EUROPEAN
SPALLATION
SOURCE

Hardware integrity assessment of the Fast Beam Interlock System (FBIS) at ESS

PRESENTED BY DR. JOANNA WENG (ZHAW) AND JOHANNES GUSTAFSSON (ESS)

CO-AUTHORS: SILVAN FLURI, PATRICK PROBST,
MARTIN REJZEK, CHRISTIAN SOMMER (ZHAW)

2022-10-20

Agenda

1 Introduction ESS and ZHAW

2 Machine Protection at ESS

3 FBIS Reliability Analysis

4 ESS integration of FBIS reliability analysis

5 Benefits of detailed reliability studies

1

Introduction ESS and ZHAW

European Spallation Source

ESS aims to be brightest Neutron Source worldwide

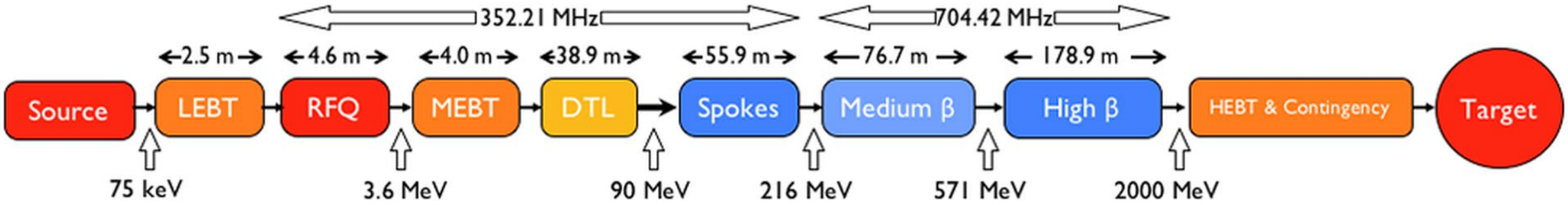
Commissioning of first 50m of the proton accelerator started in 2021

Beam on Target is planned for end of 2024

User programme starts in 2025

Decommissioning in 2065

ESS Proton Accelerator



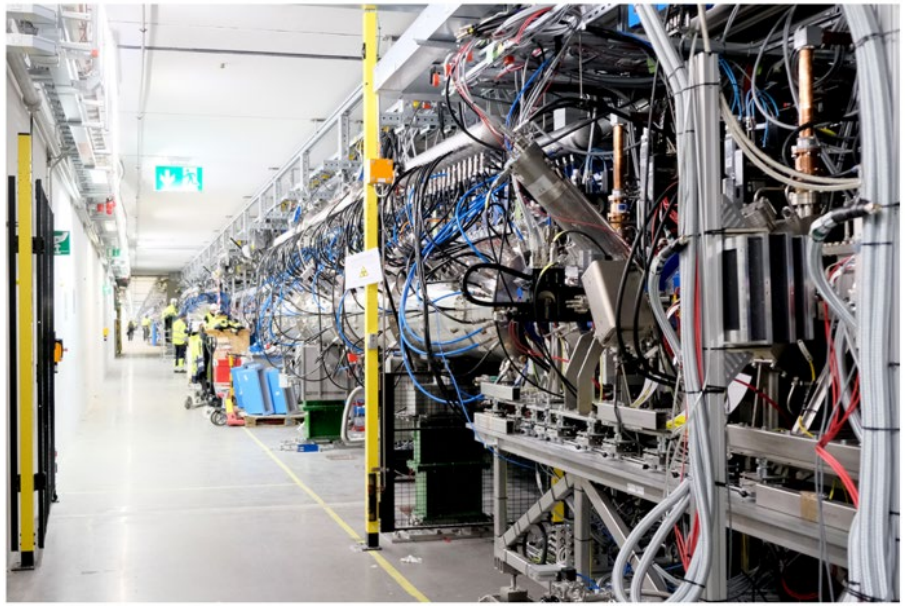
Proton beam energy: 2 GeV

Pulse length: 2.86 ms

Pulse repetition rate: 14 Hz

Average beam power: 5 MW

Average beam current: 62.5 mA



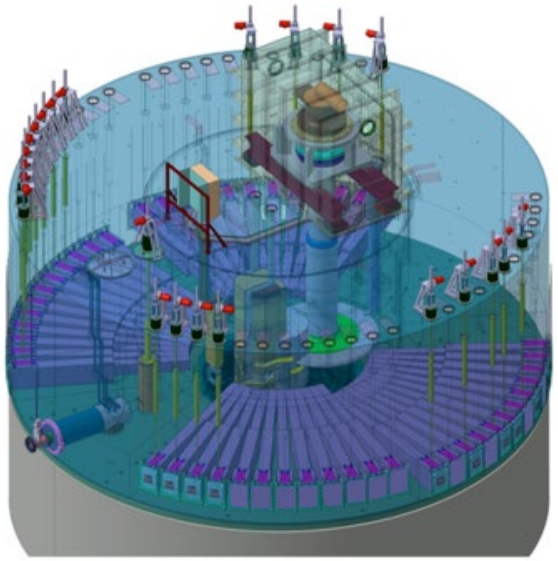
ESS Target Station

Rotating Tungsten target

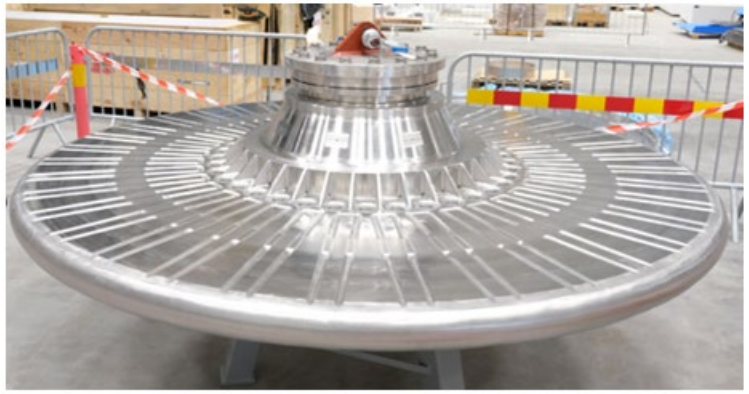
36 sectors with cooling channels (Helium)

