www.cern.ch

BE/ICS-CSE

Personnel Protection Systems at CERN

NI Big Physics Summit @ CERN - 11-12 February 2016

Authors: P. Ninin, F. Valentini

Outline

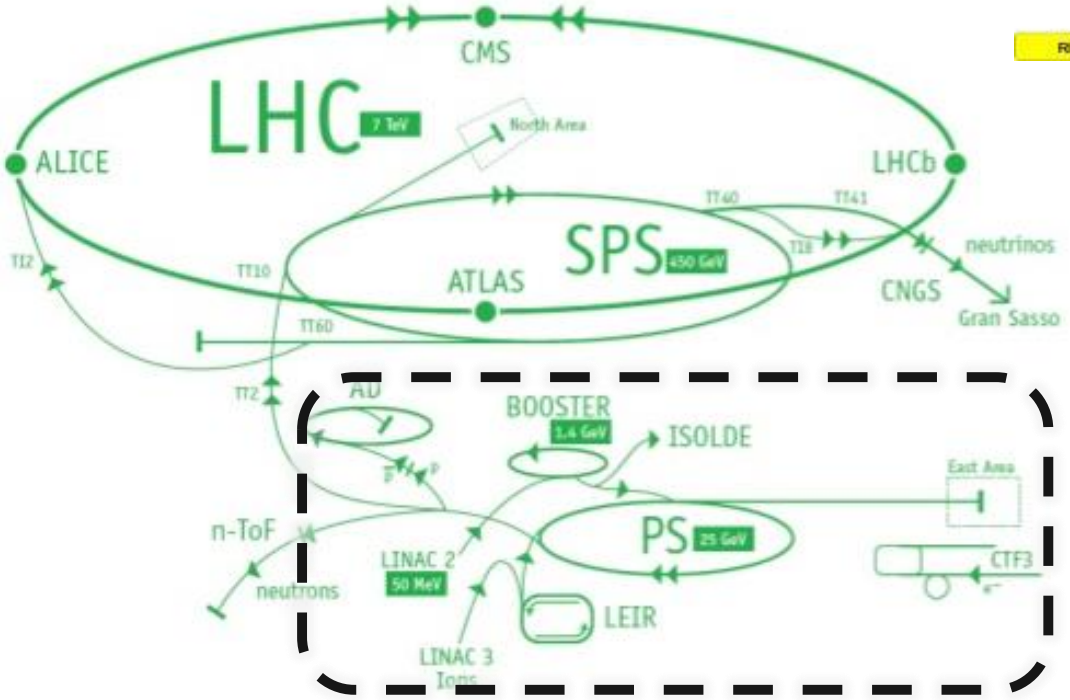
Personnel Protection Systems @ CERN

Development process (iec-61511)

Evaluation of NI Technology

Conclusions

What a PPS is?



