The Raster Scanning Magnet System and ESS Machine Protection

Christian Hilbes
Institute of Applied Mathematics and Physics - School of Engineering
Zürich University of Applied Sciences ZHAW
E-Mail: hilc@zhaw.ch

Danfysik A/S - Taastrup
2016-06-22

Collaboration ESS and ZHAW

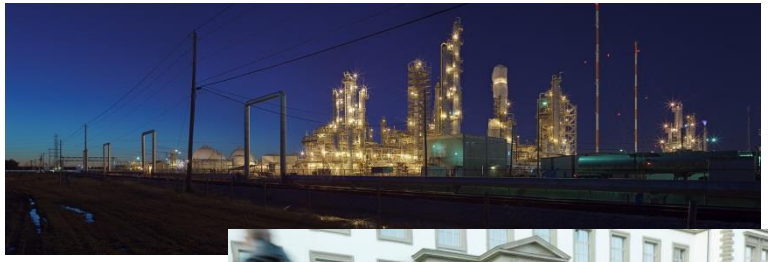
EUROPEAN SPALLATION SOURCE

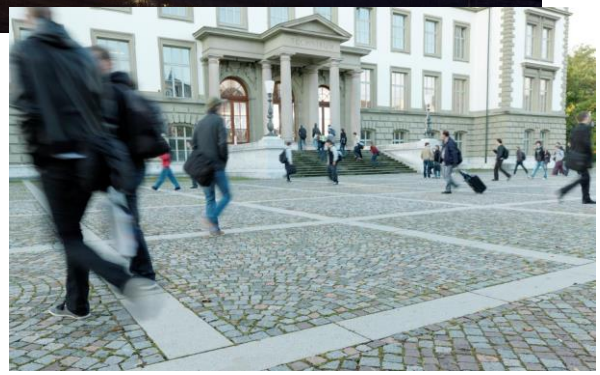
School of Engineering
IAMP Institute of Applied Mathematics and Physics

- ZHAW supports ESS with respect to
  - Machine Protection System-of-Systems Engineering following IEC 61508, including support for
    - overall architectural design and integration of constituent systems.
    - End-to-End Verification and Validation (Protection Integrity Level Assessment) of all Protection Functions.
  - Raster Scanning Magnet System Hazard and Risk Analysis
  - RSMS Local Protection System (aka “ESS Raster Fault Detection Unit”) Specification and Design
  - Real-time Hardware-in-the-Loop Simulator for “ESS Raster Fault Detection Unit” Verification and Validation

About myself…

- Christian Hilbes
  - Physics Diploma ETH Zürich
  - PhD Experimental Particle Physics
    ETH / PSI
  - Research Associate Center for Proton
    Therapy – PSI **(3d p-beam Scanning)**
  - Head Therapy-Control and Patient-Safety-Systems
    CPT – PSI
  - Product Safety Manager Rheinmetall Air Defence AG
  - Co-Founder SafeCert Consulting GmbH
  - Lecturer IAMP: Physics, RAMS, Risk-Management
  - Head **Safety-Critical Systems Research Lab** at the Institute of Applied Mathematics and Physics
  - TÜV Süd Certified Functional Safety Professional IEC 61508/IEC61511





ESS Machine Protection

- Purpose
  - Support the high availability requirement of ESS.
- Capability Objectives
  - Prevent and mitigate damage and unnecessary activation
    - of any part of the machine
    - be it beam-induced or from any other source
    - in any operating condition
    - in any lifecycle phase
    - in accordance with availability requirements.

ESS Machine Protection

- Purpose
  - Support the high availability requirement of ESS.
- Capability Objectives
  - Minimize Downtime
    - Minimize spurious trips probability.
    - Provide adequate level of support for fault diagnostics and analysis.
    - Support operation in degraded mode
      - in case of failure of parts of the machine.
      - in case of failure of protection functions.
    - Include concepts for preventive and predictive maintenance.

