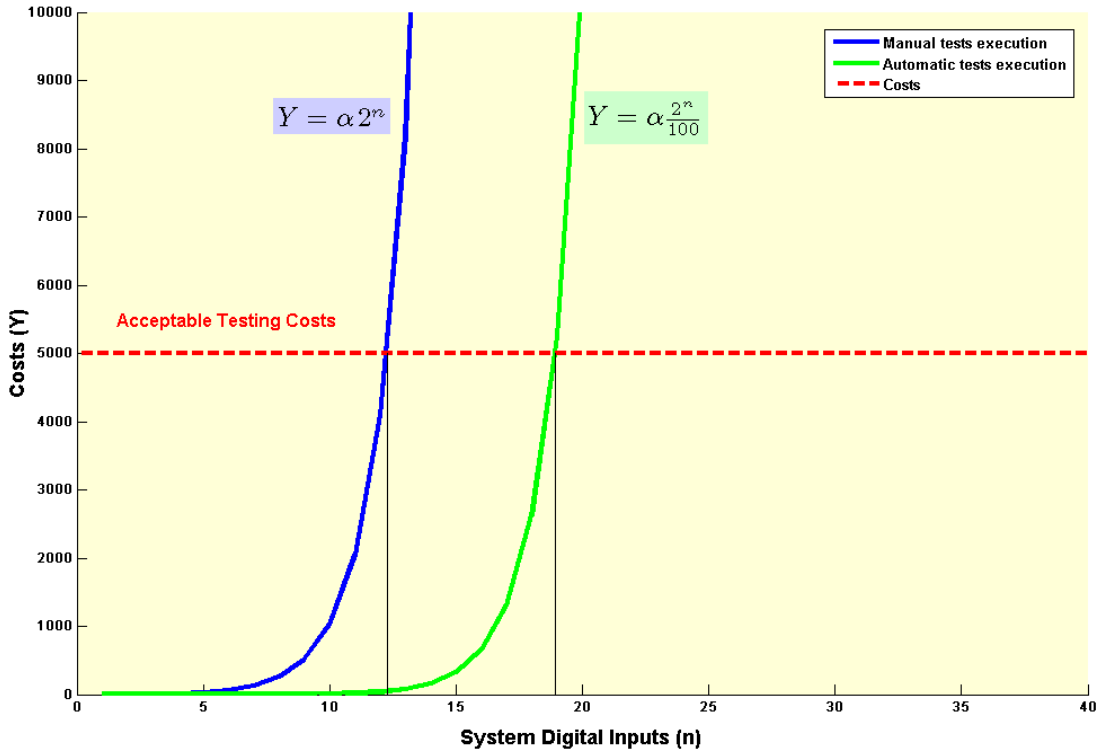
Safety Functions – Testing Problem

MAIN OBJECTIVE: *Validate efficiently all Safety Instrumented Functions in order to discover all major bugs related to safety before the final system deployment phase.*

Safety Functions – Testing Problem

MAIN OBJECTIVE: *Validate efficiently all Safety Instrumented Functions in order to discover all major bugs related to safety before the final system deployment phase.*

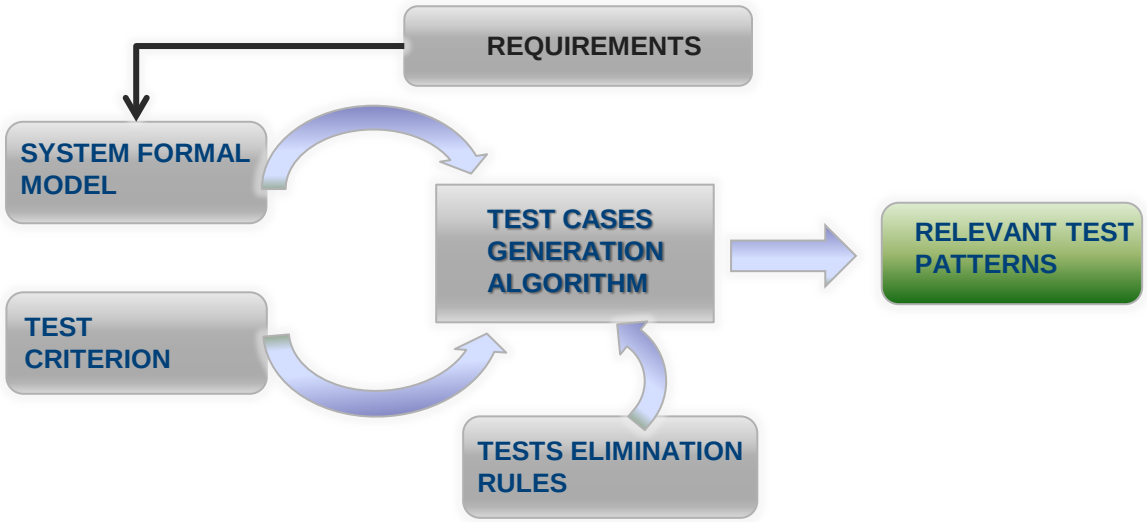
Solution 1: **EXAUSTIVE TESTING STRATEGY**



- Simple to implement
- Detect 100% of system errors
- Unsustainable execution times and costs

