Equipment Protection System (EPS) for ePIC
Life cycle of EPS development

Prashanth

November 13, 2025

Slow Controls Scope Workshop with EIC Controls

Electron-Ion Collider

Developing a Safety PLC System for Equipment Protection in DOE Experiments

- An **Equipment Protection System (EPS)** uses a Safety PLC to monitor and interlock experiment subsystems to prevent **damage, unplanned downtime, or unsafe equipment operation/states**
- It complements — but is distinct from — the **Personnel Safety System (PSS** DOE O 420.2D)
- Not credited as personal safety, still meet **DOE quality and reliability standards** and often adopts **functional safety principles (IEC 61508 / IEC 61511 / ISO 13849) or** internal lab standards, but not DOE O 420.2D directly
- **Equipment protection system should include personal protection**, especially when equipment hazards could indirectly endanger personnel or cause major operational losses
- The building infrastructure has its own HSSD, sprinkler system, and ODH monitoring, which are managed separately under facility safety systems but can handshake with the EPS for coordinated safety actions

1. Define Scope and System Boundaries

- Identify:
  - **What EPS protects** (e.g., magnet, electronics, gas chambers/ systems, vacuum chambers, detectors, power supplies)
  - **Key process variables:** temperature, flow, vacuum, current, voltage, pressure, etc.
  - **Interfaces:** PLC/HMI, control system (EPICS), hardware I/O, alarms, data logging, and shutdown circuits (e.g-shunt-breakers)
  - **How EPS protects** Automatically brings systems to a safe equipment state (e.g., power-down, isolation, or venting)
- Output documents:
  - Equipment Protection Requirements Specification (EPRS)
  - Interface Control Document (ICD)
  - Functional Block Diagram showing signal flow and safety logic

2. Perform Hazard and Failure Analysis

- Identify what could go wrong and what happens if it does
- Tools: Perform structured analysis such as:
  - FMEA (Failure Mode and Effects Analysis)
    - Structured, systematic process used to identify how a system or component can fail, determine the effects of those failures, and prioritize actions to reduce or eliminate the risks
  - What-If analysis
- Identify:
  - **Failure modes that could damage equipment** (e.g., loss of cooling, overcurrent, vacuum loss, power fault)
  - **Detection and mitigation methods** (interlocks, shutdowns, bypass timers)
  - **Criticality ranking** — use risk reduction factors to prioritize controls
- Output: Document the results in a **Hazard & Risk Analysis Report**, forming the foundation for functional safety design

3. Determine Reliability Targets

- Define *how reliable* the system must be to prevent or control those failures
- **Quantifying how dependable** a system, subsystem, or component must be to achieve acceptable performance or safety levels
- For DOE experiments, equipment protection functions are typically Safety Integrity Levels (**SIL) 1–2** (moderate integrity):
  - SIL 1: Prevents costly downtime or component replacement.
  - SIL 2: Prevents major hardware loss or long recovery (e.g., magnet quenches, cryogenic rupture)
  - SIL 3 is for personal protection, not applicable here
- Use **IEC 61508** or **IEC 61511** to assign target SIL for each function and justify these based on hazard severity and occurrence likelihood

4. Select Safety PLC Platform and Architecture

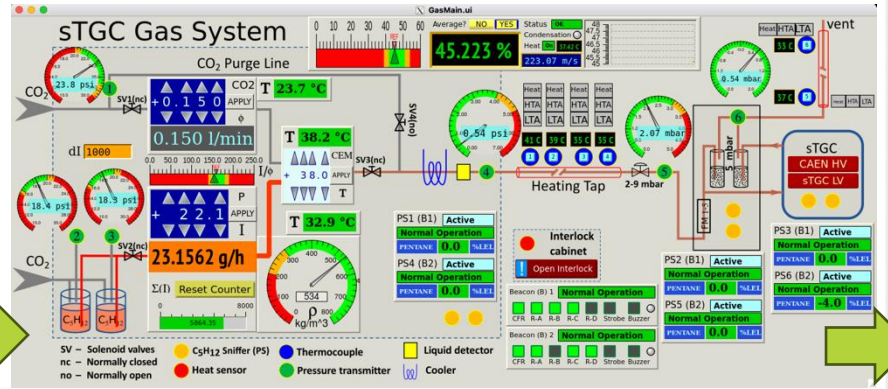
- Choose a **TÜV-certified Safety PLC** suitable for industrial or experimental environments:
  - Redundant CPU and safety task separation (1oo2, 2oo3 voting system)
  - Fail-safe digital and analog I/O modules
  - Internal diagnostics for stuck bits, communication faults, watchdogs
- Design **fail-safe logic**:
  - **De-energize-to-safe** outputs (e.g., open valve, inhibit current)
  - Redundant sensors for critical parameters (dual pressure transducers, dual thermocouples/heat fire sensors)
  - Trip relays or hardware interlocks for final shutdown actions
  - Include **self-diagnostic routines** for stuck signals, communication errors, and analog drifts