Synchronized to 14 Hz proton beam pulses

Target Monolith
r=6m, h=10m



Target Wheel

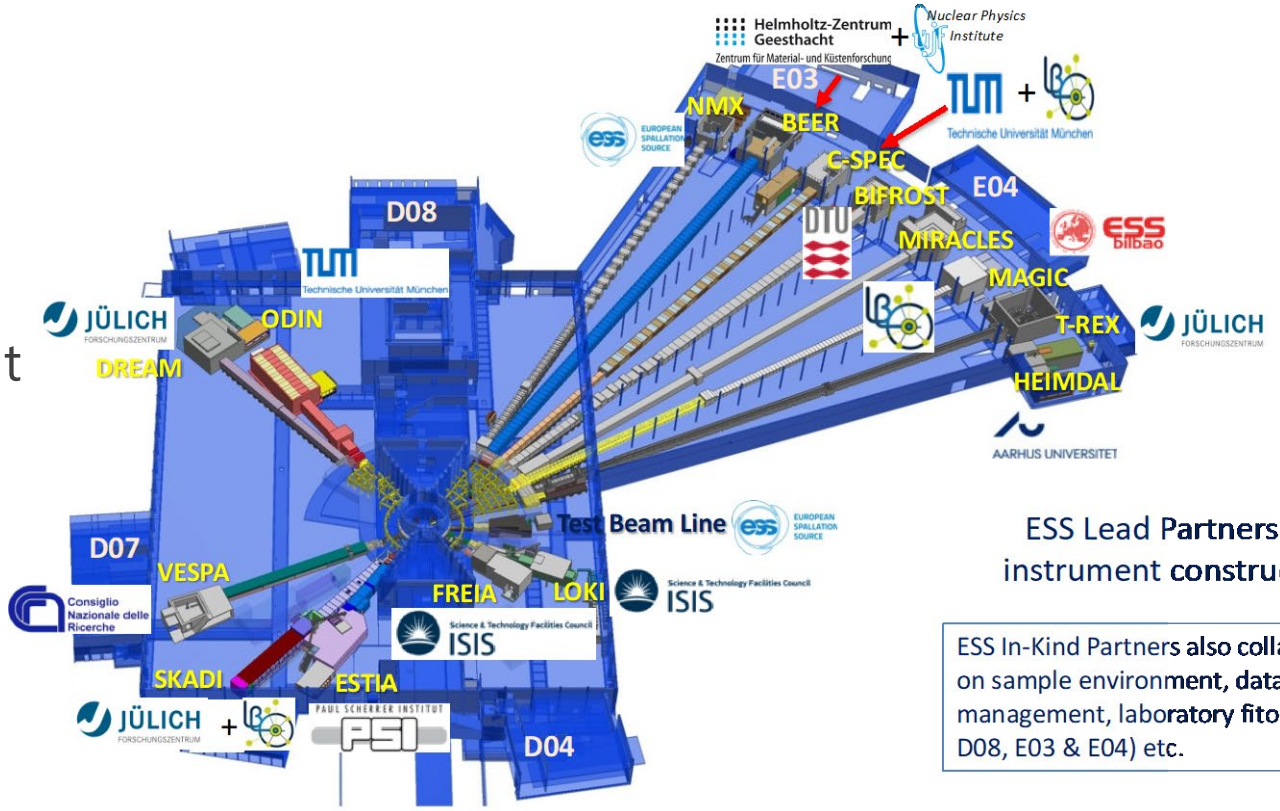


Instrument Suite

15 Instruments in Design and Construction

- 15 instruments in detailed design
- Most instruments are a collaboration between scientists from the member states

Timeline for first science to be carried out in 2027 on the first opened instruments

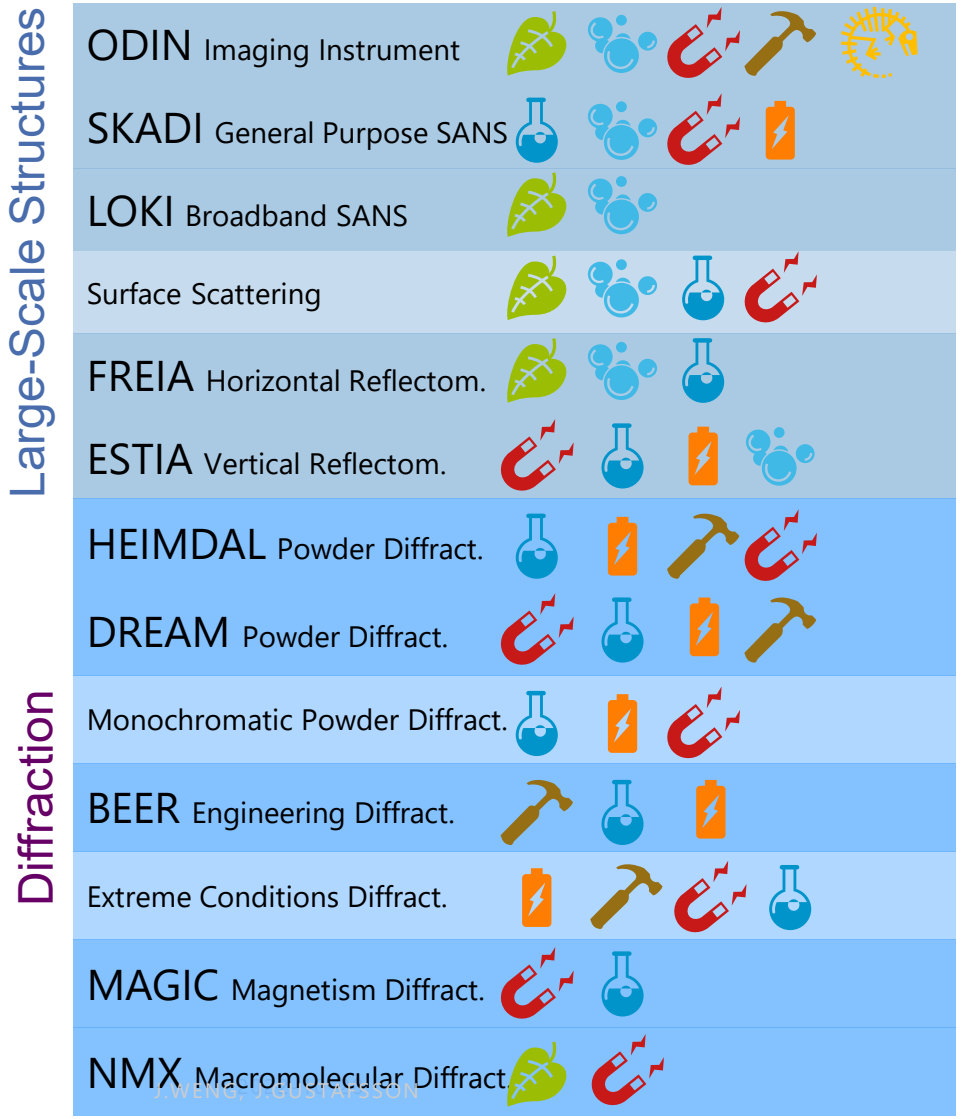


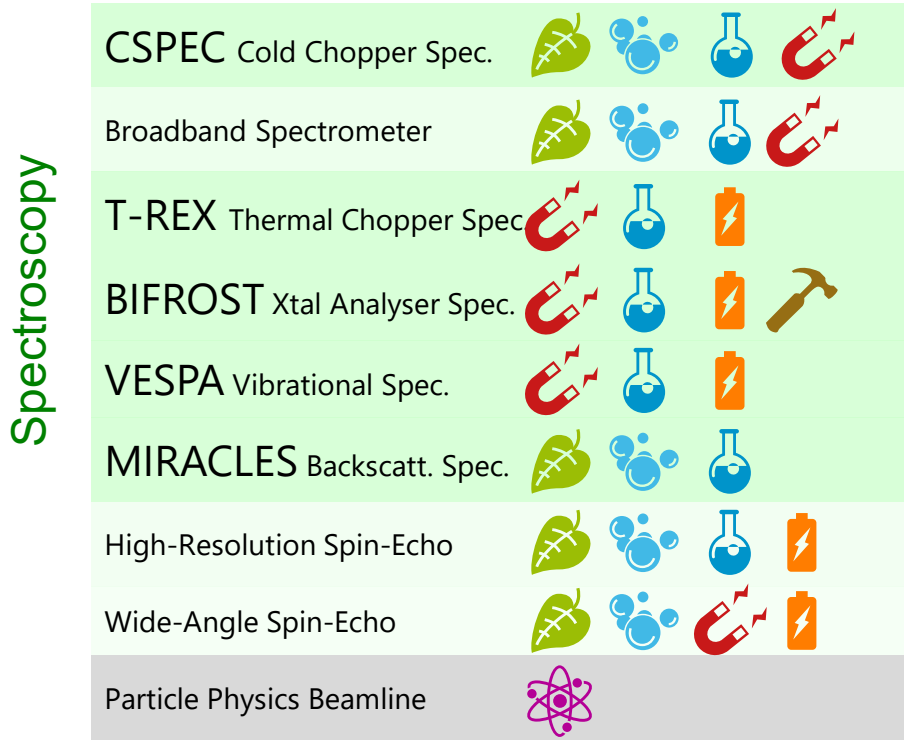
ESS Lead Partners for instrument construction

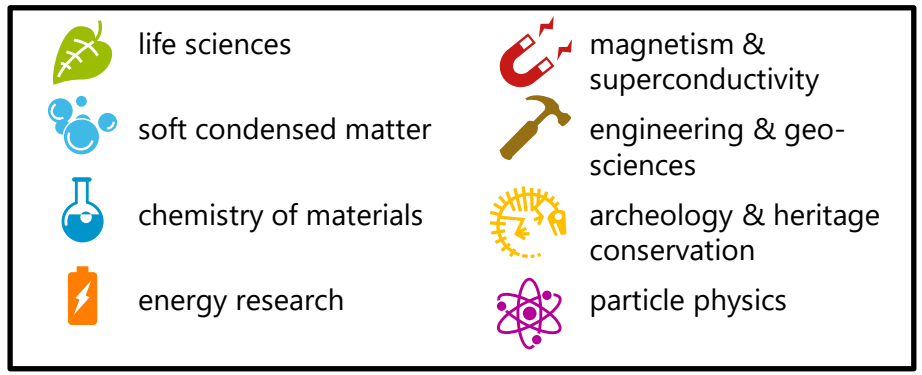
ESS In-Kind Partners also collaborate on sample environment, data management, laboratory fitout (D04, D08, E03 & E04) etc.