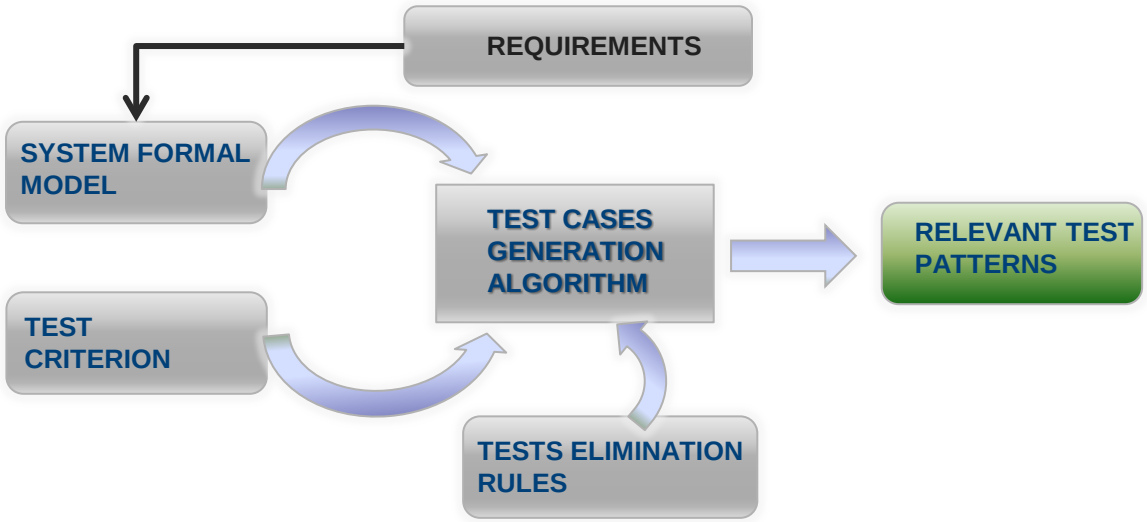
Safety Functions – Testing Problem

Solution 2: **MODEL-BASED TESTING STRATEGY**



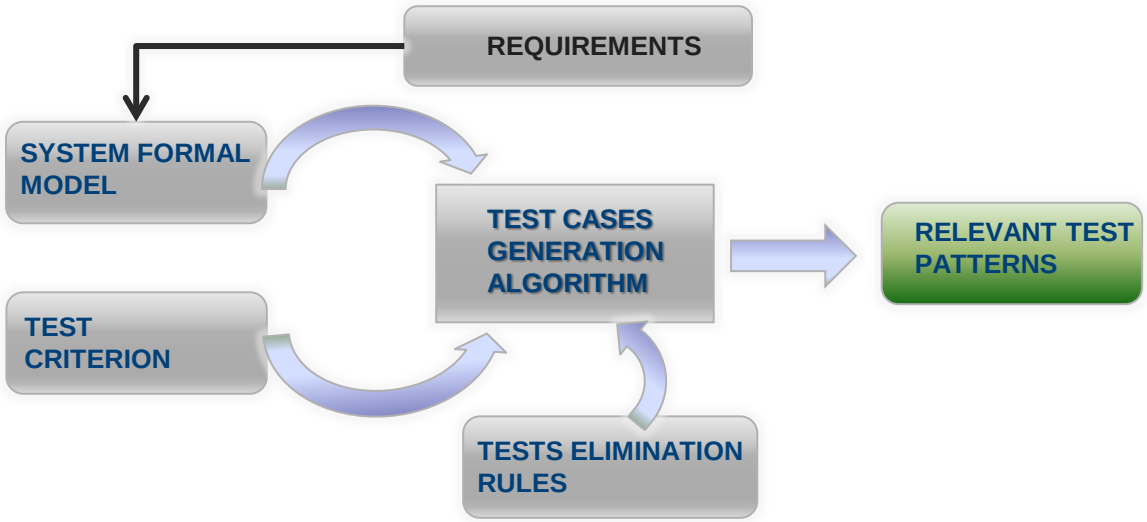
Safety Functions – Testing Problem

Solution 2: **MODEL-BASED TESTING STRATEGY**



Safety Functions – Testing Problem

Solution 2: **MODEL-BASED TESTING STRATEGY**



Maximize the probability of detecting errors, reducing the tests execution costs.

Mathematical proof of the test Coverage (**C**) obtained:

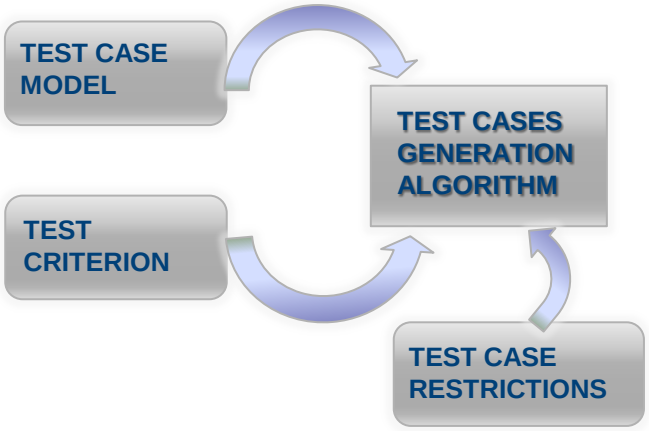
C = <# *Executed Tests*> / <# *Total Tests*>

Do not guarantee 100% detection of all system errors. In general:

Er(x) = *C* * *P(x)* **(Confidence index for detecting an error x)**

Safety Functions Model-Based Testing

Test Criterion: *Verify the output values for all possible events triggering the SIF interlock actions.*



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

TEST CASE MODEL:

$\Phi_1_1 = ((MODE_Acc = 1 \vee MODE_TFA = 1 \vee MODE_Tra = 1) \wedge ACC_Tst = 0 \wedge ACC_TfT = 0 \wedge EISb_Pos = 0) \vee (MODE_Acc = 0 \wedge EISa_Safe = 0)$

TEST CASE RESTRICTIONS:

$R_1 = (MODE_Acc=1 \wedge MODE_TFA=1) \vee (MODE_Acc=1 \wedge MODE_Tra = 1) \vee (MODE_TFA=1 \wedge MODE_Tra = 1)$

$R_2 = (ACC_Tst=1 \wedge ACC_TfT=1)$

$R_3 = (MODE_Acc=0) \wedge (ACC_Tst=1 \vee ACC_TfT=1)$

TEST CASE GENERATION MODEL:

$$\omega : (\Phi_1_1 = 1) \wedge (R_1 = 0) \wedge (R_2 = 0) \wedge (R_3 = 0)$$

SYSTEM VERIFICATION PROPERTY:

$$(MODE_Rep = 1)$$

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

Safety Functions Model-Based Testing

Test Instances auto-generated by MATLAB:

	MODE_Acc	MODE_TFA	MODE_Tra	ACC_Tst	ACC_TtT	ElSb_Pos	ElSa_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	

Safety Functions Model-Based Testing

Test Instances auto-generated by MATLAB:

