# Functional Safety Activities (3)

ALBA – CERN workshop

Borja Fernández Adiego BE/ICS

# Safety management and test proof catalogue (some tips)

- **IEC 61508 (or IEC ) safety concepts** should be consider at the design time
  - Possibility to select the instrumentation for the SIFs
  - Possibility to select the architecture for the SIFs (redundancy, etc.)
  - Possibility to include other risk reduction measures
  - Possibility to include protection barriers

- **Sources of safety information is a real challenge**
  - Site specific (Currently there is no failure records at CERN, at least for most of devices)
  - Industry specific
  - Generic (large number of applications)
  - Manufacturer data

- **Systematic Safety Integrity (software measures)**
  - Simplicity in the safety program (when possible)
  - Testing strategy
  - Formal verification can be applied to the PLC program (PLCverif)

- **Hardware safety integrity usually** cannot be proven, but we reasonably increased the safety of the system:
  - Proven in use techniques can be applied in certain cases
  - Consider architectural constrains, not only hardware random failures

# Safety management and test proof catalogue (some tips)

- The **frequency of the proof tests (T)** has a big impact in the **Hardware safety integrity**

$$PFD = \lambda_D . \frac{T}{2}$$

- Outputs of the safety analysis: Safety report and recommendations (test proof catalogue)

- Management of the safety system is critical