Ionizing radiations hazards

Cryogenic (ODH) hazards

Electrical hazards

Magnetic field hazards

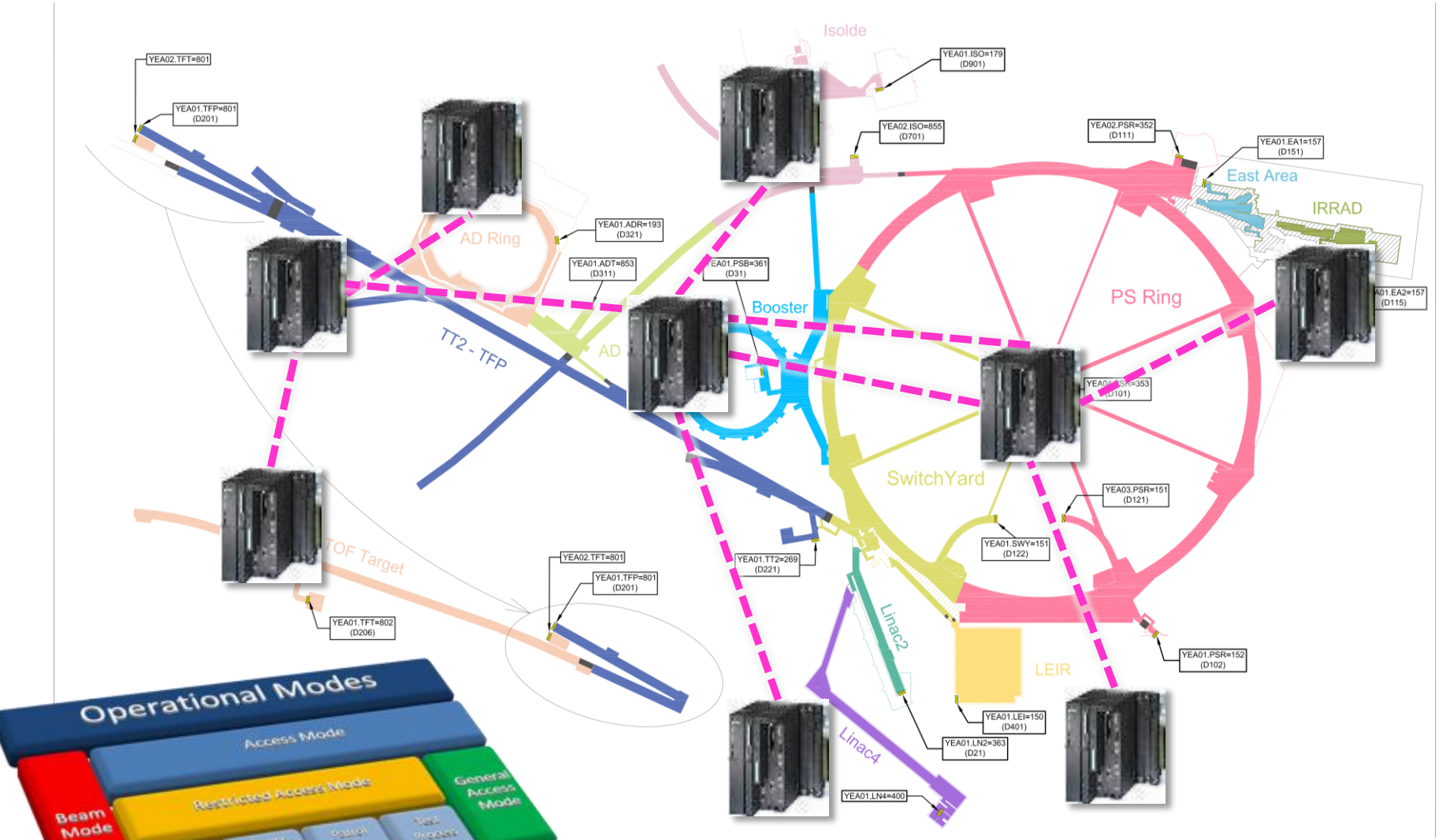
Laser hazards

Mechanical hazards

BEAM ON → **NO ACCESS**

ACCESS ON → **NO BEAM**

Primary Zones - PPS



Primary Zones - PPS

Fun-01 • **PAD - Access Cycle Management**. Implementation of all rules regulating the access cycles, control of the two doors motors and detection of *passage unicity*.

Fun-02 • **MAD - Access Cycle Management**. Implementation of all rules regulating the access cycles and control of the two doors motors.

Fun-03 • **MAD - Anti Intrusion Detection**. The internal volume is surveilled by two human detection systems based on motion detection and video image analysis algorithms.

Fun-04 • **Dynamic Information Dispatch**. Visualization of the state of the zone behind the access point. A graphical application drives the users during the access procedure.

Fun-05 • **Remote Supervision**. Publishing of diagnostic data related to the different subsystems to SCADA systems of Control Room Operators (e.g. Technical Infrastructure Monitoring - TIM).

Fun-06 • **Remote Maintenance**. The maintenance team needs to perform remote commands on different subsystem components (e.g. cut the power of certain devices).

