Personnel safety systems for PETRA IV

Planed 4'th generation synchrotron light source @ DESY

Michael Dressel
Hamburg, May 29, 2023

Outline

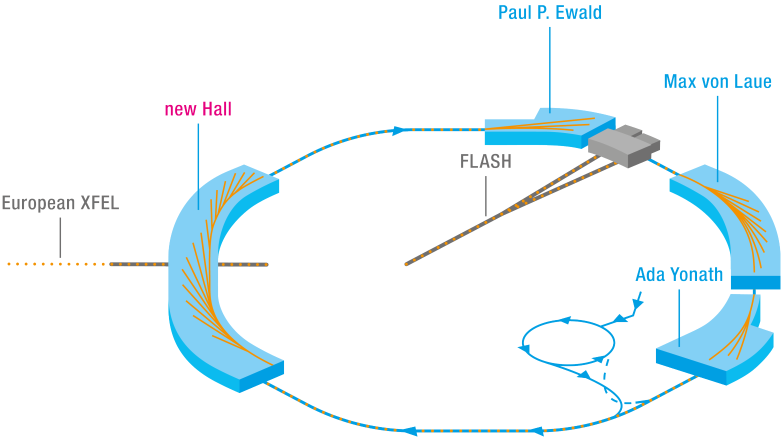
> PETRA IV Overview
> PSSs for PETRA IV
> SF: Safety functions in general
> Legal requirements
> MFS: Management of Functional Safety
> Example

PETRA IV project overview

PETRA IV.
NEW DIMENSIONS

- Upgrade PETRA III to PETRA IV
- Ultra-low-emittance source
- Hard x-rays up to 10-50 keV
- High brightness in excess of 10^{22} phot./mm/mrad/0.1%BW
- 6 GeV electrons, in 2.3 km circumference PETRA tunnel

PETRA IV overview



PETRA IV complex

Number of interlock areas, ZZ- and other doors, PLC systems and PC of the three accelerators

	Linac	Booster	PETRA	total
interlock-areas	2	2	6	10
ZZ-doors	3	4	17	24
other doors	4	16	15	35
PLC systems	1	1	2 (interlock, and ZZ)	4
PC	1	3	5	9
el. cabinet (el. room)	2	3	8	13
el. cabinet (doors)	5	19	24	48

ZZ: Procedure with safety key for temporal access without losing search state

PETRA IV beam lines

Number of beam-lines, hutches, main- plus back-doors in the PETRA 4 experiments halls

	PXN	MvL	PXE	PXW	total
beam-lines	3	11	4	13 (+5)	36
optics, hutches	3	15	4	13 (+5)	40
exp. hutches	6	24	9	23	62
(main+back) doors ∼	11	60	13	50	134
PLC system and PC	3	11	4	18	36
el. cabinet (el. room)	1	2	1	2	6
el. cabinet (beam-line)	3	11	4	18	36
el. cabinet (door)	9	39	13	41	102

Usual safety function structure

Sensor - Logic - Actuator

Example for requirements on PFH$_d$ of a sub system and the overall SF, a.o.:

- sub-system and overall architecture
- DC and test interval
- CCF
- failure rate λ_d of element
- useful lifetime (commonly: 20 years)
- SIL / PL
- …

PFH$_d$: Probability of dangerous failure per hour
DC: diagnostic coverage
CCF: common course failure
SIL / PL: safety integrity level, PL: performance level

Some typical safety sensors

- door contacts
- key locks or switches (for door latching, ZZ, beam permission)
- beam shutter position switches
- magnets currents or position
- emergency-off switches
- light barrier
- …

Logic

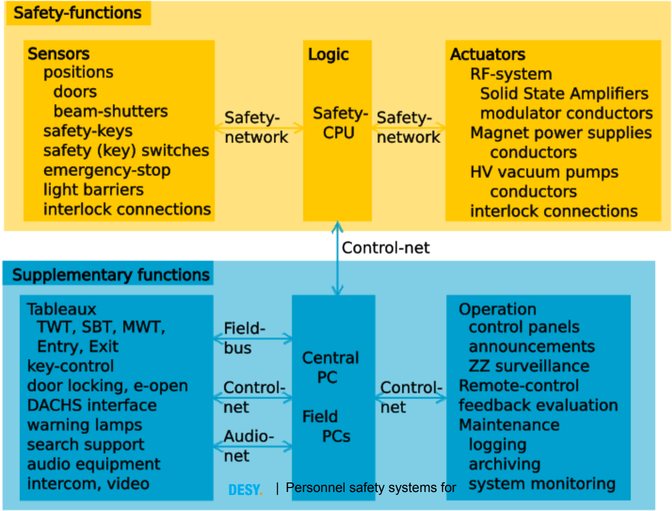
- Safety PLC for beam permission
- Safety-relays for emergency-off
- Safety diagnostics
- Safety network

Some typical actuators

- contactors (circuit breaker) of rf-modulators
- contactors of hv power supplies
- safety signals to solid state amplifiers
- switches of getter pumps
- …