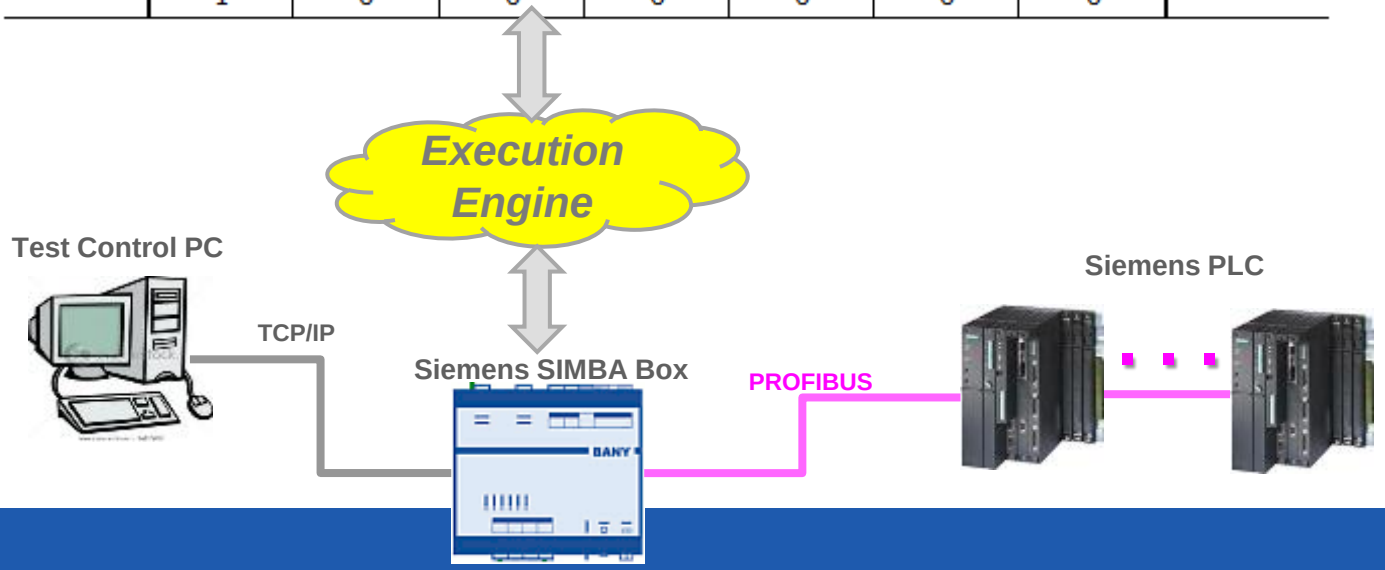
	MODE_Acc	MODE_TFA	MODE_Tra	ACC_Tst	ACC_TtT	ElSb_Pos	ElSa_Safe	RESULTS
Test 1	0	0	0	0	0	1	0	
Test 2	0	0	0	0	0	0	0	
Test 3	0	0	1	0	0	0	1	
Test 4	0	0	1	0	0	0	0	
Test 5	0	0	1	0	0	1	0	
Test 6	0	1	0	0	0	0	1	
Test 7	0	1	0	0	0	0	0	
Test 8	0	1	0	0	0	1	0	
Test 9	1	0	0	0	0	0	1	
Test 10	1	0	0	0	0	0	0	

Safety Functions Model-Based Testing

Test Instances auto-generated by MATLAB:

	MODE_Acc	MODE_TFA	MODE_Tra	ACC_Tst	ACC_TIT	ElSb_Pos	ElSa_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



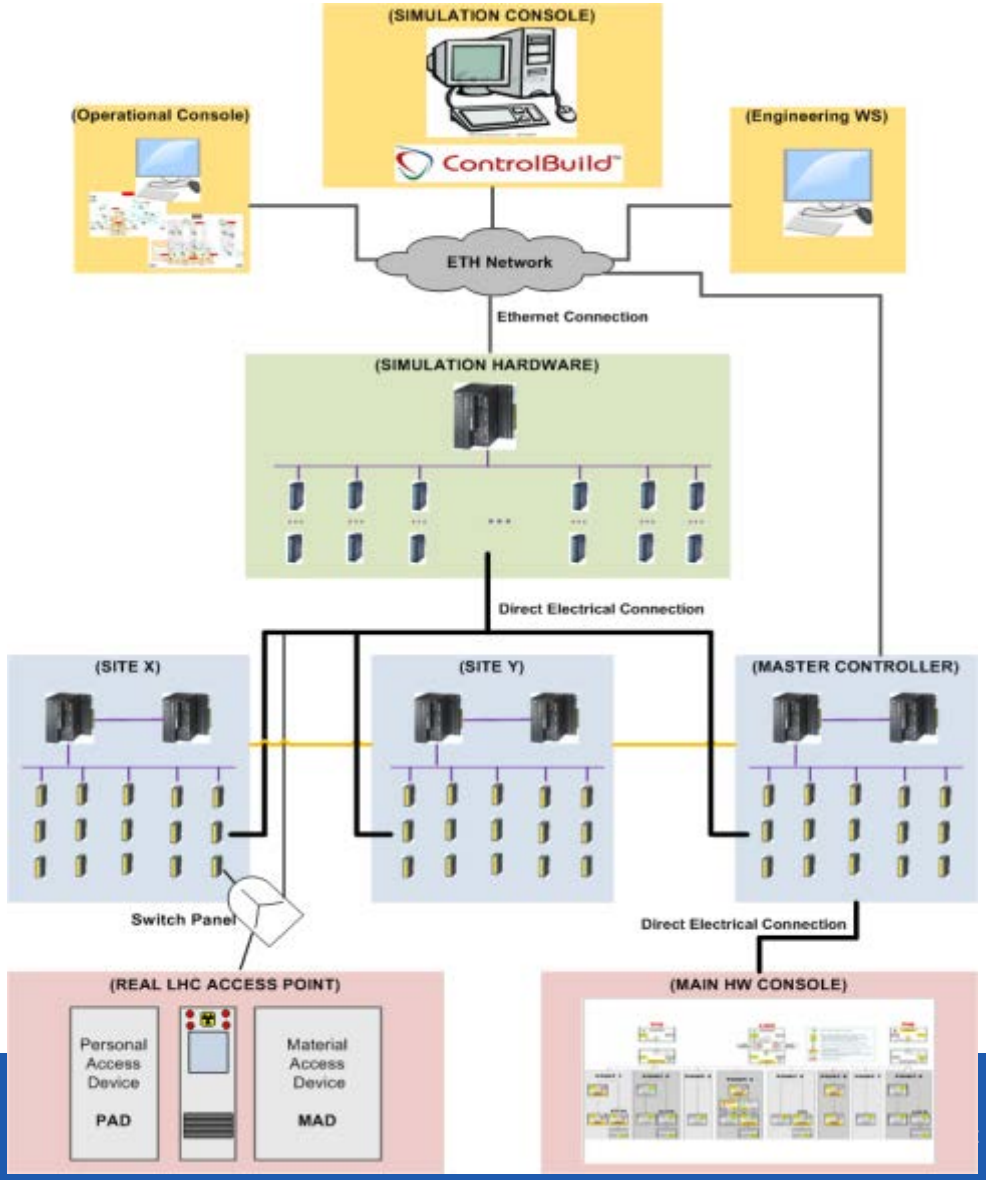
Conclusions

- **It is essential to clearly fix the testing objectives in order to obtain a performing Test Bench for Safety Validation.**
- **The main Test Bench realization principles shall be related to: Scalability, Flexibility, coherence with the real system, easy operability and maintainability.**
- **The adoption of formal languages for the Safety Functions modeling is an essential key to implement a Model-Based Testing strategy, improving the quality of the final Validation Test Plan.**