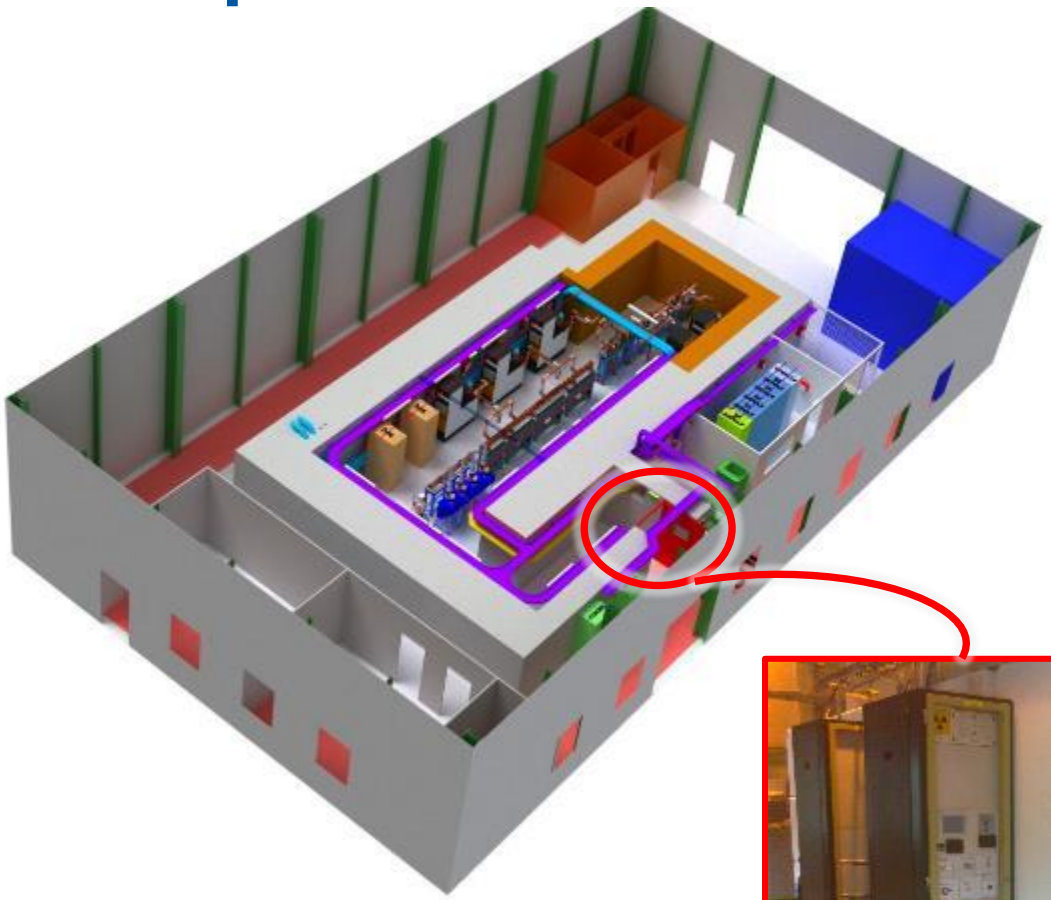
Fun-07 • **Personnel Safety Tokens Distribution**. Delivery of safety tokens to every user accessing the zone. The tokens are stored inside an electronically controlled distributor.

Fun-08 • **RFid User Identification**. An RFid reader is used to perform a first identification of the user and verify that he is in possession of a CERN radiation dosimeter.

Fun-09 • **Biometric User Identification**. A biometric identification is performed via an iris scanner to verify that the identity of person inside the PAD corresponds with the dosimeter id.

Fun-10 • **Access Privileges Verification**. The identity of the identified user is checked againt a central access database to verify that the user is holding all required credentials to access the zone.

Experimental Zones - PPS



Particularities:

- *Lower risks than in primary areas.*
- *Reduced facility size.*
- *Reduced number of I/O signals.*
- *Small population of trained users.*
- *Local operation of the system.*
- *Low realization cost requirements.*

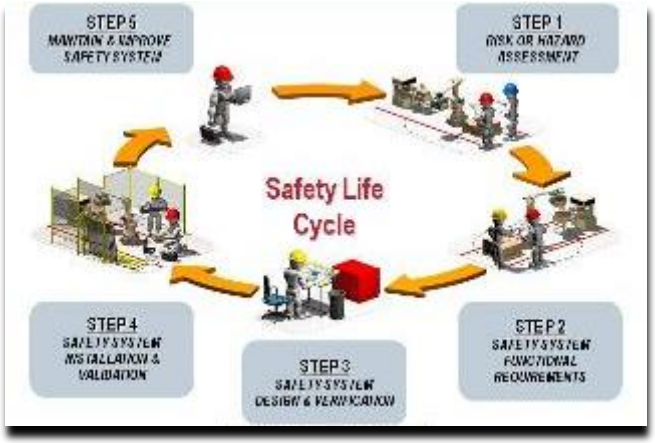
Outline

Personnel Protection Systems @ CERN

Development process (iec-61511)

Evaluation of NI Technology

Conclusions



Development Process (IEC-61511)

(1) Hazard Identification & Risks Assessment

Hazard ID *Hzd-1.3*	**LOCALIZATION:** M7 and M9 – Horizontal bunkers
Danger Exposure to X-ray emissions when tests take place in M7 or M9. Person inside the horizontal bunker.	**X-Rays generation** Conducting surfaces emit electrons when exposed to a properly oriented electromagnetic field. The emitted electrons follow complicated trajectories inside the cavities and ultimately land on the cavity walls originating X-ray emissions. The following are the main known operational parameters of M7 and M9: • **M7** → 1.2MW pulsed 352 MHz klystron supplied by 110 kV modulator at 50 Hz for Linac4 or SPL • **M7** → 10 kW 400MHz IOT for CRAB module • **M9** → 300 kW 400 MHz klystron supplied by 60 kV PC for LHC module • **M9** → 5x 500W 100 MHz solid state amplifier for HIE ISOLDE module REFERENCES: e-mail P. Maesen (22.09.2015).