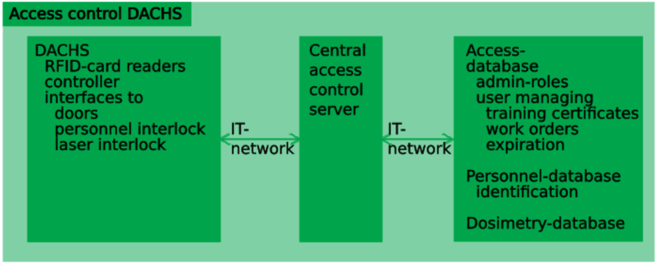
PETRA IV functions

Components within safety functions and related supplementary functions



PETRA IV access control, DACHS

For authentication



Legal requirements

- Machinery Directive 2006/42/EC
- German regulations for occupational safety (i.e. TRBS 1115)
- Both refer to the same standards: ISO 12100, ISO 13849, EN 62061 (TRBS1115 also to IEC 61511)
- Top-Down Procedure
- General risk assessment and MFS if safety functions required
- Management of Functional Safety:
  - organisational responsibilities
  - qualification and competence
  - specification
  - verification
  - examination
  - evaluation

Risk assessment in General

> Risk assessment

In case measures are required for risk reduction:

> Safety concept / independence
> Appropriateness / Effectiveness
> Reasoning / Evaluation
> Traceability / Documentation

Basic MFS goals

MFS must make sure that

- methods,
- work flows (processes) as well as,
- the safety systems

reach the following goals permanently:

- appropriateness
- effectiveness
- traceability
- maintainability

Top-Down Procedure

Systematic identification of all hazards of the overall system.

- Essential hazards of the overall system are evident from start, e.g. accelerators are to deliver electron beams and undulators are to deliver photon beams with high brightness. This already puts demands on beam shutters.
- Additional hazards occur by combining subsystems. E.g. RF-system produces additional ionizing radiation when combined with cavities.
- Controlling these hazards puts requirements to subsystems that can not be realized within the subsystems alone. E.g. SIL-requirement on shutting off the modulators.
- Hazards of the overall system and hazards occurring by combining subsystems generate additional requirements on the overall system and the subsystems in turn. These should be added as soon as possible to the requirements of the subsystems.

Functional Safety Realization

Two classes of requirements

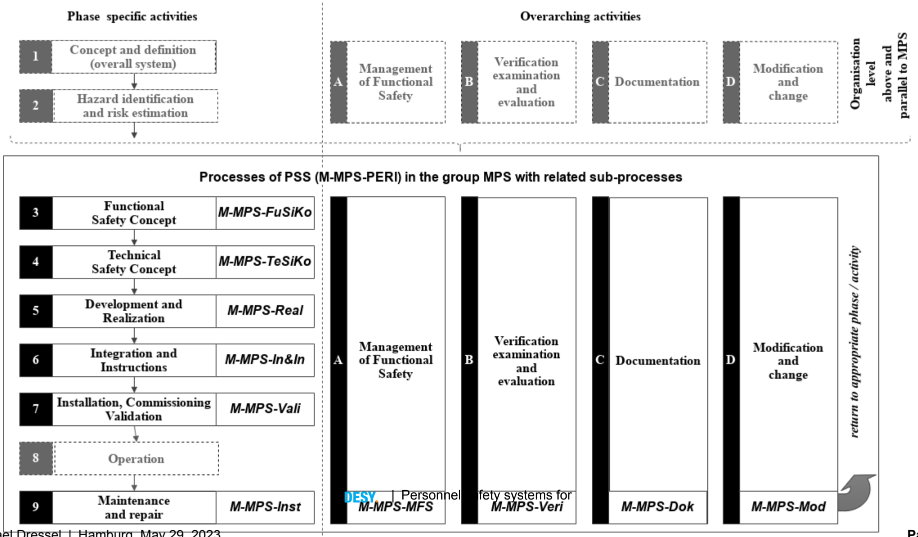
In order to meet the required SIL_r or PL_r:
Functional Safety demands both:

Systematic Safety Integrity	Hardware Safety Integrity
prevent systematic failures	cope / master random failures
robust process	robust design

Higher safety levels put increasing demands on:

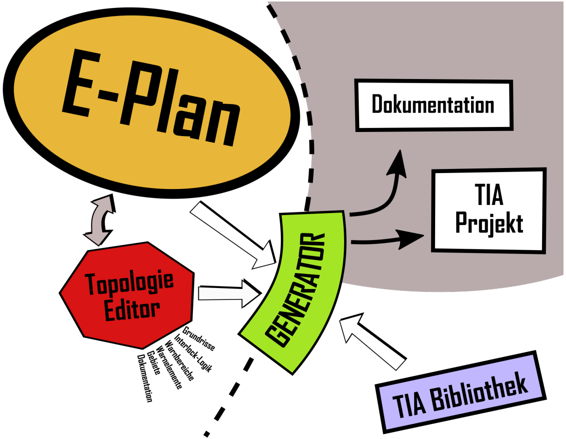
management	reliability
planing	diagnoses
documentation	architecture
quality	failure modes
V&V	redundancy
independence	