www.cern.ch

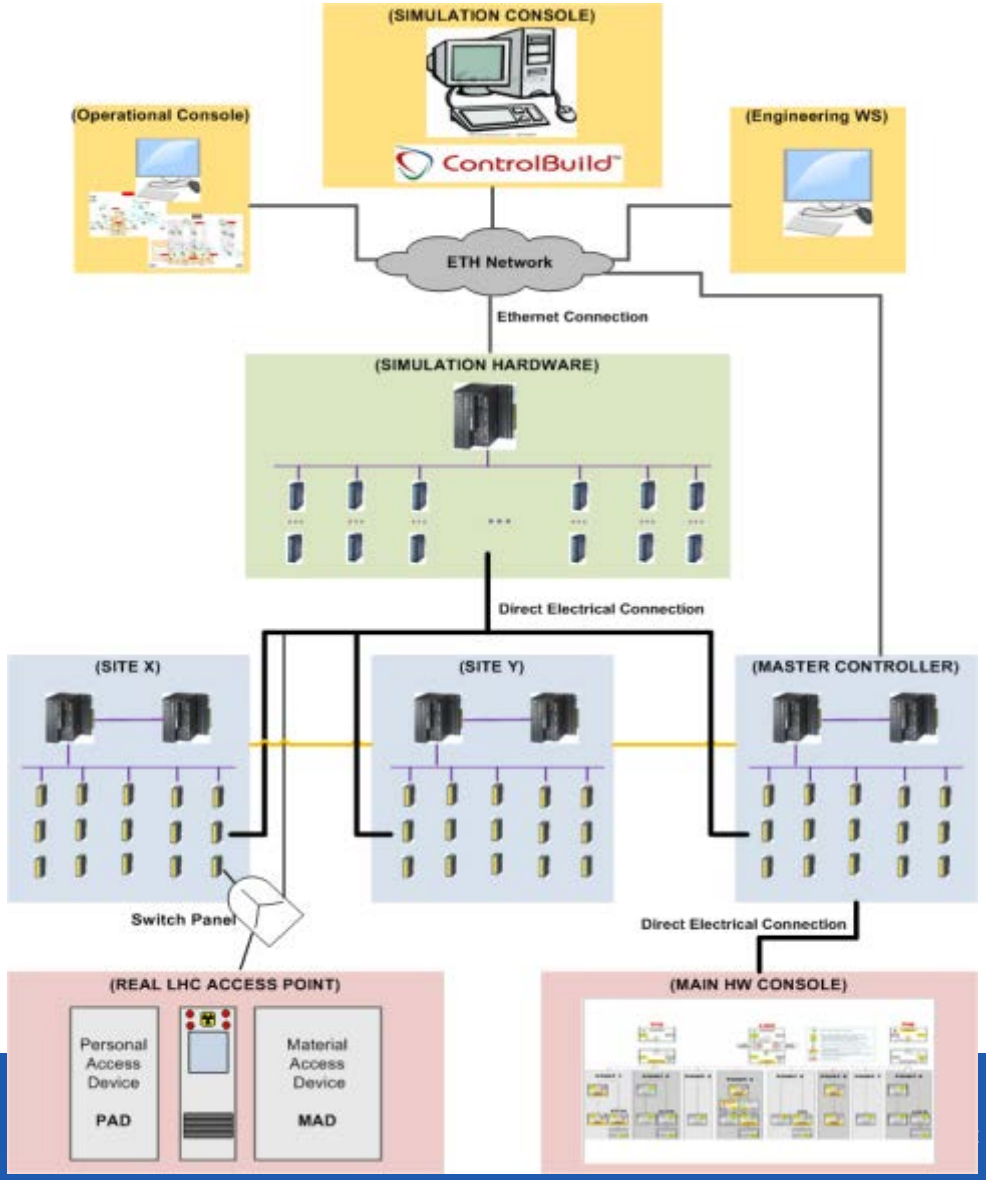
Safety Test Bench Conception

Classic Architectural Model Example



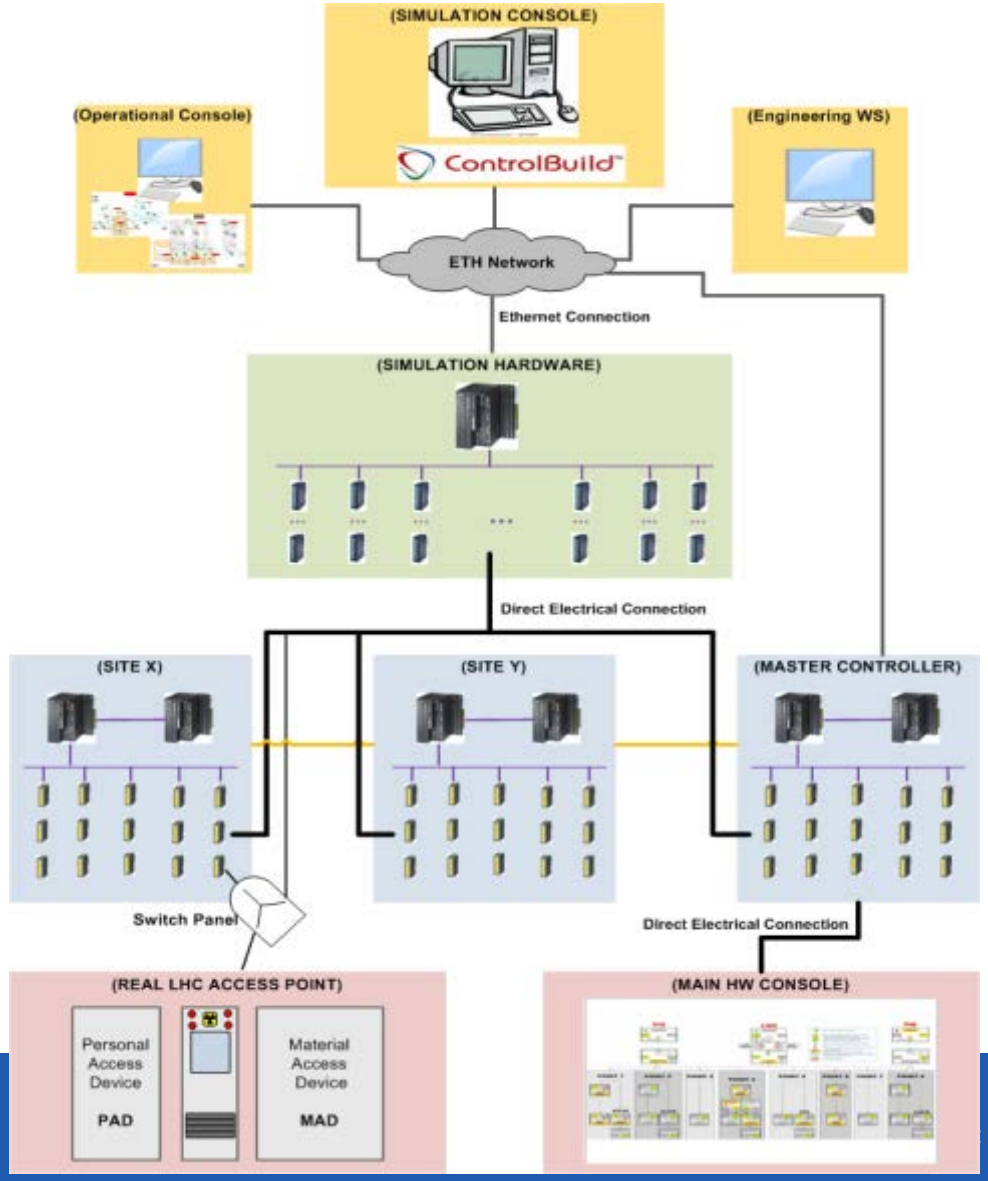
Safety Test Bench Conception

Classic Architectural Model Example