SEVERITY OF EXPOSURE (C)	**Mitigating Barriers**	***RRF*: (RED_Csq)**
The consequence for the health of X-ray exposition depends directly from the quantity of radiation produced by the RF equipment. No available RP dose rates for low emission tests inside the horizontal bunkers. Hypothesis: risk of single exposure to a radiation higher than 2mSv. Measurements when high emission tests in V3 lead to 1Sv/h values inside V3 bunker. REFERENCES: e-mail P. Maesen (22.09.2015). EVALUATION: **D**	**(M1)** Evacuation sirens alerts before the start of operations. **(M2)** AUG button presents inside bunker. *Note: RP interlock is not considered as a mitigating barrier since monitors are not located where personnel stands inside the bunker area.*	**10**

INITIATING EVENT	**Exposure frequency**	**Preventive Barriers**	**Last Risk Rank**
(IE-01) ***Intrusion***. The possibility for a user to gain access by no respecting the physical barriers and access procedures when RF cavities are powered.	E[IE-01]= **1** *Event/Year*	**(P1)** RF flashing sign at the entrance indicating RF tests ON ***Reduction factor*** → (RED_IE-01): 10	**C3**
(IE-02) ***Undetected user***. A person is present in the area when the accelerating field of the cavities is active. This event may occur for an error of operation regarding the user or by a voluntary violation of access rules.	E[IE-02]= **0.03** *Event/Year*	**(P3)** Operational RF procedure that patrol the areas before RF is on. ***Reduction factor*** → (RED_IE-02): 10	**C2**
(IE-03) ***Unintended restart***. Because of an error of operation, RF cavities are powered while the access is granted to the area. This may be consequence of **one single** operation error.	E[IE-03]= **1** *Event/Year*	**(P4)** RF team ensures by procedure of electrical consignations that the RF modules are OFF when access is allowed to the bunkers. ***Reduction factor*** → (RED_IE-03): 10	**C3**

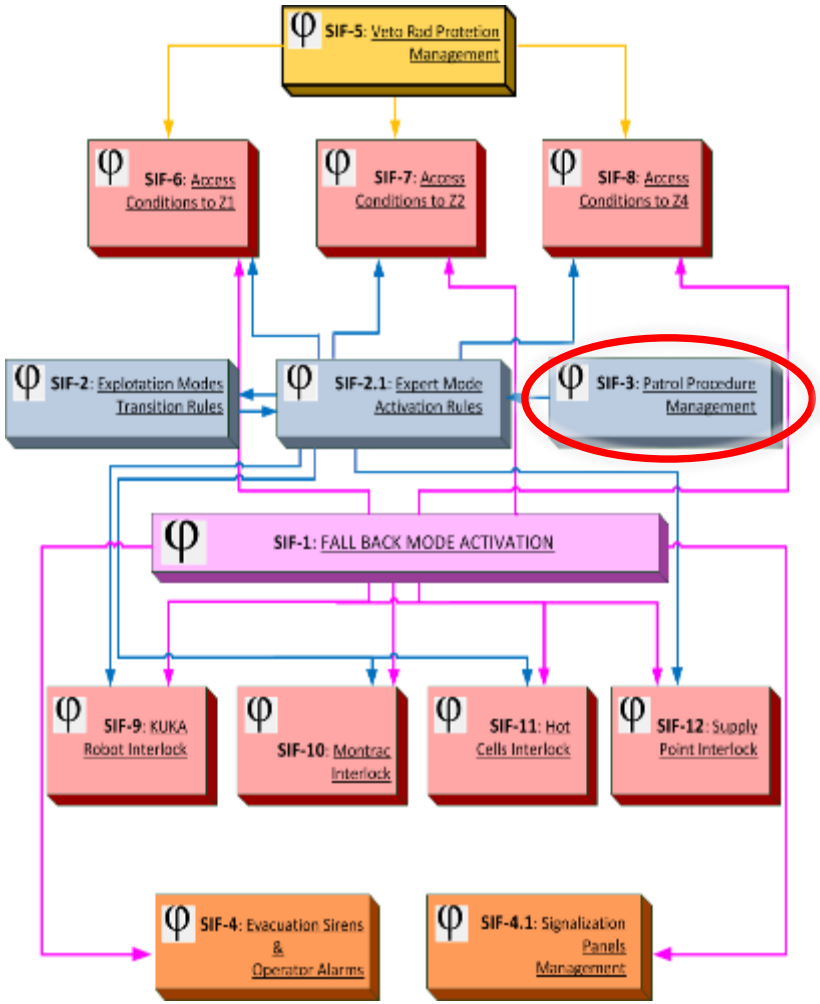
Risk evaluation		Probability of the hazardous event			
		Very low (1)	Low (2)	Medium (3)	High (4)
Potential severity	Minimal (A)	(A1)	(A2)	(A3)	(A4)
	Low (B)	(B1)	(B2)	(B3)	(B4)
	Medium (C)	(C1)	(C2)	(C3)	(C4)
	High (D)	(D1)	(D2)	(D3)	(D4)