Instrument Suite

15 Instruments in Design and Construction



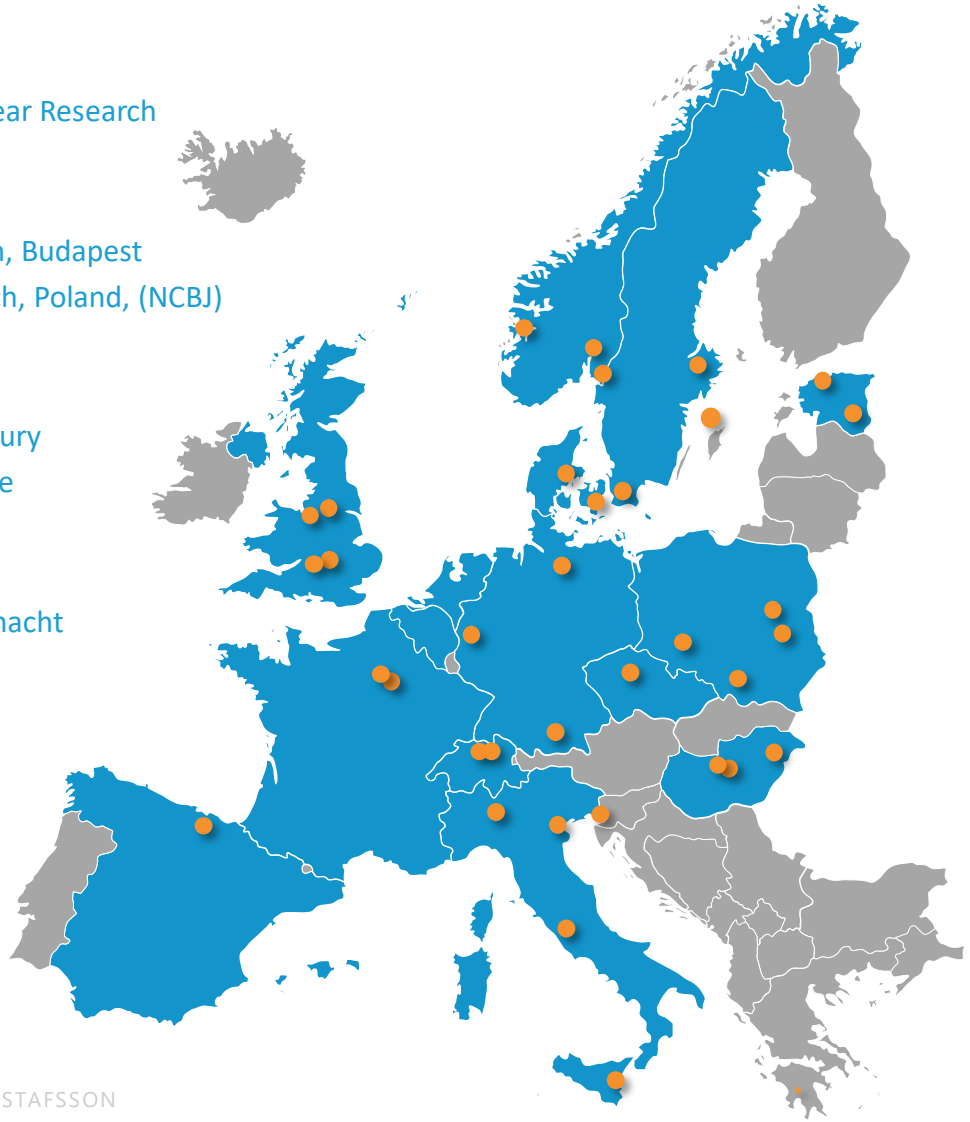




ESS – a Pan-European Project

ESS has 13 member states and more than 40 EU partner institutes

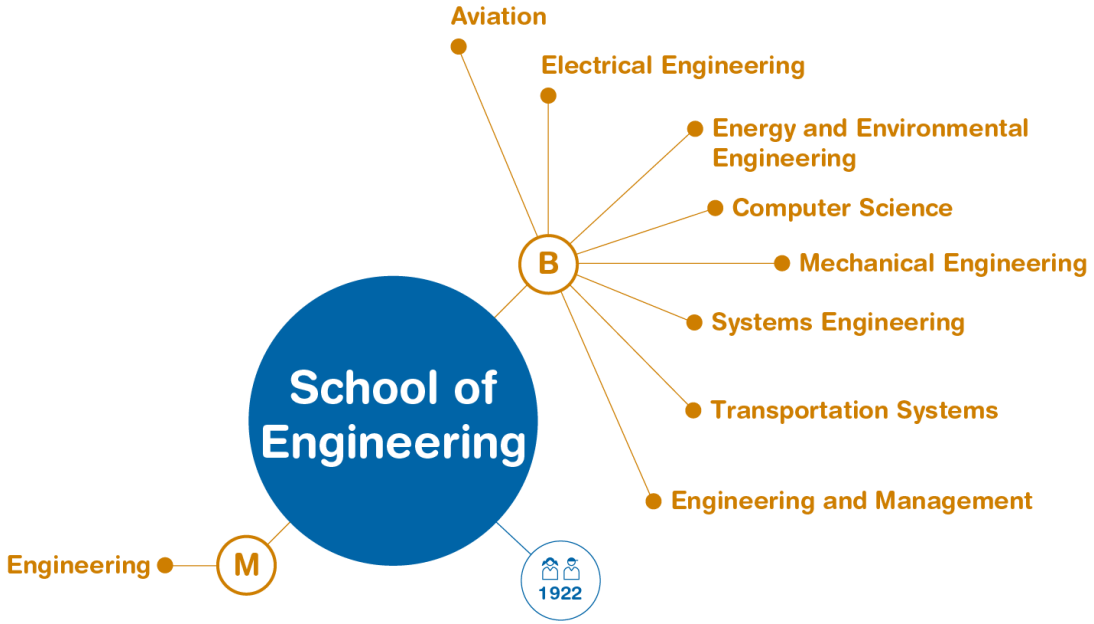
Aarhus University
Atomki - Institute for Nuclear Research
Bergen University
CEA Saclay, Paris
Centre for Energy Research, Budapest
Centre for Nuclear Research, Poland, (NCBJ)
CNR, Rome
CNRS Orsay, Paris
Cockcroft Institute, Daresbury
Elettra – Sincrotrone Trieste
ESS Bilbao
Forschungszentrum Jülich
Helmholtz-Zentrum Geesthacht
Huddersfield University
IFJ PAN, Krakow
INFN, Catania
INFN, Legnaro
INFN, Milan
Institute for Energy Research (IFE)

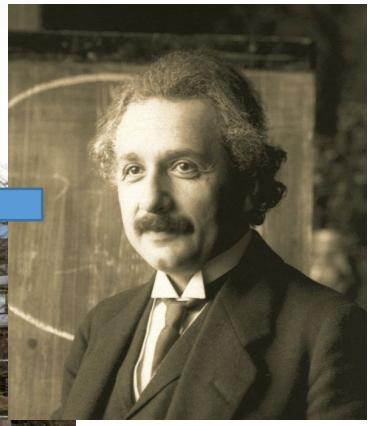


ISIS - Rutherford-Appleton Laboratory, Oxford
Laboratoire Léon Brilouin (LLB)
Lund University
Nuclear Physics Institute of the ASCR
Oslo University
Paul Scherrer Institute (PSI)
Polish Electronic Group (PEG)
Roskilde University
Tallinn Technical University
Technical University of Denmark (DTU)
Technical University Munich (TUM)
Science and Technology Facilities Council
University of Copenhagen (KU)
University of Tartu
Uppsala University
Wigner Research Centre for Physics
Wroclaw University of Technology
Warsaw University of Technology
Zurich University of Applied Sciences (ZHAW)