Allen-Bradley GuardLogix safety PLC
And Safety IO cards

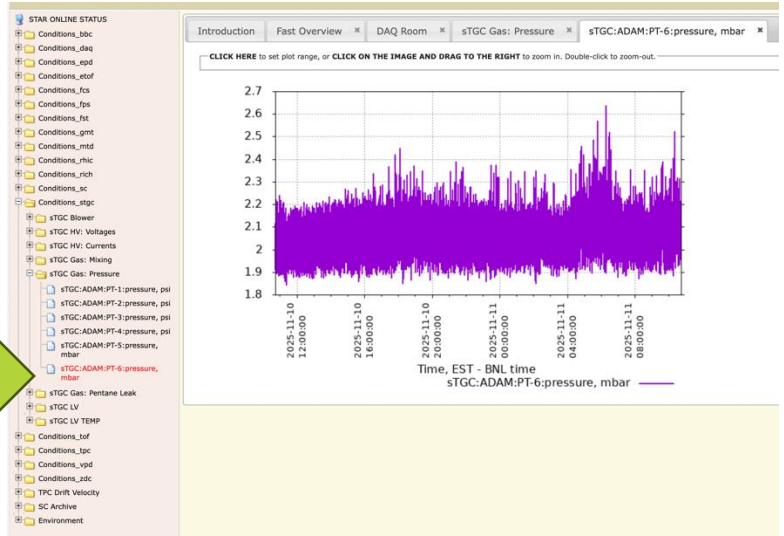
5. System Integration and Interfaces

- Integrate EPS safely with experiment control systems:
  - Communicate with supervisory control (EPICS) via **read-only safety data** channels
  - Avoid allowing non-safety systems to modify safety logic or parameters
  - Include watchdog signals between PLC and control system to detect communication failure
  - Ensure hardwired outputs to physical interlocks (e.g., inhibit signals to power supplies, HV relays).

PLC/HMI



EPICS monitor



Archive PVs
STAR sTGC Gas system

6. Cybersecurity and Configuration Management

- EPS falls under **DOE cybersecurity and QA oversight**
- ICS segmentation, firewalling, and secure programming (NIST SP 800-82/ DOE O 205.1C?)
- All code and logic revisions must be versioned and reviewed
  - Implement configuration control per **DOE O 414.1D** - QA (?)

7. System Design and Verification

- Develop logic (structured text or ladder diagram)
- Each interlock or protection function traceable to a hazard or design requirement
- Peer review and independent verification
- Simulate fault conditions (loss of signal, out-of-range, stuck-on) during testing
- Maintain traceability from **Requirement** → **Implementation** → **Verification** in the EPRS (Equipment Protection Requirements Specification)

8. Testing and Commissioning

- Develop formal tests:
  - Factory Acceptance Test (FAT): Validate PLC configuration and basic logic operation.
  - Site Acceptance Test (SAT): Validate I/O mapping, field devices, trip sequences, and reset behavior.
  - Proof Testing: Define periodic testing intervals for each function (typically 12 months at BNL).
- Test scenarios might include:
  - Loss of cryo flow → magnet ramp-down
  - Cooling water temperature > threshold → trip shunt-trips
- All test results are logged under DOE QA records
  - In a recent audit these logs were produced to DOE at RHIC

9. Operation, Maintenance, Change Control & Periodic Revalidation

- Establish procedures for:
  - Normal operation and reset sequences
  - Maintenance mode (bypass logic) with controlled access and documented duration
  - Periodic proof testing with calibration of sensors and verification of trip points
  - Change control through an **Engineering Change Request (ECR)** process
  - Training & Conduct of Operations
    - Train operators/maintainers on the safety system, abnormal response, impairments, lockout/tagout
- (?)Use **DOE O 433.1B** principles for graded maintenance and recordkeeping

10. Documentation and Review

- Maintain the following documentation set:
  - Equipment Protection Requirements Specification (EPRS)
  - Functional Design Specification (FDS)
  - Logic diagrams, I/O maps, and safety architecture drawings
  - Test and proof-test procedures
  - Maintenance plan and QA records
  - Configuration management logs

Summary

- The **Equipment Protection System (EPS)** safeguards experiment hardware and infrastructure — **not personnel**
- It is **non-credited**, but must follow **DOE QA, maintenance, cybersecurity, and conduct of operations** requirements
- Use **IEC 61508/61511** functional safety lifecycle to ensure reliability, diagnostics, and predictable failure behavior
- Maintain rigorous **testing, documentation, and configuration control** comparable to personnel safety systems