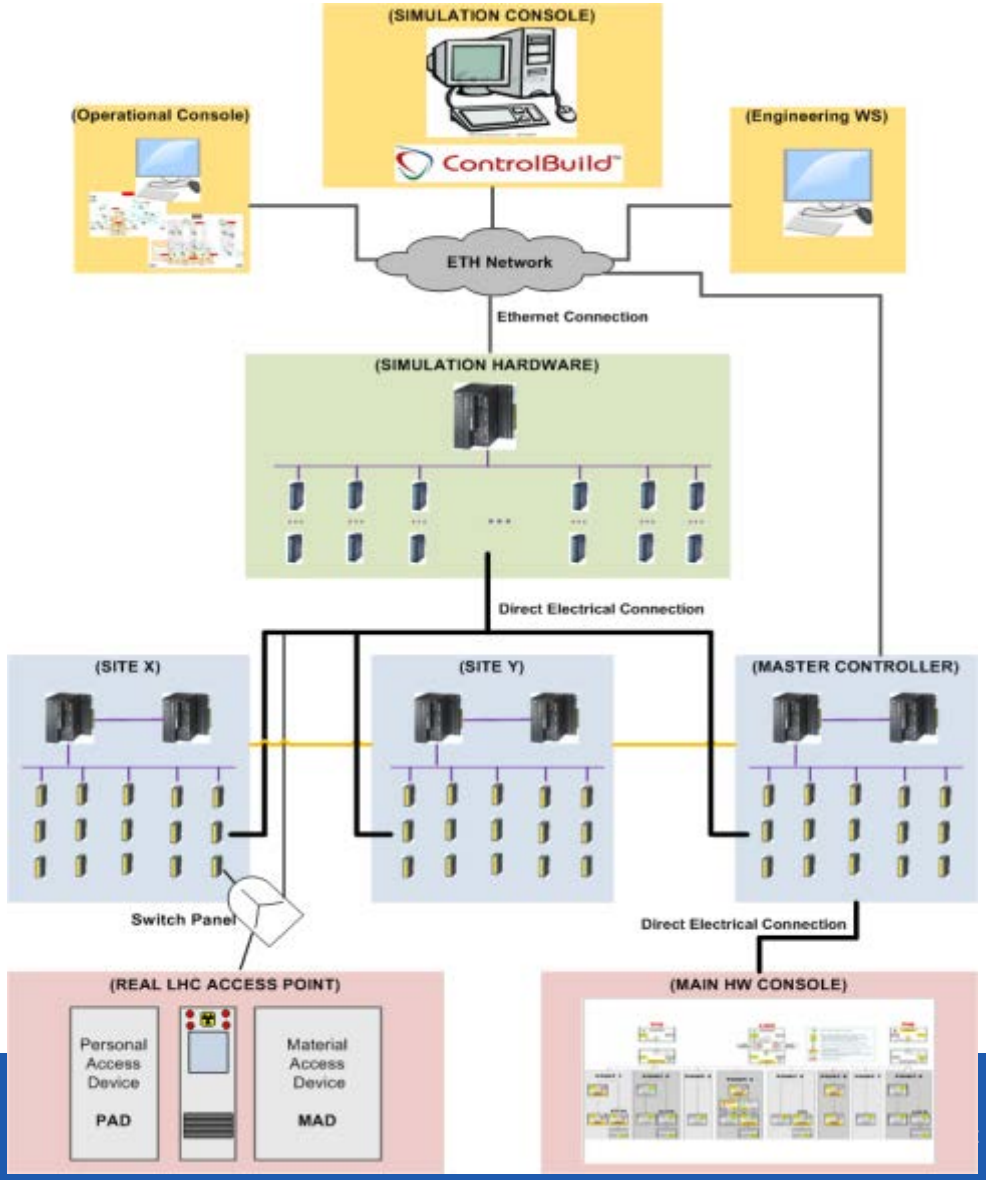
Safety Test Bench Conception

Classic Architectural Model Example



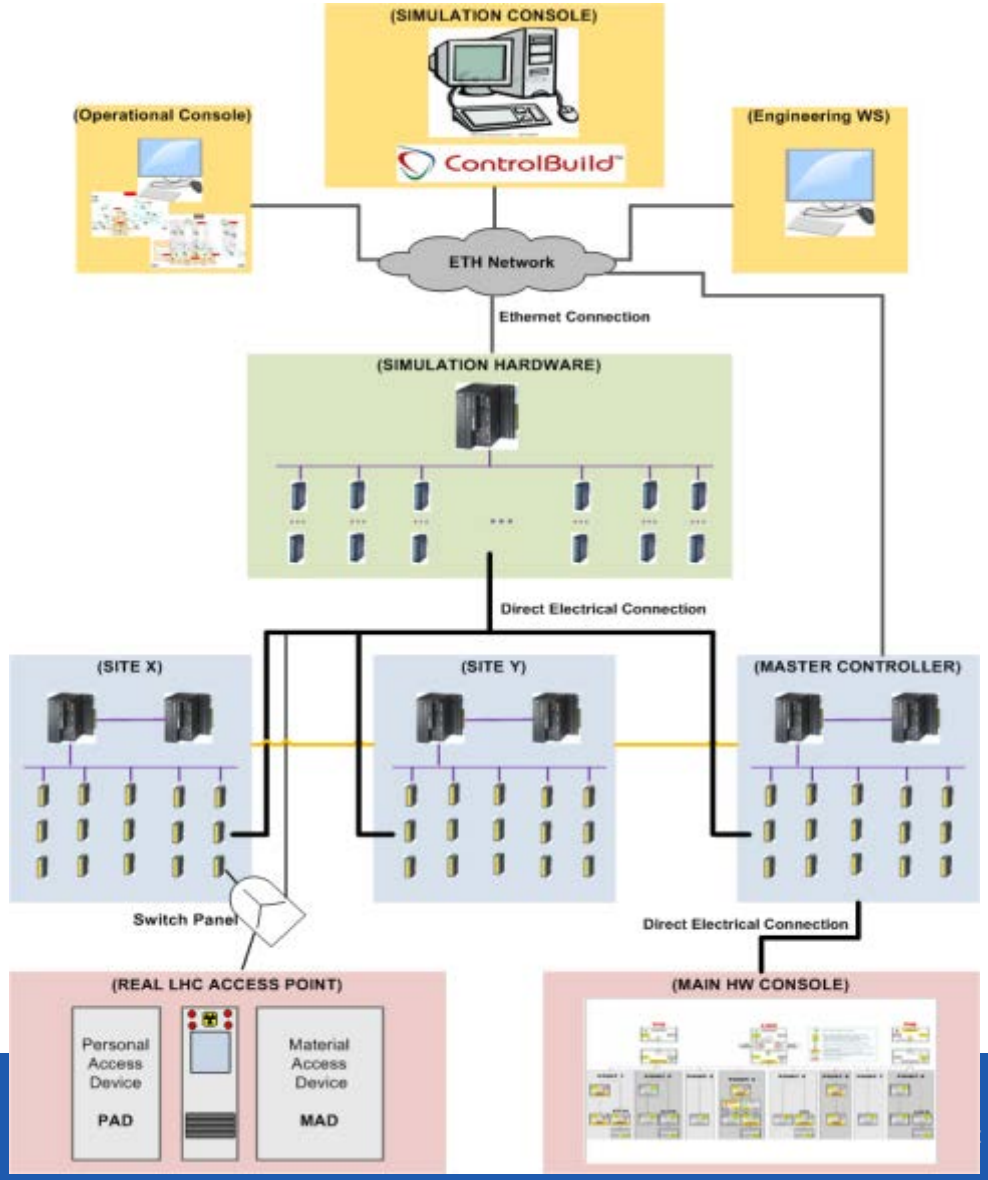
Safety Test Bench Conception

Classic Architectural Model Example