FINAL RISK RANK: C3

RISK REDUCTION FACTOR (RRF): ***1000***

Development Process (IEC-61511)

(2) System formal specification by Safety Instrumented Functions (SIF)



TRIGGERING EVENT-CONDITIONS FOR *PATROL PROCEDURE* ACTIVATION ON SECT X{1..3}:

(MODE_Acce=1) Λ (ACCE_Patrol_Sx=0) Λ (AUG=1) Λ (Patrol_Sx_ON=1)

OUTPUT → **ACCE_Patrol_Sx = 1**
OUTPUT → **PB_x_Arm = 0** {All patrol boxes of sector X are disarmed}
OUTPUT → **Sx_Srch = 0**

TRIGGERING EVENT- CONDITIONS FOR *PATROL PROCEDURE* QUIT ON SECT X{1..3}:

(MODE_Acce=0) V (Patrol_Sx_OFF=1)

OUTPUT → **ACCE_Patrol_Sx = 0**

TRIGGERING EVENT- CONDITIONS FOR GENERAL DISARMING OF A SECT DURING PATROL:

(ACCE_Patrol_Sx=1) Λ (Sx_Srch=1) Λ (YY_Pos=0) {YY_Pos = access door position for sector X}

OUTPUT → **PB_x_Arm = 0** {All patrol boxes of sector X are disarmed}
OUTPUT → **Sx_Srch = 0** {The search of sector X is disarmed}

TRIGGERING EVENT- CONDITIONS FOR PATROL BOX (SECT 1, PB1-ext) ARMING:

(ACCE_Patrol_S1=1 Λ S2_Srch=1 Λ PZ01_Pos=1 Λ MM01_Pos=1 Λ PB_2_Arm=1 Λ PB1_Arm_Req=1)

OUTPUT → **PB_1_Arm = 1**
OUTPUT → **S1_Srch = 1**

TRIGGERING EVENT- CONDITIONS FOR PATROL BOX (SECT 1, PB2-int) ARMING:

(ACCE_Patrol_S1=1 Λ PB2_Arm_Req=1)