Applicable DOE Orders and Guidance for Equipment Safety

Directive / Order	Title / Scope	Relevance to EPS / PSS Projects	Key Requirements / Focus
DOE O 420.2D	*Safety of Accelerator Facilities*	Primary DOE order governing **Personnel Safety Systems (PSS)** and accelerator operational safety.	• Defines PSS requirements (access control, beam interlocks) • Requires protection of personnel from radiation and hazardous energy • Establishes **Accelerator Safety Envelope (ASE)** and **Safety Assessment Document (SAD)** • EPS systems must complement, but remain **distinct** from PSS.
DOE O 420.1C	*Facility Safety*	Covers **facility-level safety**: fire protection, criticality, and natural phenomena hazards.	• May apply to large detector halls or experimental enclosures • Requires design to resist seismic, fire, and structural hazards • EPS equipment protection may be derived from facility safety needs.
DOE O 413.3B	*Program and Project Management for the Acquisition of Capital Assets*	Governs **project design and lifecycle** for DOE capital projects (e.g., large detector or beamline upgrades).	• Requires safety integration into design (safety-in-design) • Mandates **Preliminary and Final Design Reviews** (PDR/FDR) including EPS/PSS • Requires risk management and configuration control of safety systems.
DOE O 414.1D	*Quality Assurance*	Applies to all DOE R&D and engineering activities.	• Requires formal **QA program** for system design, calibration, verification, and testing • EPS and PSS design, logic verification, and documentation fall under QA control.
10 CFR 851	*Worker Safety and Health Program*	Federal regulation protecting DOE and contractor employees.	• Requires implementation of **safety and health management systems** • Equipment design must minimize worker hazards • Aligns with OSHA, NFPA, and ANSI codes.
DOE G 420.2-1A	*Implementation Guide for DOE O 420.2D*	Provides detailed **guidance and best practices** for implementing accelerator safety.	• Defines methodology for SAD, ASE, and hazard analysis • Clarifies relationship between EPS and PSS • Recommends graded approach for system reliability and documentation.
DOE O 232.2A	*Occurrence Reporting and Processing of Operations Information*	Defines requirements for **reporting and investigating** safety-related events or system failures.	• EPS and PSS faults that lead to operational interruptions or safety events must be analyzed and reported.
DOE O 231.1B	*Environment, Safety, and Health Reporting*	Covers general **safety performance reporting** across DOE sites.	• Requires documentation of reliability and system safety performance metrics • Supports continuous improvement of EPS/PSS reliability.
DOE O 151.1D	*Comprehensive Emergency Management System*	Governs **emergency response planning** for DOE facilities.	• EPS and PSS must interface with emergency systems (e.g., E-Stop, alarms, evacuation interlocks).
DOE P 450.4A	*Integrated Safety Management Policy (ISMP)*	DOE-wide **safety management policy** integrating safety into all work activities.	• Requires following the ISM principles: define scope, identify hazards, develop controls, perform work safely, and feedback for improvement • Foundation for all safety documentation, including EPS/PSS lifecycle management.

International and Industry Standards for Equipment safety

Standard	Purpose / Relevance
IEC 61508 / IEC 61511	Functional safety standards for electrical/electronic/programmable systems. Used to define **Safety Integrity Levels (SIL)** for EPS/PSS.
ISO 13849	Safety-related control system design for machinery — relevant for **equipment safety functions**.
IEC 60812	FMEA methodology — used for EPS and PSS hazard analysis.
ISO 31010	Risk assessment techniques (What-If, HAZOP, Fault Tree).
NFPA 70 / 79 / 497	Electrical and industrial safety codes governing wiring, grounding, and control system safety.
ASME / ANSI / IEEE Standards	Used for cryogenic, vacuum, mechanical, and interlock system compliance (depending on subsystem).
NIST SP 800-82 / IEC 62443	Cybersecurity for ICS. Segmentation, patching, secure remote access

Integration of DOE Orders/Directives to above 10 steps

Design Phase	Applicable Directives / Standards	Key Deliverables
Conceptual Design	DOE O 413.3B, DOE P 450.4A	What-If Analysis, Concept Hazard Review
Preliminary Design	DOE O 420.2D, DOE G 420.2-1A, 10 CFR 851	FMEA, EPRS (Equipment Protection Requirements Specification), ICD (Interface Control Document)
Final Design	DOE O 414.1D, IEC 61508/61511	SSVM (Safety System Validation Matrix), Logic Diagrams, QA Documentation
Commissioning / Operations	DOE O 232.2A, DOE O 231.1B	Test Reports, Safety Basis Documentation, Occurrence Reporting
Maintenance / Review	DOE O 420.1C, DOE O 151.1D	Calibration, Requalification, Emergency Integration