ZHAW introduction

- **Zurich University for Applied Sciences (ZHAW)**
  School of Engineering
  Switzerland



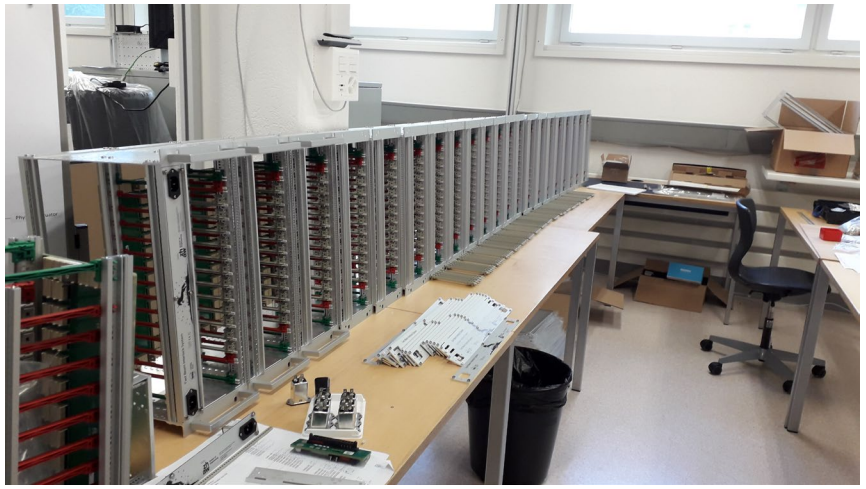


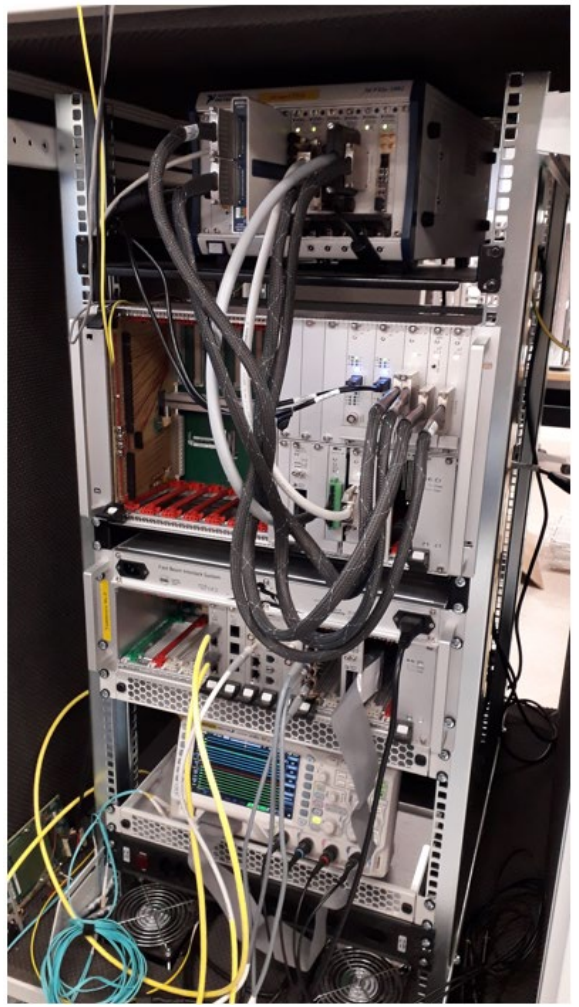
1901

- Applied R&D projects with industry partners

Safety Critical Systems Lab @ZHAW

- **Successful collaboration with ESS since 2016**
- Build Fast Beam Interlock System (FBIS) in our lab
- Developed verification for FBIS
  (Hardware in the Loop simulation)
- Performed FBIS hardware integrity assessment
- Support ESS Machine Protection (MP)
  integrity assessment
- Functional safety assessment of ESS
  Personal Safety System (PSS)





2

Machine Protection at ESS

Machine Protection at ESS

Risk management

To define machine protection requirements, the machine protection related risks at ESS are evaluated according to a risk management procedure that follows international standards.

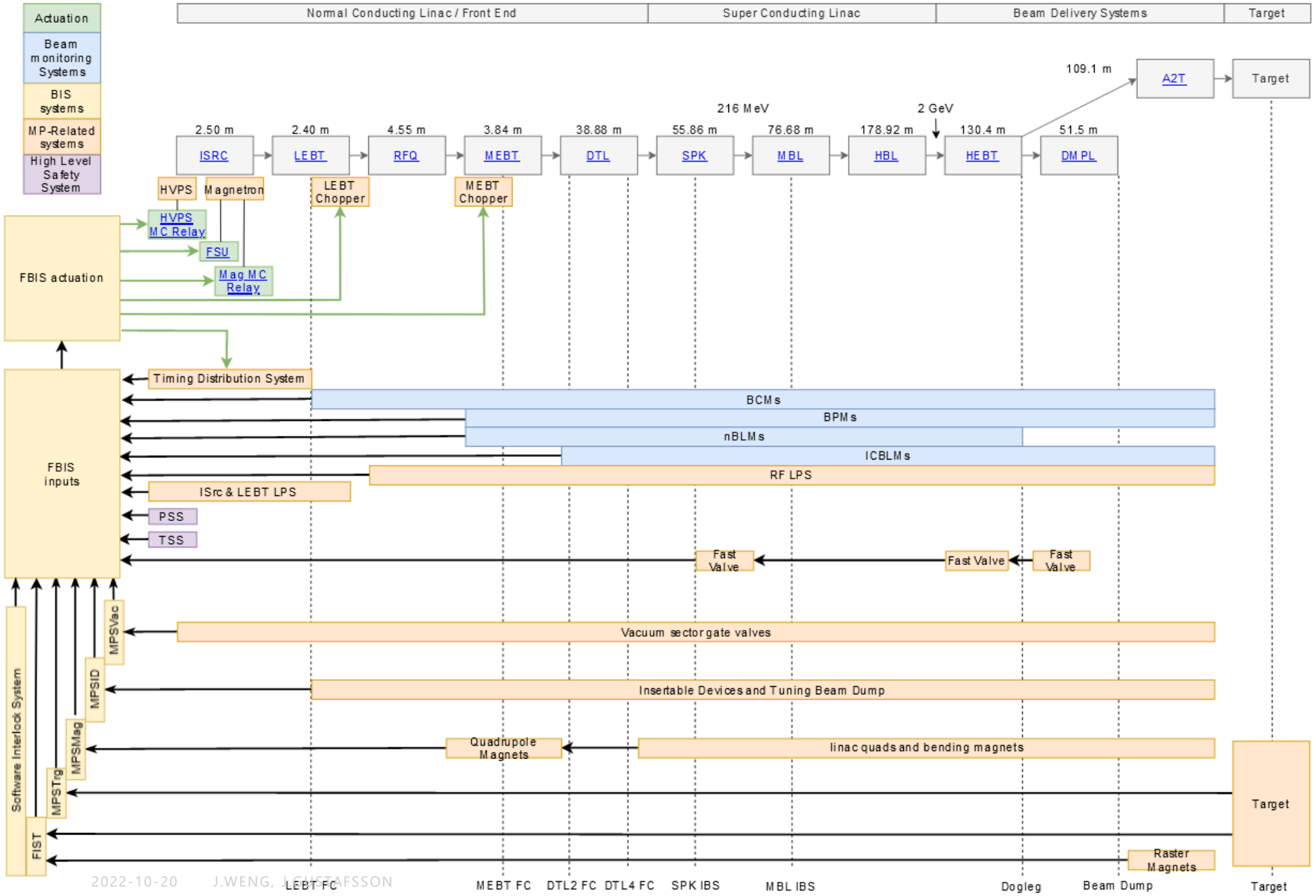
To comply with the requirements each defined protection function is evaluated according to the functional safety standard IEC 61508.