OUTPUT → **PB_2_Arm = 1**

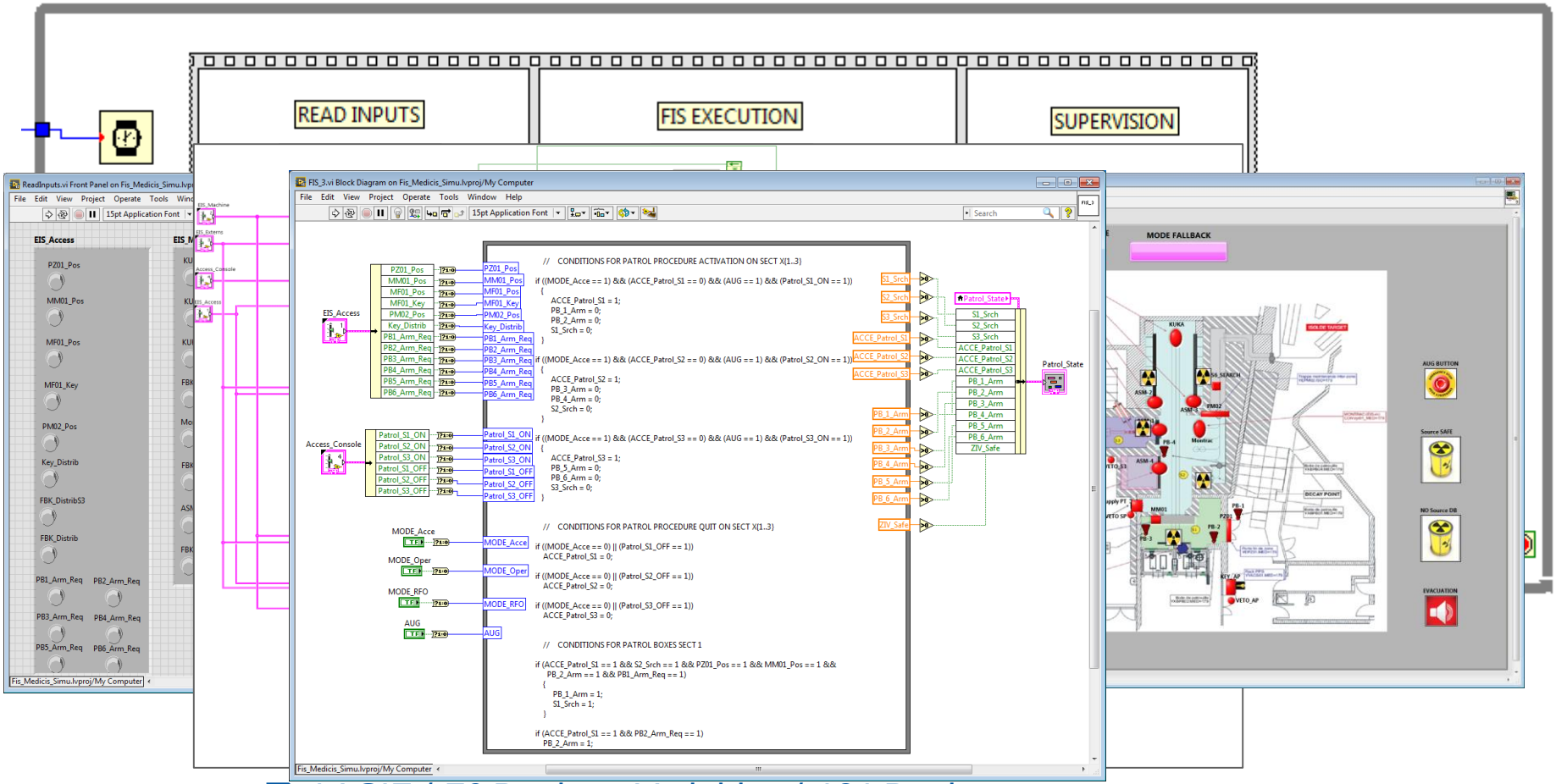
TRIGGERING EVENT- CONDITIONS FOR PATROL BOX (SECT 1, PB1-ext) DISARMING:

(ACCE_Patrol_S1=0 Λ (PZ01_Pos = 0 V (MM01_Pos=0 Λ S2_Srch=0)))

OUTPUT → **PB_1_Arm = 0**
OUTPUT → **S1_Srch = 0**

Development Process (IEC-61511)

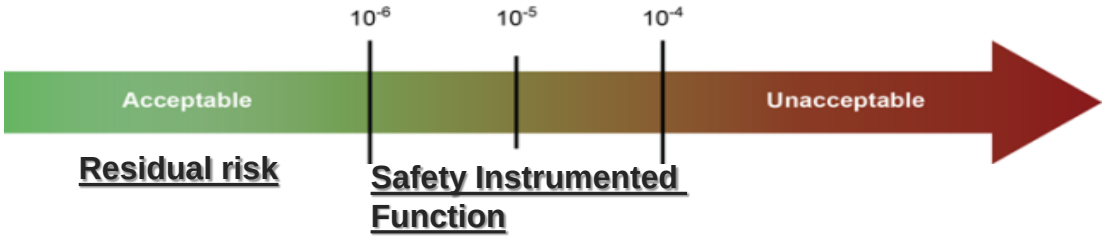
(3) Formal Verification of Safety Functions



- *14* SIF / *70* Boolean Variables / *121* Boolean operators

Development Process (IEC-61511)

(4) Safety Integrity Level (SIL) Allocation to SIF



Safety Integrity Level	Demand Mode of Operation (average probability of failure to perform its design function on demand - PFD)	Continuous / High Demand Mode of Operation (probability of a dangerous failure per hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

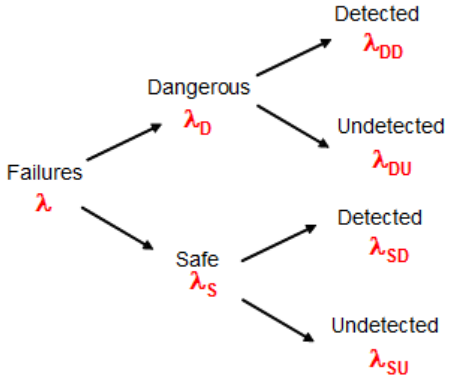
SIL Interpretation

- **Probability of failure of the SIF in ensuring its mission.**
- **Factor of risk reduction to be provided by the SIF.**