Compliance Matrix

EPS Document / Element	Purpose / Description	Applicable DOE Directives / Requirements	Supporting Technical Standards / Guides	Key Deliverables / Compliance Requirements
EPRS (Equipment Protection Requirements Specification)	Defines all EPS protective functions, safe states, interlocks, and equipment fault responses.	• **DOE O 420.2D** – Safety of Accelerator Facilities (equipment protection complement to PSS) • **DOE O 414.1D** – Quality Assurance (design control & traceability) • **10 CFR 851** – Worker & equipment safety	• **IEC 61508 / 61511** – Functional safety • **ISO 13849** – Machine safety • **IEC 60812** – FMEA methodology	• Identify protection functions and hazards • Define safe states and reliability targets (SIL/PL) • Provide traceability to FMEA and validation plan
ICD (Interface Control Document)	Defines electrical, logical, and data interfaces between EPS, PSS, and control systems (e.g., EPICS).	• **DOE O 413.3B** – Design & configuration integration • **DOE O 420.2D** – Defines EPS–PSS boundaries • **DOE O 414.1D** – QA & configuration management	• **IEEE 1220** – Systems engineering process • **INCOSE SE Handbook**	• Define all interface signals and protocols • Include ownership, fault response, and grounding • Joint review by responsible system engineers
FMEA (Failure Modes and Effects Analysis)	Identifies potential failure modes, their effects, and required mitigations for EPS hardware and logic.	• **DOE O 420.2D** – Hazard identification • **DOE O 413.3B** – Risk management in design	• **IEC 60812** – FMEA • **ISO 31010** – Risk assessment • **IEC 61508** – Safety integrity allocation	• Analyze component and system failure modes • Determine severity, occurrence, detection • Link risk mitigations to EPRS functions
Reliability Target / SIL Assignment	Defines quantitative reliability goals and required Safety Integrity Levels (SIL) for EPS functions.	• **DOE O 420.2D** – Reliability commensurate with hazard • **DOE O 414.1D** – QA of reliability documentation	• **IEC 61508 / 61511** – SIL methodology • **ISO 13849** – Performance Level approach	• Assign SIL/PL levels per function • Allocate reliability to sensors, logic, actuators • Document basis in EPRS and validation plan
SSVM (Safety System Validation Matrix)	Maps each EPS safety function to its validation test and acceptance criteria.	• **DOE O 414.1D** – QA verification & validation • **DOE O 420.2D** – Accelerator safety verification	• **IEC 61508** – Validation methods • **ISO 9001** – QA processes	• Define test steps, expected results, and frequency • Trace each test to EPRS requirement • Capture pass/fail and sign-off records
Analog / Sensor Calibration Plan	Defines procedures for maintaining measurement accuracy and detecting analog drift.	• **DOE O 414.1D** – QA calibration & test control • **10 CFR 851** – Worker/equipment safety compliance	• **IEC 61508** – Diagnostic coverage • **ISO 10012** – Measurement management	• Define calibration intervals and tolerances • Record traceable calibration data • Address analog drift detection and correction
EPS Logic Design & PLC Configuration	Details the PLC or logic solver implementation ensuring safe operation and fail-safe design.	• **DOE O 420.2D** – Functional safety implementation • **DOE O 414.1D** – Software QA and design control	• **IEC 61131-3** – PLC programming standard • **IEC 61508 Part 3** – Software safety lifecycle	• Provide structured, modular PLC logic • Implement watchdogs, diagnostics, redundancy • Maintain controlled versioning and change logs
Testing & Commissioning Records	Verification of all EPS functions and interlocks prior to operation.	• **DOE O 420.2D** – Startup safety approval • **DOE O 414.1D** – QA verification & validation	• **IEC 61508 / 61511** – Proof test and validation • **IEEE 7-4.3.2** – PLC-based safety systems testing	• FAT/SAT documentation with pass criteria • Link results to SSVM • Ensure independent validation witness
Configuration Management & Change Control	Ensures all EPS logic, documentation, and test results remain under controlled revision.	• **DOE O 414.1D** – QA configuration control • **DOE O 413.3B** – Project design baseline management	• **ISO 9001** – Quality system • **DOE G 413.3-10** – Configuration management guide	• Document logic revisions, approvals, and test revalidation • Maintain controlled document repository
Occurrence Reporting / Event Logging	Reporting and analysis of EPS-related faults or unsafe conditions.	• **DOE O 232.2A** – Occurrence reporting • **DOE O 231.1B** – ES&H reporting	• **DOE Manual 231.1-2** – Reporting process	• Record EPS faults and failure events • Submit reports as required • Track corrective actions and recurrence prevention
Operational Readiness Review (ORR)	DOE's final verification before operational approval of EPS.	• **DOE O 420.2D** – Safety readiness • **DOE O 413.3B** – Project completion criteria	• **DOE G 413.3-9** – ORR implementation guide	• Present all EPS documentation (EPRS, SSVM, FMEA, calibration) • Demonstrate tested reliability and safe operation