Machine Protection at ESS

Machine Protection Risk Analysis

- Functional description
- Reaction time requirements
- Reliability requirements
- Preliminary architecture

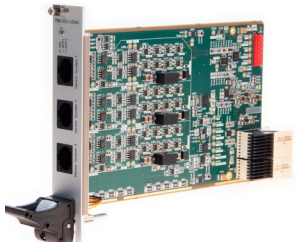
Layout and scope of Machine Protection Systems of Systems

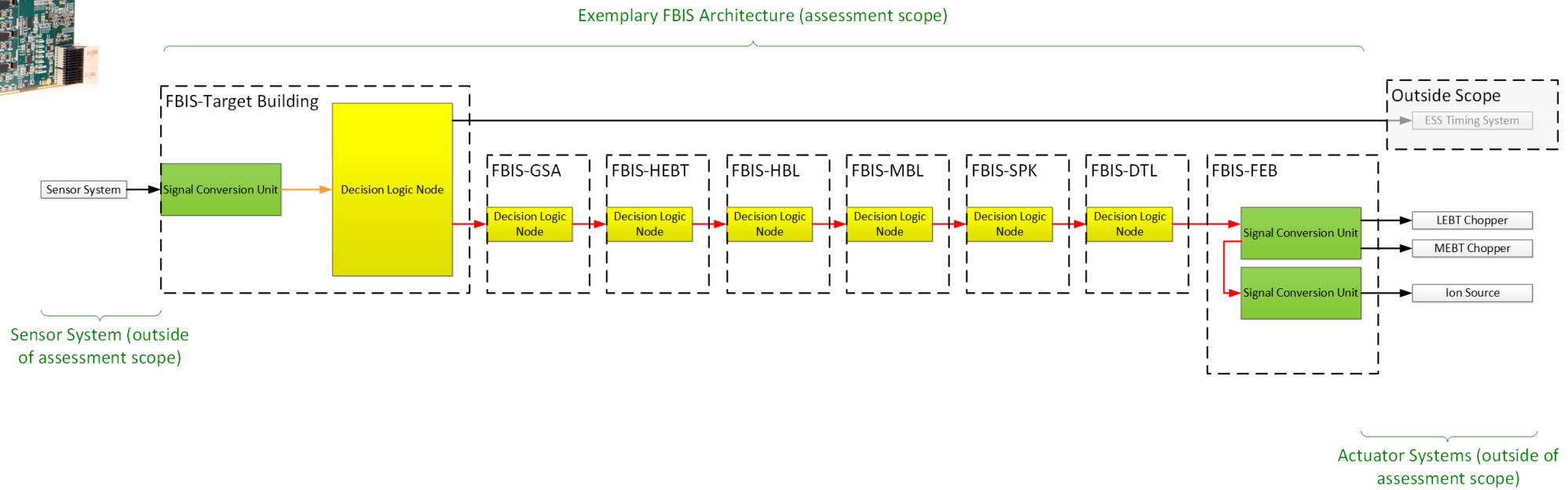


3

FBIS Reliability Analysis

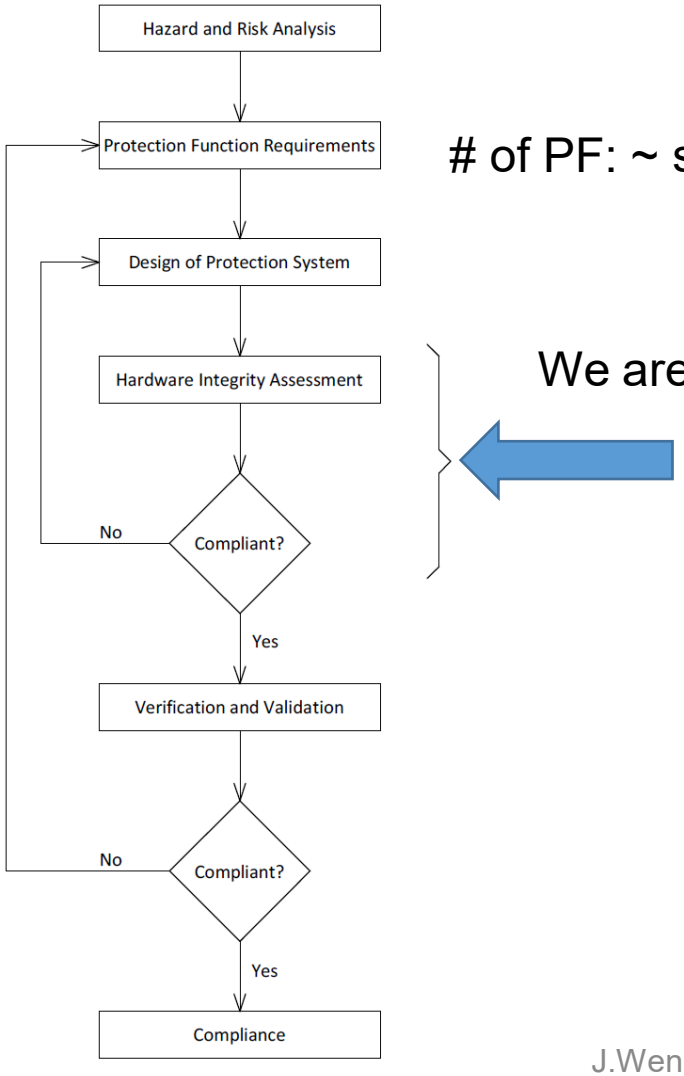
FBIS Architecture: Overview





- Left SCU handles interfaces to Sensor Systems. Signal is pre-processed, aggregated, and communicated to the DLN.
- DLN performs the protection logic
- Right SCUs handle the interfaces to Actuation Systems.

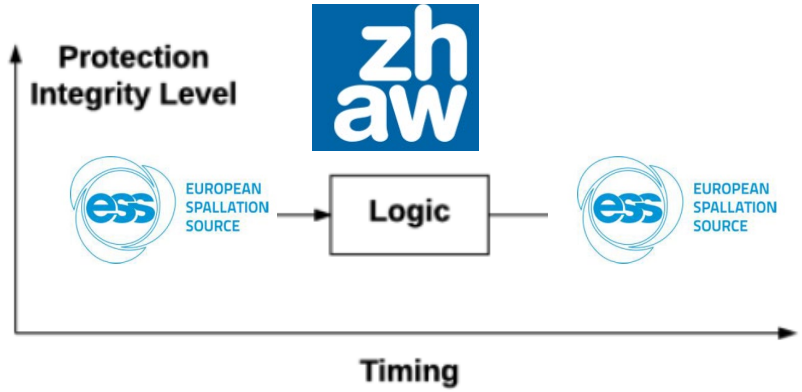
Analysis Methodology



# of PF: ~ several hundreds.

We are here

Simplified PF Specification: 5 elements



PIL Requirements

- Requirement on integrity against random hardware failures for machine protection are guided by the IEC 61508 standard
- Highest PIL requirement @ESS: **PIL 2**

PIL	SIL (IEC 61508)	Required PFH	Required PFD
PIL0	N/A	$<= 1 * 10^{-4}$	<= 1
PIL1	SIL1	$<= 1 * 10^{-5}$	$<= 1 * 10^{-1}$
PIL2	SIL2	$<= 1 * 10^{-6}$	$<= 1 * 10^{-2}$
PIL3	SIL3	$<= 1 * 10^{-7}$	$<= 1 * 10^{-3}$
N/A	SIL4	$<= 1 * 10^{-8}$	$<= 1 * 10^{-4}$

PFH:
probability of failure per hour
PFD:
probability of failure per demand

- FBIS has a hardware fault tolerance (HFT) of 1, -> safe failure fraction (SFF) of ≥60% is required.