MFS process within group MPS



Generator

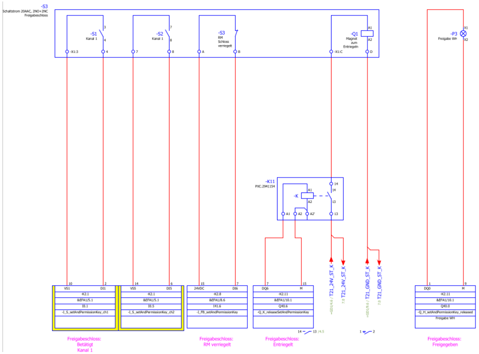
Code generation based on self verified/qualified modules



Electrical construction

Electrical cabinets, wiring, cabling

- Create and use modules in electrical construction
- Export construction (aml data)
- Use aml in the code generator



SOFTEMA

Matrix method tool from occupational insurance. Supports systematic documentation from specification to validation.

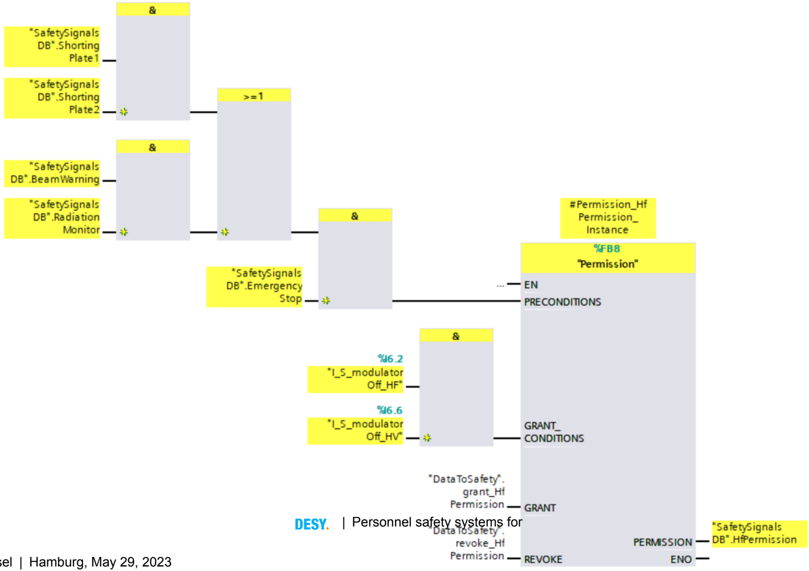
	C	D	E	F	G	H	I	J	K	
1										
2										
3										
4										
5	_Symbol	_Adresse	_Datentyp	_Modul	_Aktiv_in_C+E	_Aktiv	_Sperre	_SW-Verif.	_IO-Test	_DIAC
6	relevant	nicht relevant (_Nr. übertragen)	relevant			relevant	relevant	relevant	nicht relevant (immer OK)	Releva (nicht
7										
8	REVOKE	I1	Bool		-	Aktiv	x	OK	OK	OK
9	PRECONDITIONS	I2	Bool		Aktiv	Aktiv	x	OK	OK	OK
10	GRANT	I3	Bool		-	Aktiv	x	OK	OK	OK
11	GRANT_CONDITIONS	I4	Bool		-	Aktiv	x	OK	OK	OK
12										
13	PERMISSION	O1	Bool		Aktiv	Aktiv	x	OK	OK	OK
14										
15							x	OK	OK	OK
16							Datum	09.02.2023	09.02.2023	09.02.
17							Name	Alessandro Kropmanns / Stefan May	Alessandro Kropmanns / Stefan May	Alessa Stefar
18							Signatur	576DBFD8	576DBFD8	576DE
19										
20							Datum	13.02.2023	13.02.2023	13.02.
21							Prüfen1	Andreas Cords	Andreas Cords	Andre
22										
23							Datum			
24							Prüfen2			

A3 Maßnahmen | A4 Anforderungen | B3 Modularchitektur | B4 Matrix C+E | B4 Matrix kompakt | C1 Codereview | D1 Validierung | Personen | Änderungen | Dokumente

Generator input snippet

```xml
<permission id="HfPermission">
  <preconditions>
    <or>
      <and>
        <internal>ShortingPlate1</internal>
        <internal>ShortingPlate2</internal>
      </and>
      <and>
        <internal>BeamWarning</internal>
        <internal>RadiationMonitor</internal>
      </and>
    </or>
    <internal>EmergencyStop</internal>
  </preconditions>
  <grantconditions>
    <input>I_S_modulatorOff_HF</input>
    <input>I_S_modulatorOff_HV</input>
  </grantconditions>
</permission>
```

Generated code networks



Summary

- The PSS for PETRA IV aims to be safe and compliant with the safety standards.
- Processes are developed and implemented to manage functional safety.
- Software tools are used to support the documentation and verification from specification to validation.
- Modularization and automated project generation is developed in order to deal with the large variability of accelerators and experiments safety systems.

Thank You