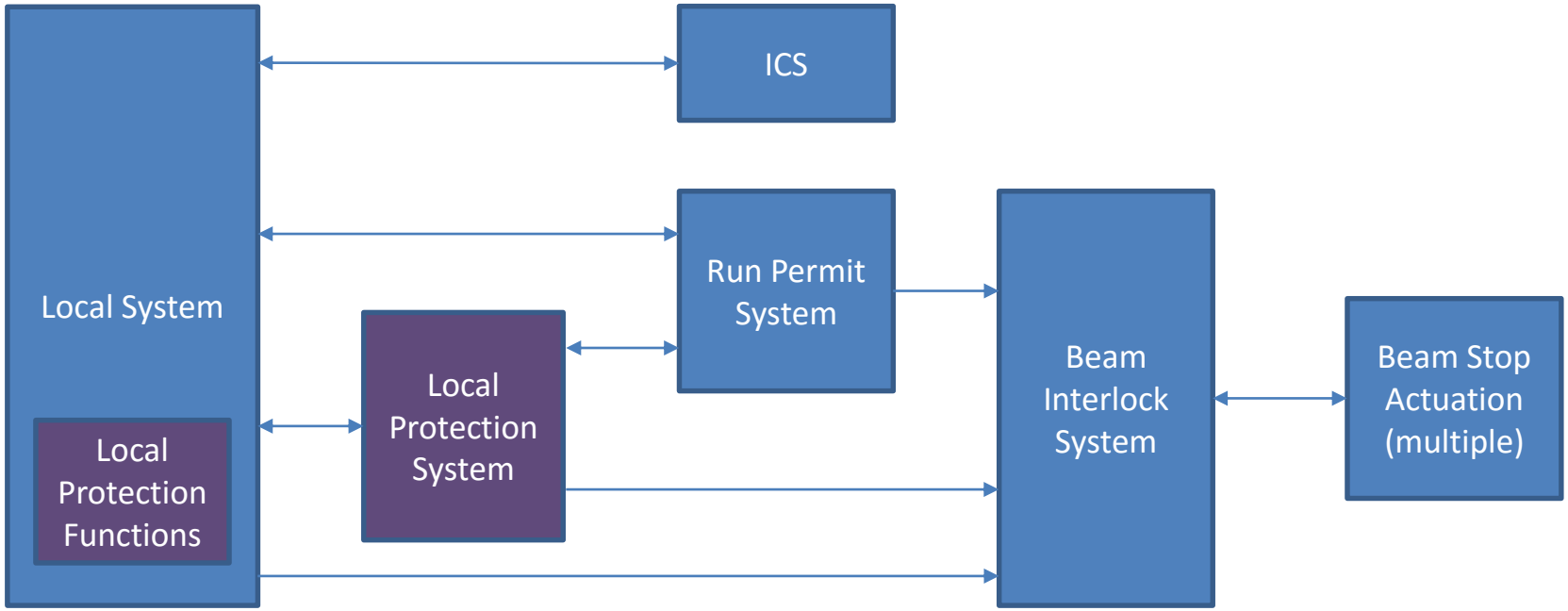
System-of-Systems Concept

- There can't be a single "Machine Protection System" that watches over all others.
- Each system that is part of ESS is required to
  - take over responsibility for itself
    - make sure to detect all local states that might lead to local damage and take necessary local measures.
  - provide information for dependent systems if necessary
    - detect local states that might lead to trouble for other systems and provide adequate information.
  - trigger a beam stop and/or inhibit beam if necessary
    - tell if ready for beam operation; detect local states that might lead to non-nominal beam behavior and trigger Beam Interlock.