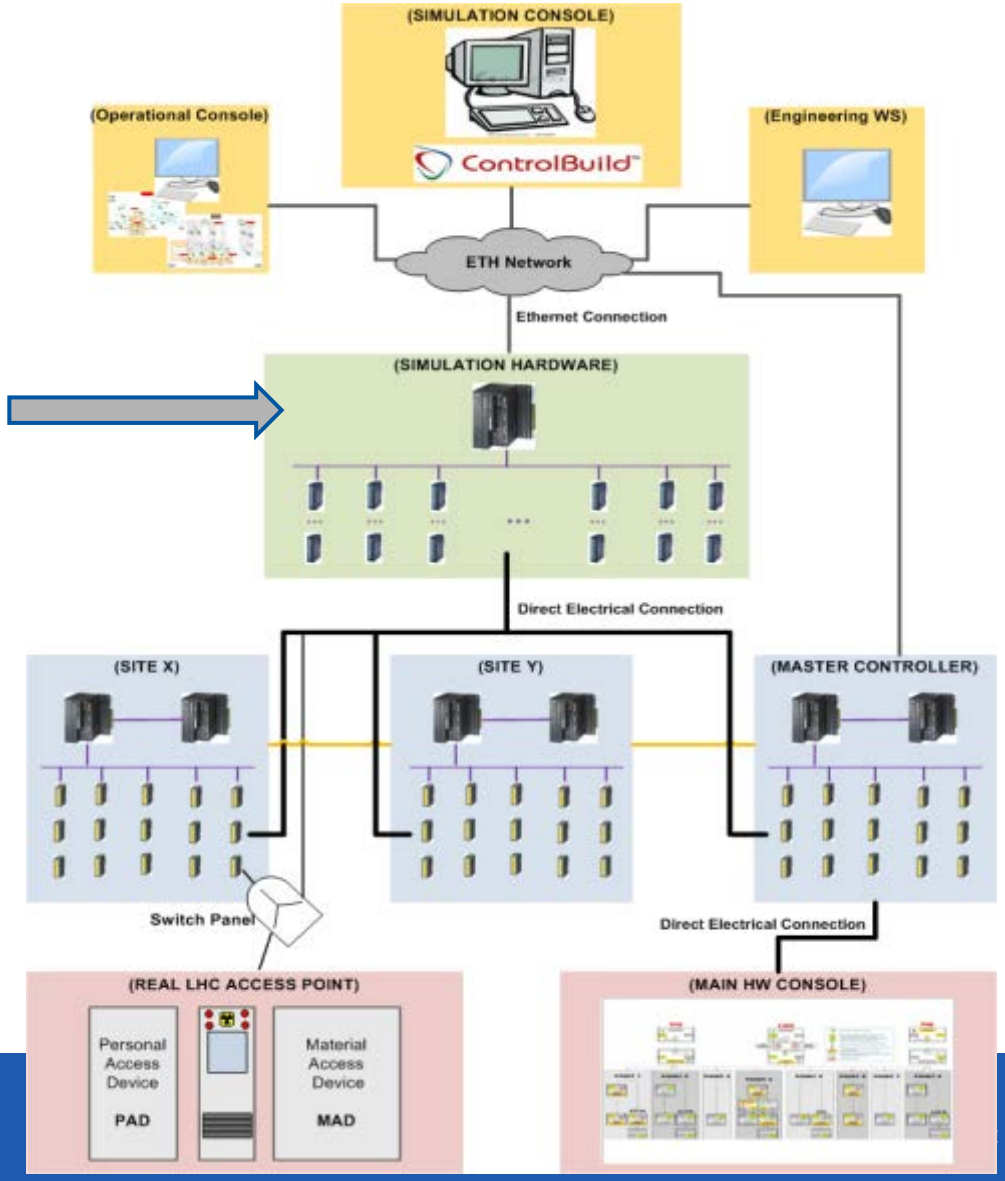
Safety Test Bench Conception

Classic Architectural Model Example



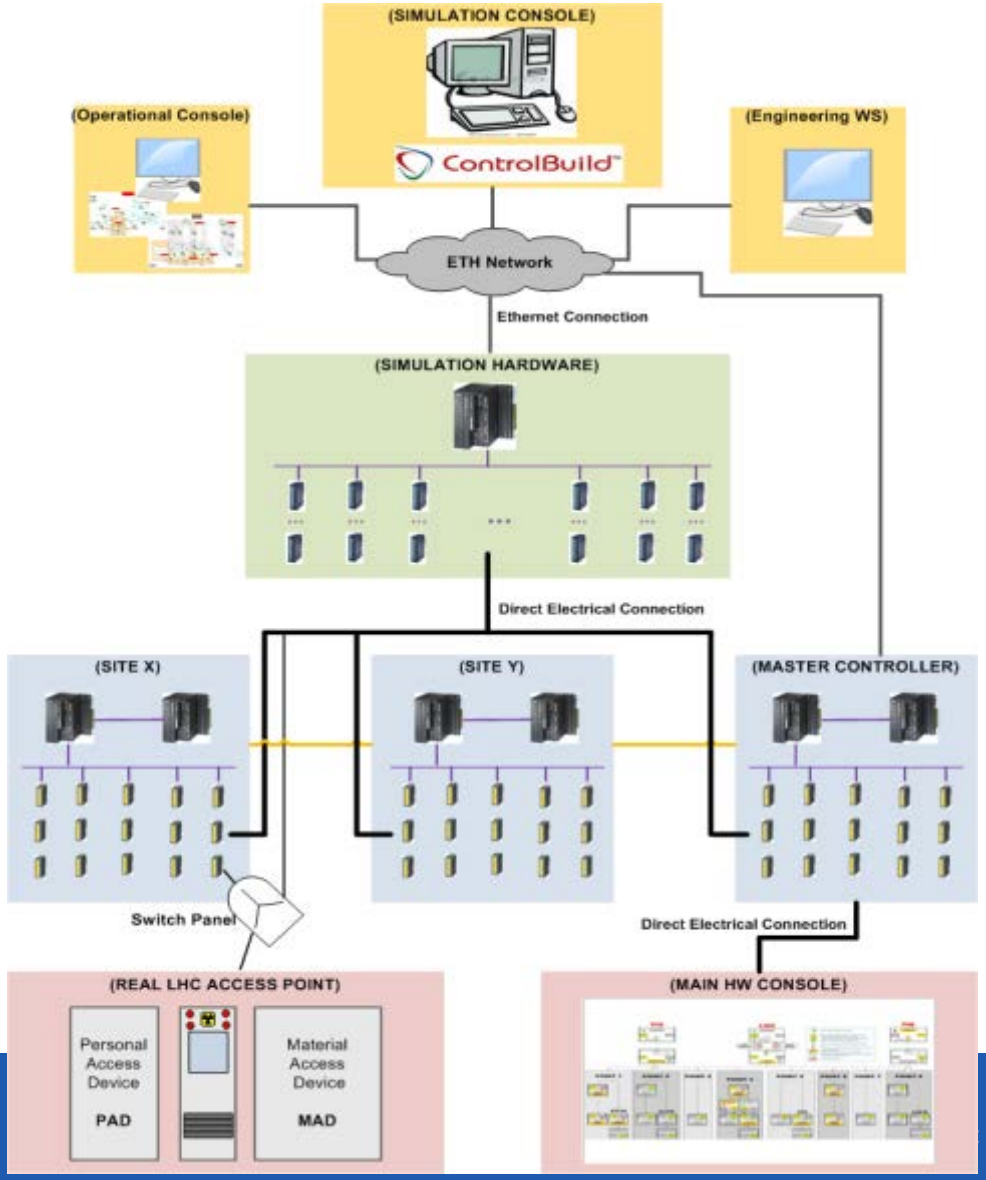
Safety Test Bench Conception

Classic Architectural Model Example