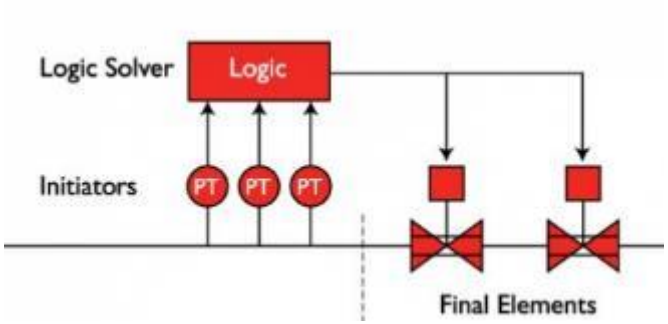
Development Process (IEC-61511)

(5) SIL Demonstration

Failure Rate:



SIF Architecture:



Safe Failure Fraction (SFF):

The percentage of failures that do not prevent the safety function to ensure its mission.

Mission Time (T):

It is the period of time after which the device is fully verified and all undetected faults can be revealed.

Statistical Model:

$$F(t) = 1 - e^{-\lambda_{DU} t}$$

Outline

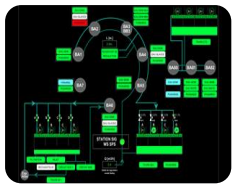
Personnel Protection Systems @ CERN

Development process (iec-61511)

Evaluation of NI Technology

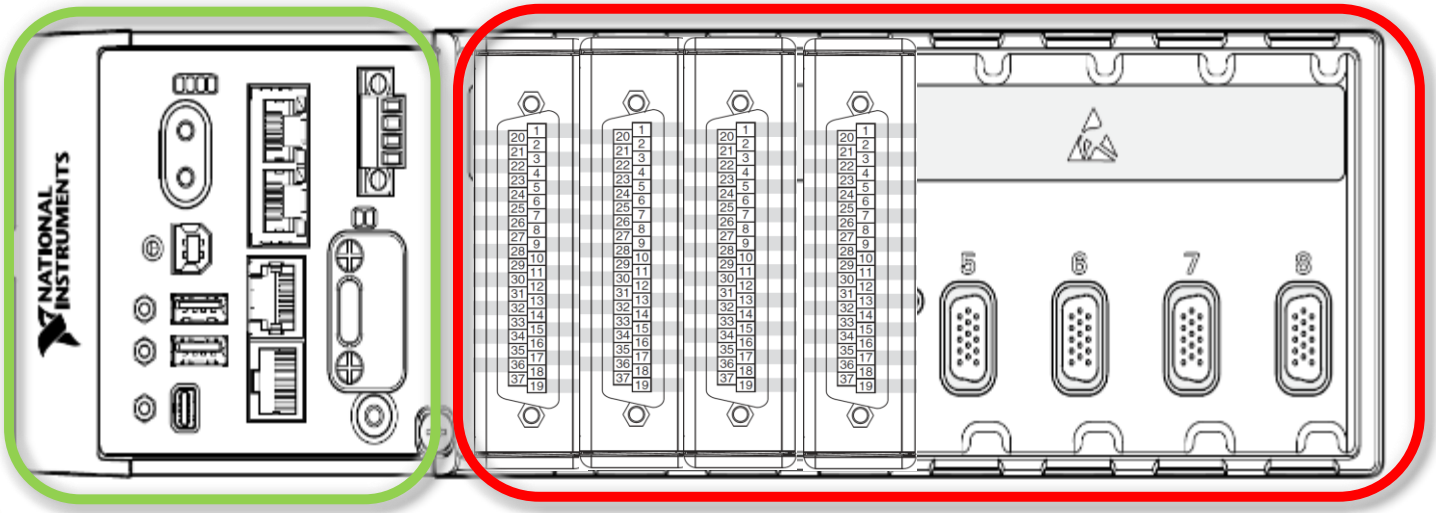
Conclusions

Evaluation of NI cRIO 903x



Standard Program

Safety Program (SIF execution)