Safe Failure Fraction
(usually determined by FMEDA):

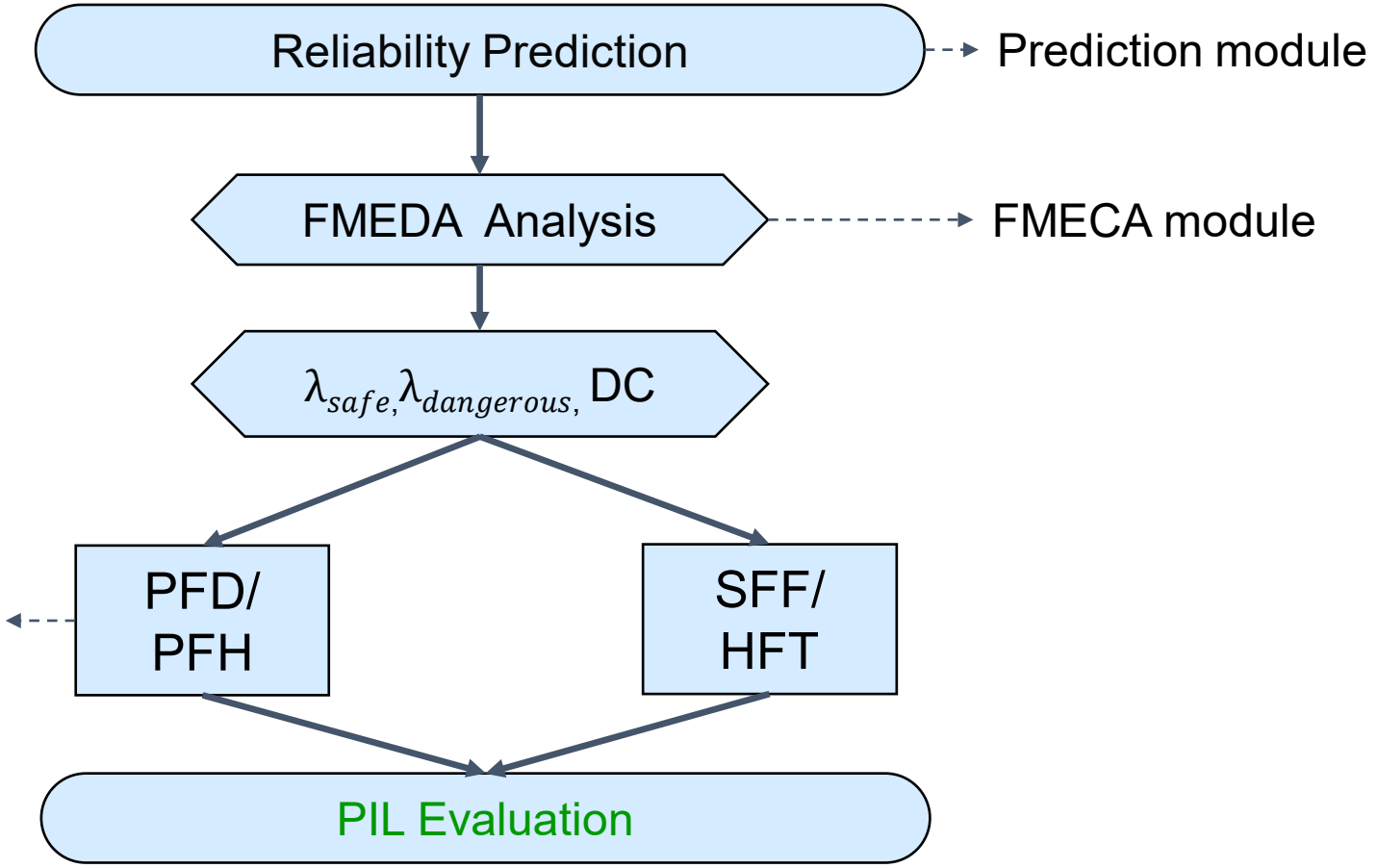
$$SFF = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}}$$

Table 3 – Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	Not Allowed	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

PIL Verification Methodology

Isograph software



Reliability Block Diagram (RBD) module

PF Tag	Required PIL	Required PFH	Achieved PFH	Max allowable PIL (Architectural Constraints)	Result
BLE-MAG-PF-1.1	PIL 1	<= $1 * 10^{-5}$	$4{,}8 * 10^{-7}$	PIL 1	Passed

Reliability Prediction and FMEDA: Data Sources

Zürcher Hochschule für Angewandte Wissenschaften

Reliability

Priority	Failure rate data source
1	Manufacturer datasheet / analysis report
2	SN 29500 [2]

$$\lambda = \sum_{i}^{n} (\lambda)_i = \sum_{i}^{n} (\lambda_{ref} * \pi_U * \pi_I * \pi_T * \pi_E * \pi_S * \pi_{ES} * \pi_Q * \pi_{PS})_i$$

- λ Failure rate at operating conditions
- λ_{ref} Reference failure rate
- π_U Voltage stress level dependence factor
- π_I Current stress level dependence factor
- π_T Temperature stress level dependence factor
- π_E Environmental stress level dependence factor
- π_S Switching rate stress level dependence factor
- π_{ES} Electrical stress level dependence factor
- π_Q Quality dependence factor
- π_{PS} Power stress level dependence factor

FMEDA

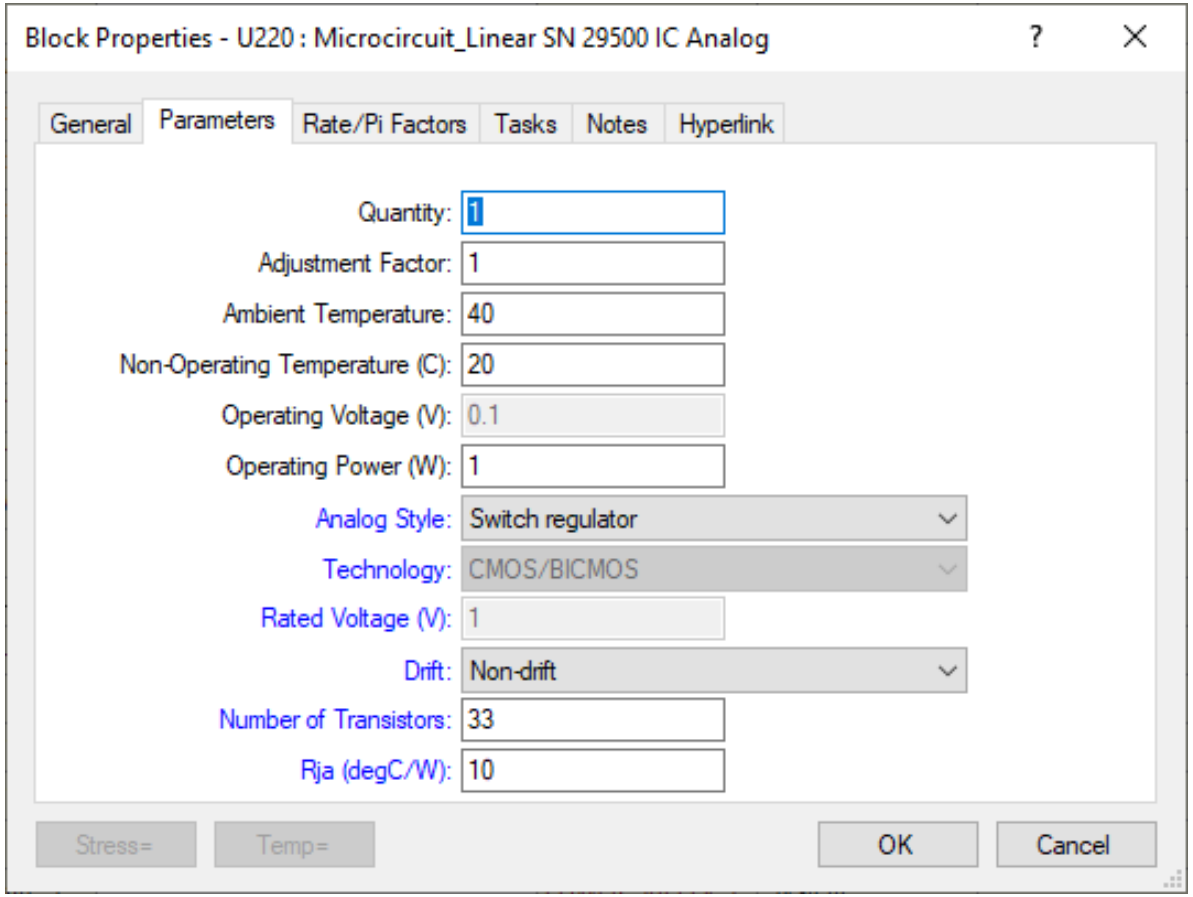
Priority	Failure modes data source
1	Manufacturer data
2	EN 61709:2017 [3]
3	FMD-2016 [4]
4	IEC 62061:2005 [5]