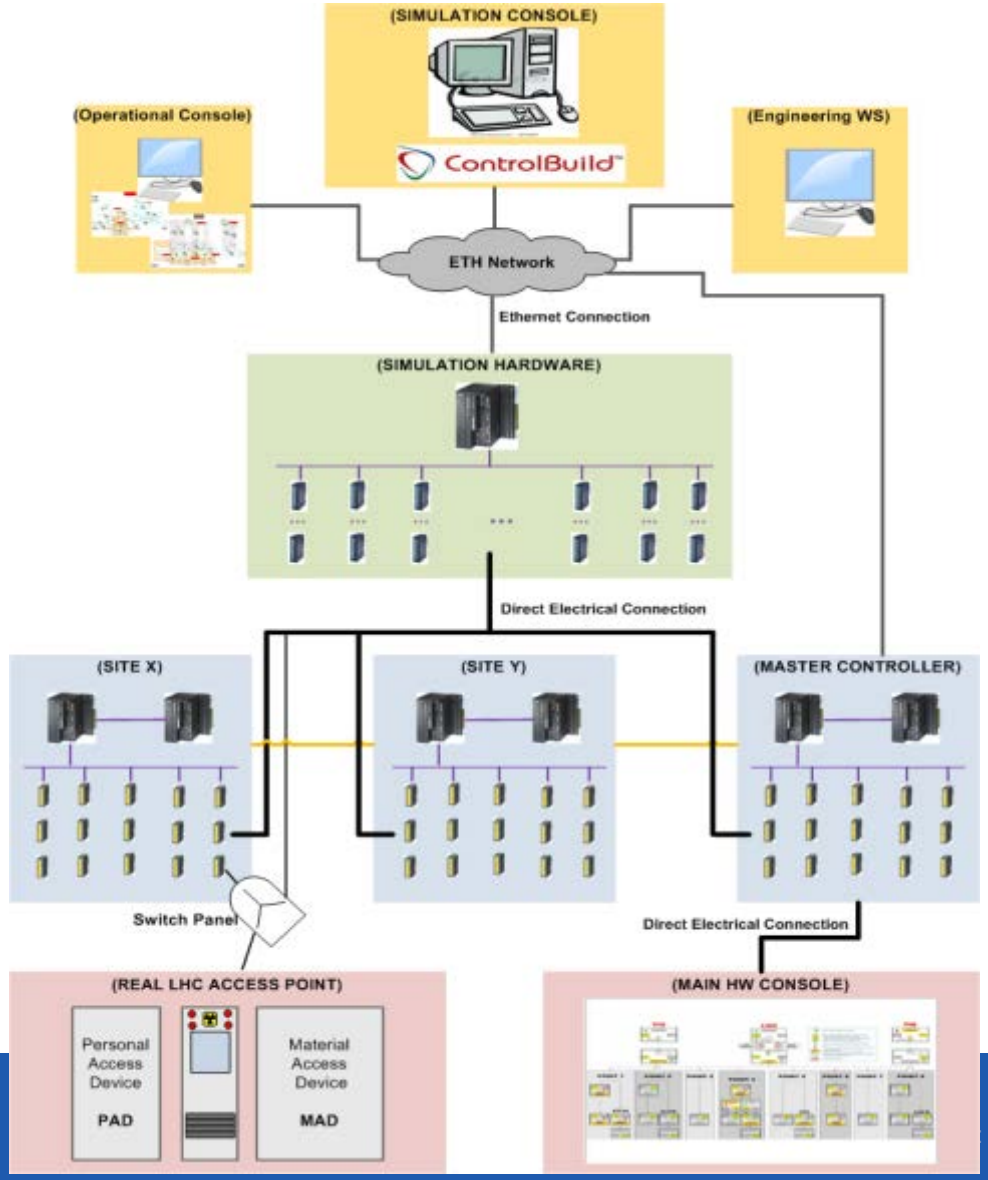
Safety Test Bench Conception

Classic Architectural Model Example



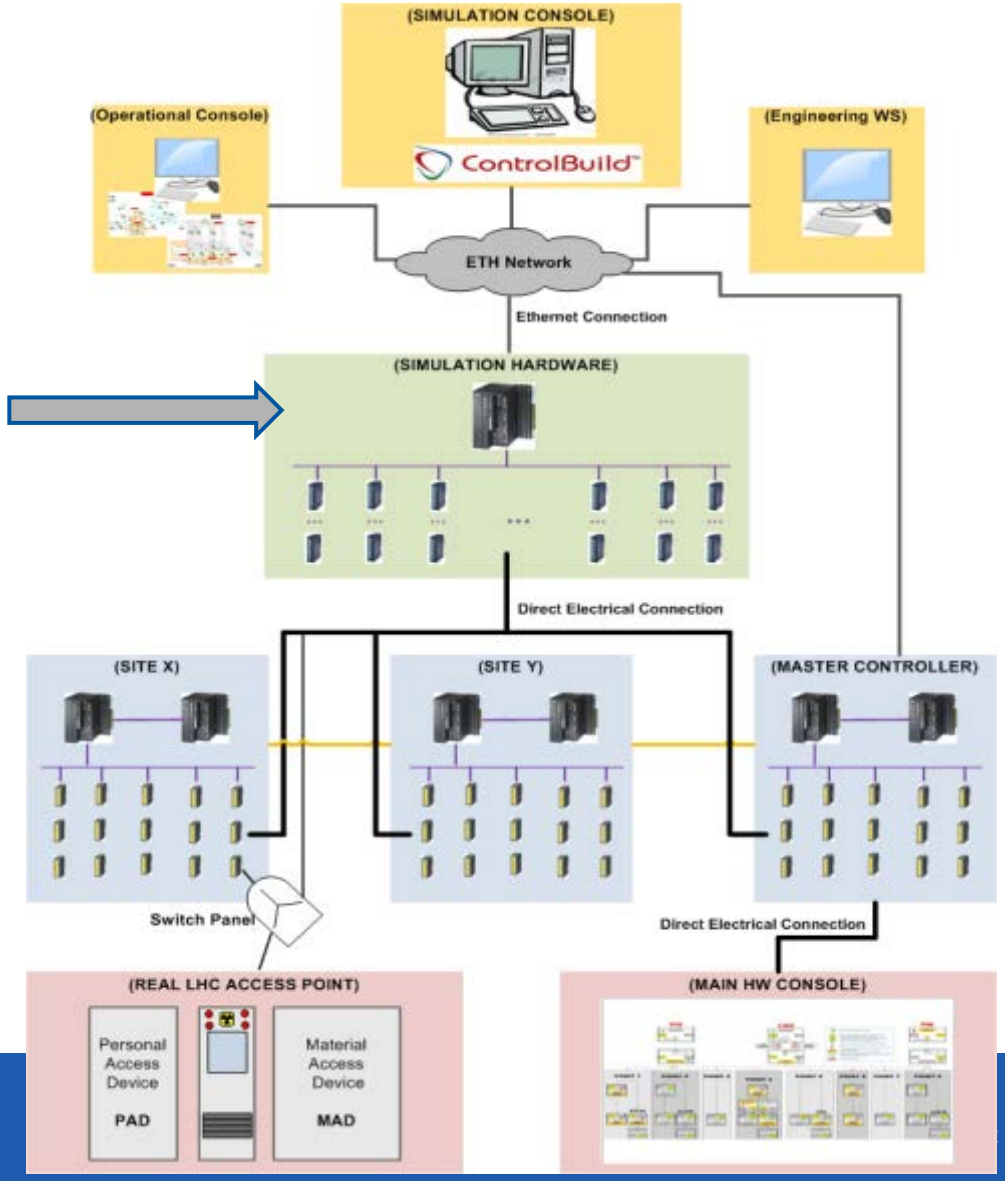
Safety Test Bench Conception

Classic Architectural Model Example