Run Permit and Beam Interlock System

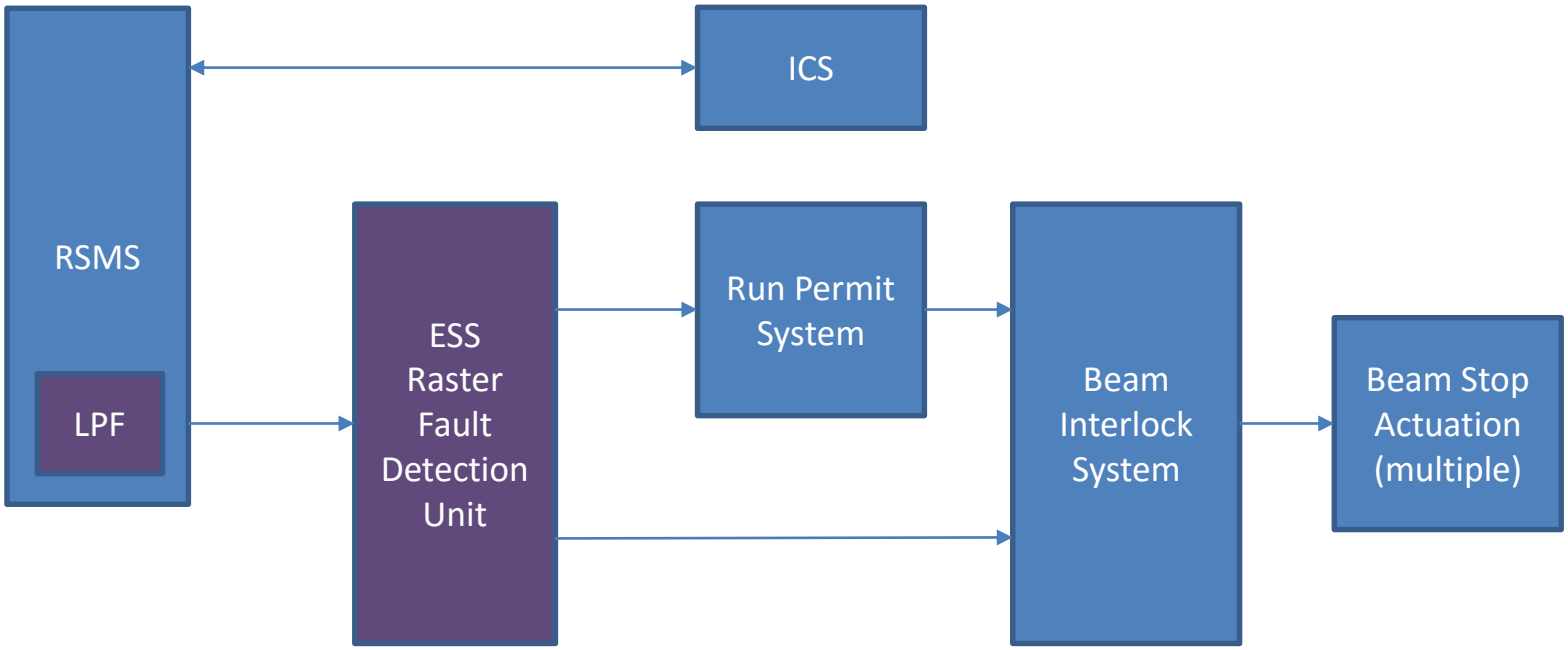
- Purpose
  - Run Permit System:
    - Check if all systems are ready for beam operation.
      - Includes gathering information on both state and configuration of relevant systems.
    - Generate a BEAM-PERMIT signal indicating readiness for beam.
  - Beam Interlock System:
    - Collect all BEAM-PERMIT states from the relevant ESS systems.
    - Evaluate those states depending on the mode of operation.
    - Stop and/or inhibit the beam by controlling actuators acting on beam production and transport.

Architectural Framework



- Local Protection Functions might be implemented
  - directly in the local system,
  - in a dedicated Local Protection System,
  - as a combination of both.

Architectural Integration Concept for the Raster Scanning Magnet System



- Architectural Integration Concept extracted from current Technical Specification (Aarhus and Danfysik)
  - needs to be clarified during Requirements Specification Phase

Protection Functions and IEC 61508

- Generic Functional Requirement
  - Detect any state that might lead to damage or activation.
  - Take all necessary actions for prevention and mitigation.
    - Prevention includes inhibiting beam pulses in the first place.
  - Do this fast enough.
  - Do it with a reliability level that matches the risk the protection function is supposed to protect from.
- Corresponds to IEC 61508 “Safety Function” Concept
  - Use IEC 61508 as guiding standard for Machine Protection related functions and systems.
  - Talk about Protection Integrity rather than Safety Integrity.

We look very much forward to the collaboration with Danfysik and Aarhus University!