FMECA failure modes ▾ General FMECA ▾

ID	Description	Effects defined	Contributors defined	Dangerous failure %	Detectable	Effects (immediate)
CR632.1	Short	No	N/A	0	Yes	
CR632.2	Open	No	N/A	0	Yes	
CR632.3	Drift	No	N/A	0	Yes	

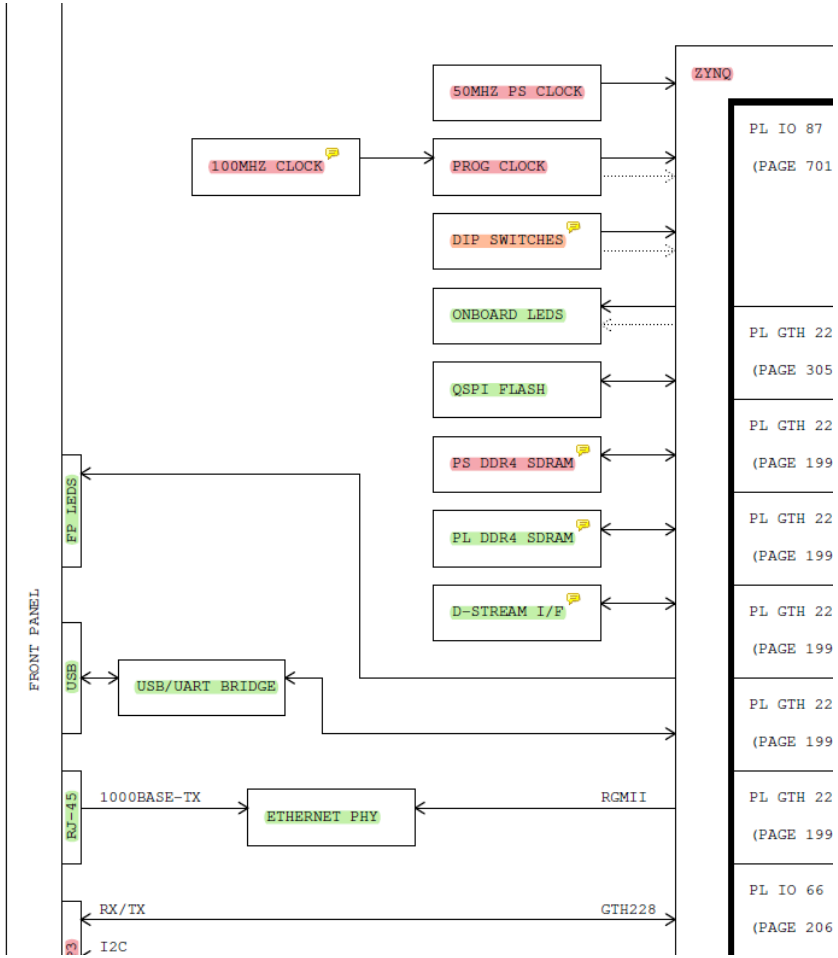
Reliability Prediction: Parameters

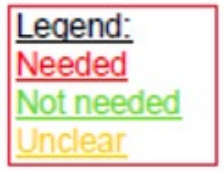
Example: Adjustment of parameters/stress factors in Isograph prediction module

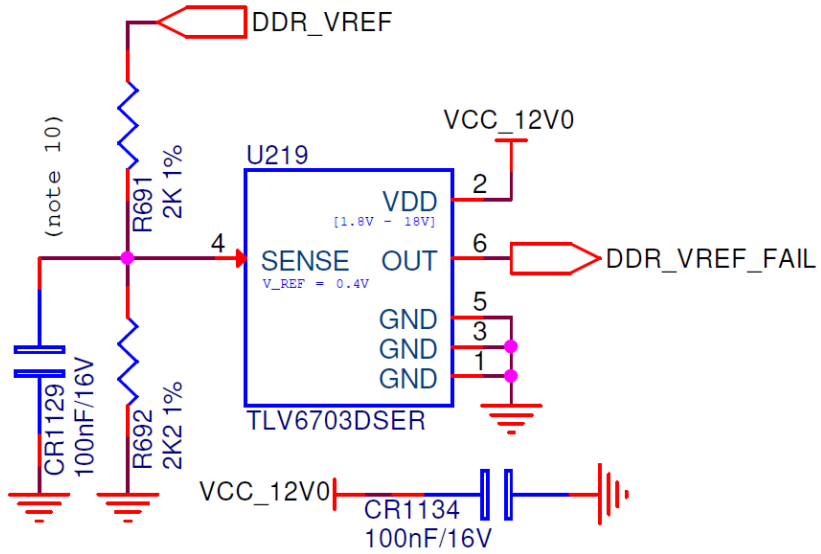


FMEDA

- Exclude all no-part and no-effect failures in protection function
- Determine safe failures from electrical drawings/schematics and credit detection methods





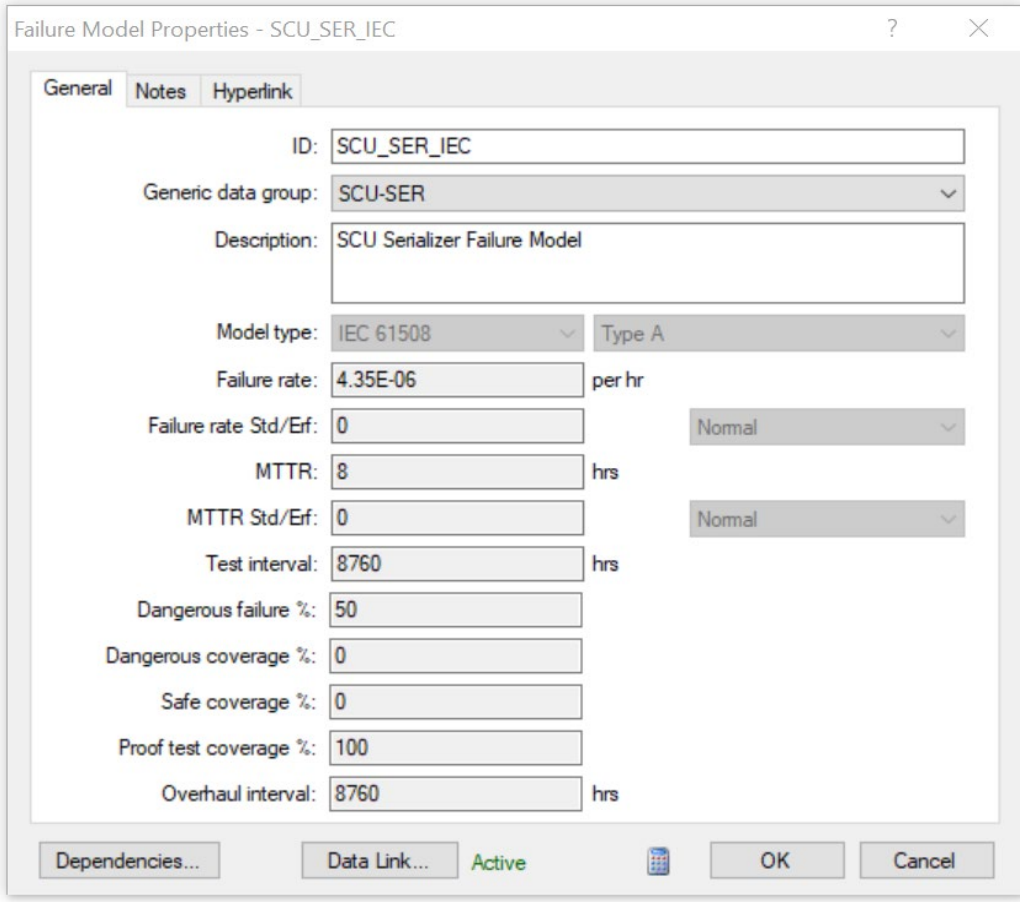


Reliability Block Diagramm (RBD)