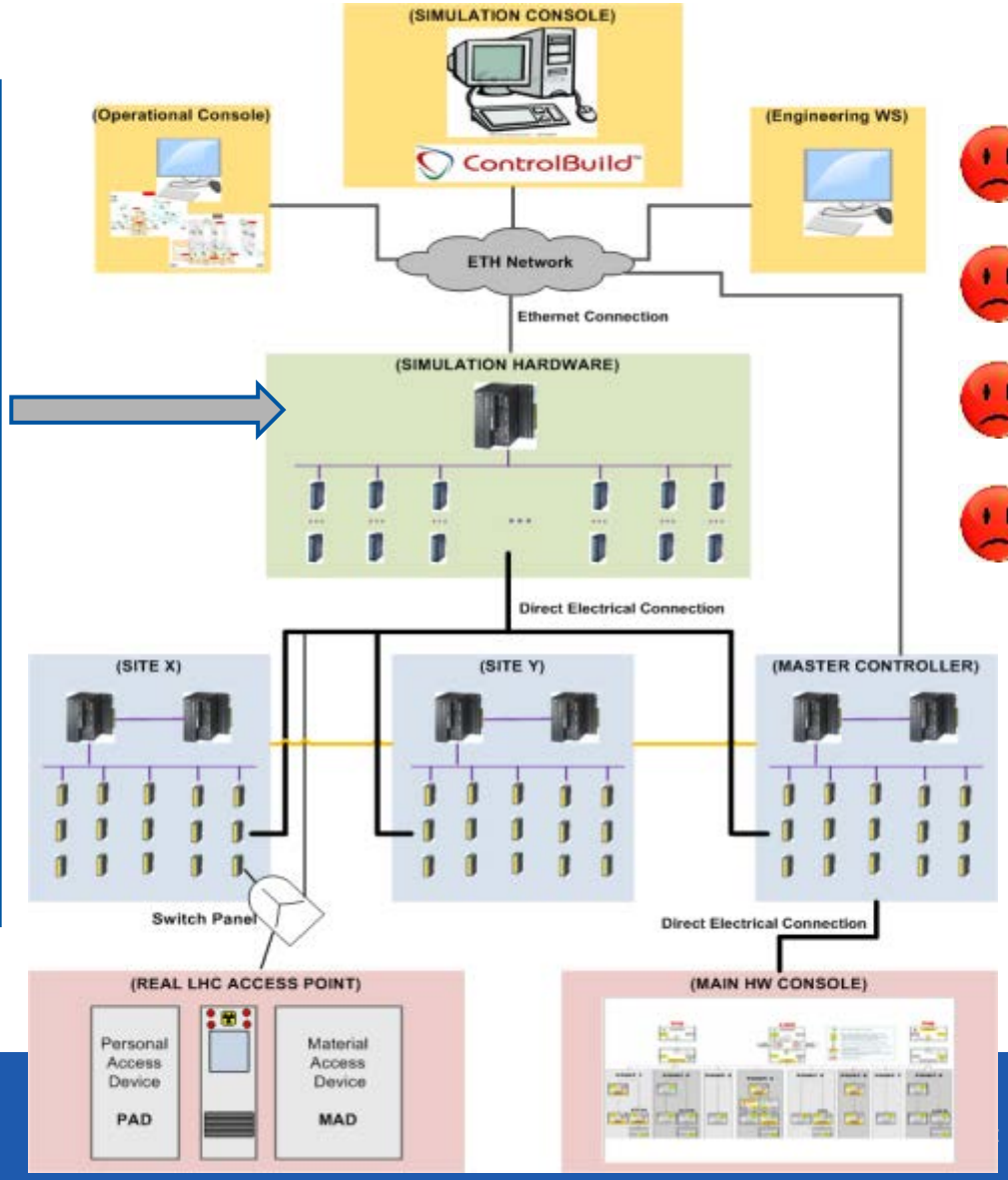
Safety Test Bench Conception

Classic Architectural Model Example



Safety Test Bench Conception

Classic Architectural Model Example



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