Linux RT

FPGA

Conclusions

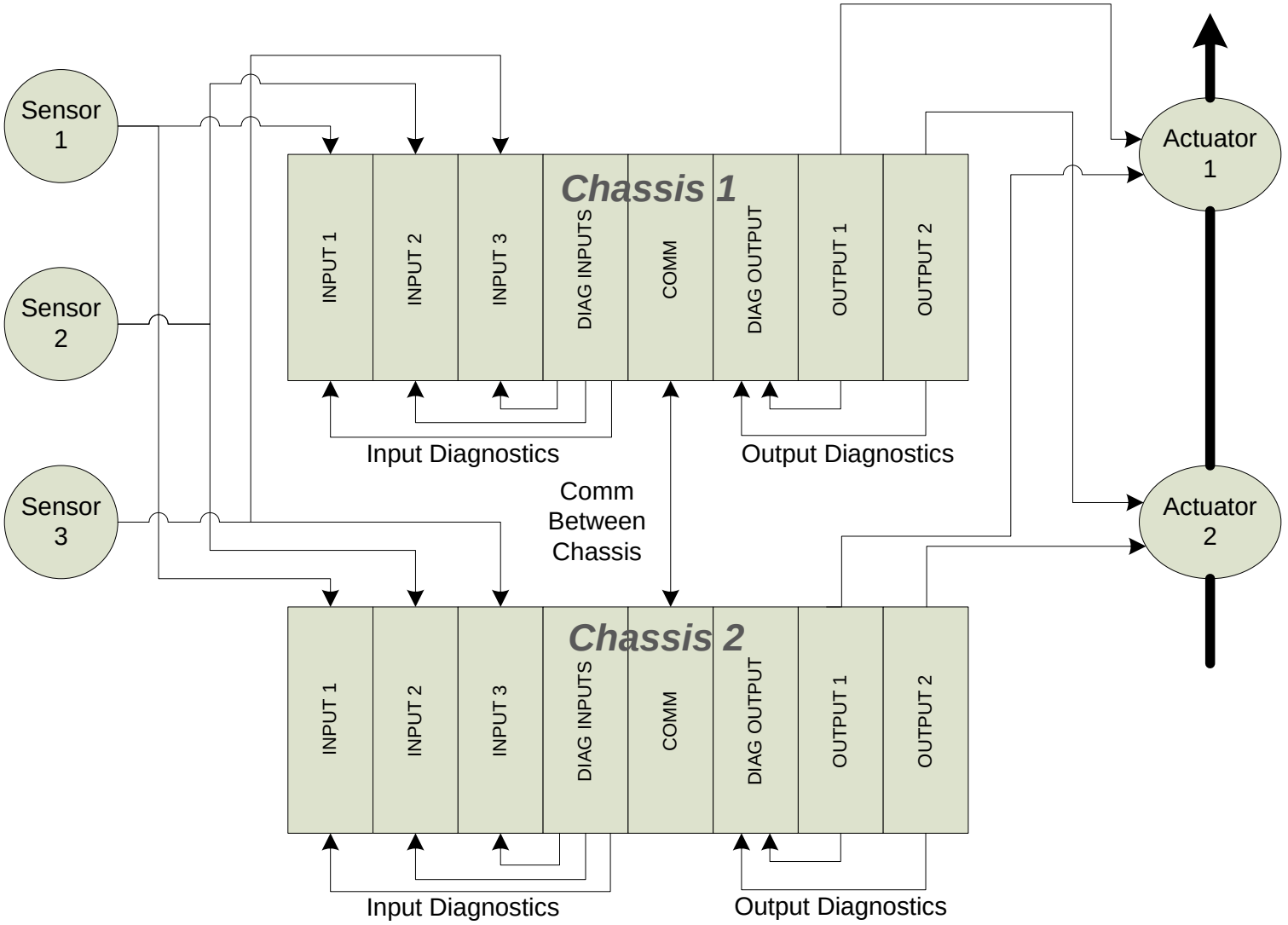
Possible improvements of NI technology for safety related applications:

- Provide mechanisms to easy handle I/O channels **redundancy**.
- Provide automatic **auto-diagnostic** functionalities at level of I/O modules and at level of FPGA in order to increase SFF.
- Provide more precise **reliability data**, estimation of dangerous failures (FMEA study).
- TUV **certification** it is not mandatory but it is required by systems integrators and it is a good way to ensure a qualitative development process.

www.cern.ch

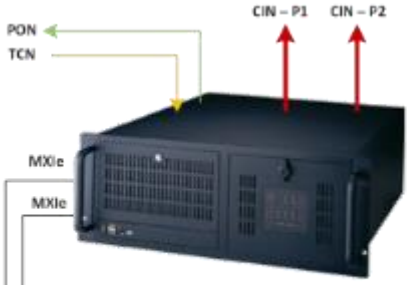
Fast PIS – Hardware Architecture

Slide from *Luis Fernandez-Hernando* (ITER)



CCPS architecture

Slide from *Luis Fernandez-Hernando* (ITER)



HOST
Red Hat linux CODAC compliant
Connected to CODAC and to CIS

Chassis A
NI 9159
14 Slots

Chassis B
NI 9159
14 Slots