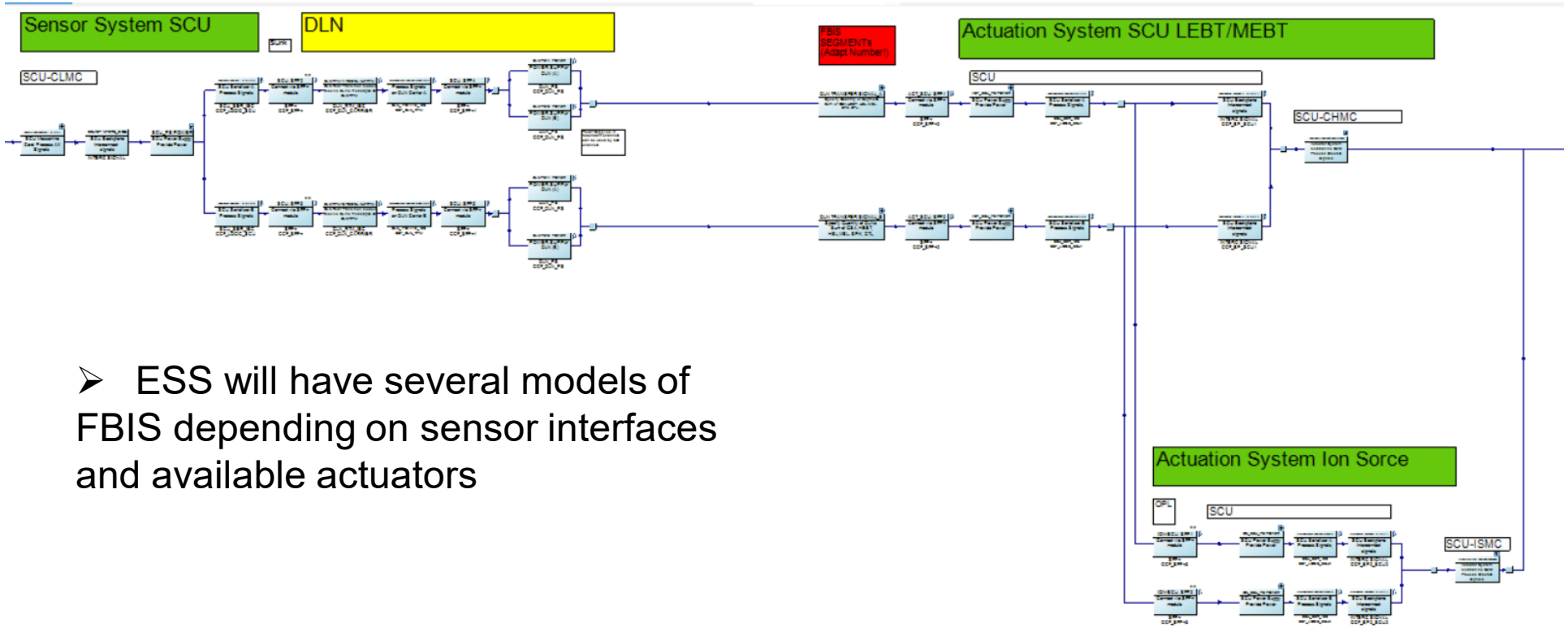
- We use the IEC 61508 Failure Model in Isograph
- When no FMEDA was performed,
  a division of failures into 50% safe and 50% dangerous is assumed
- A CCF Model with a β=factor of 5% is applied
- Diagnostic coverage determined from FMEDA:

$$DC\ (Dangerous\ Coverage) = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}}$$

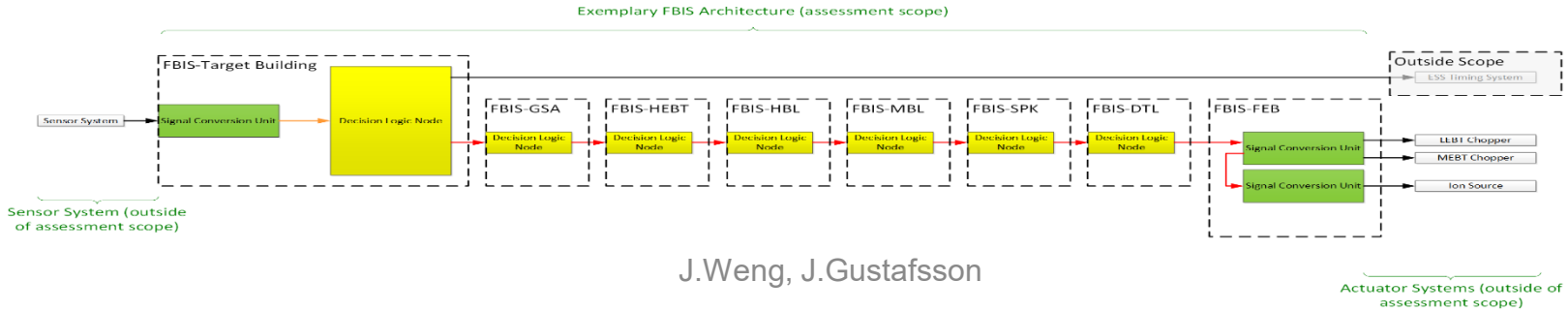
- Calculation of PFH/PFD with only dangerous undetectable failures λ_{DU}



FBIS RBD example



- ESS will have several models of FBIS depending on sensor interfaces and available actuators

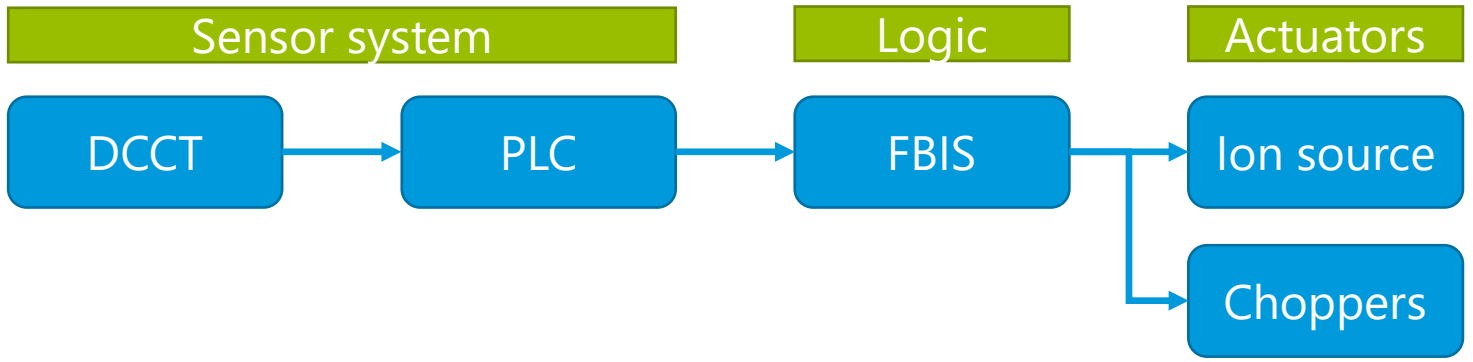


4

ESS integration of FBIS reliability analysis

Machine protection reliability analysis

Example of protection function “BLE-MAG-PF-1.1” Current monitoring of bending magnet power converter.

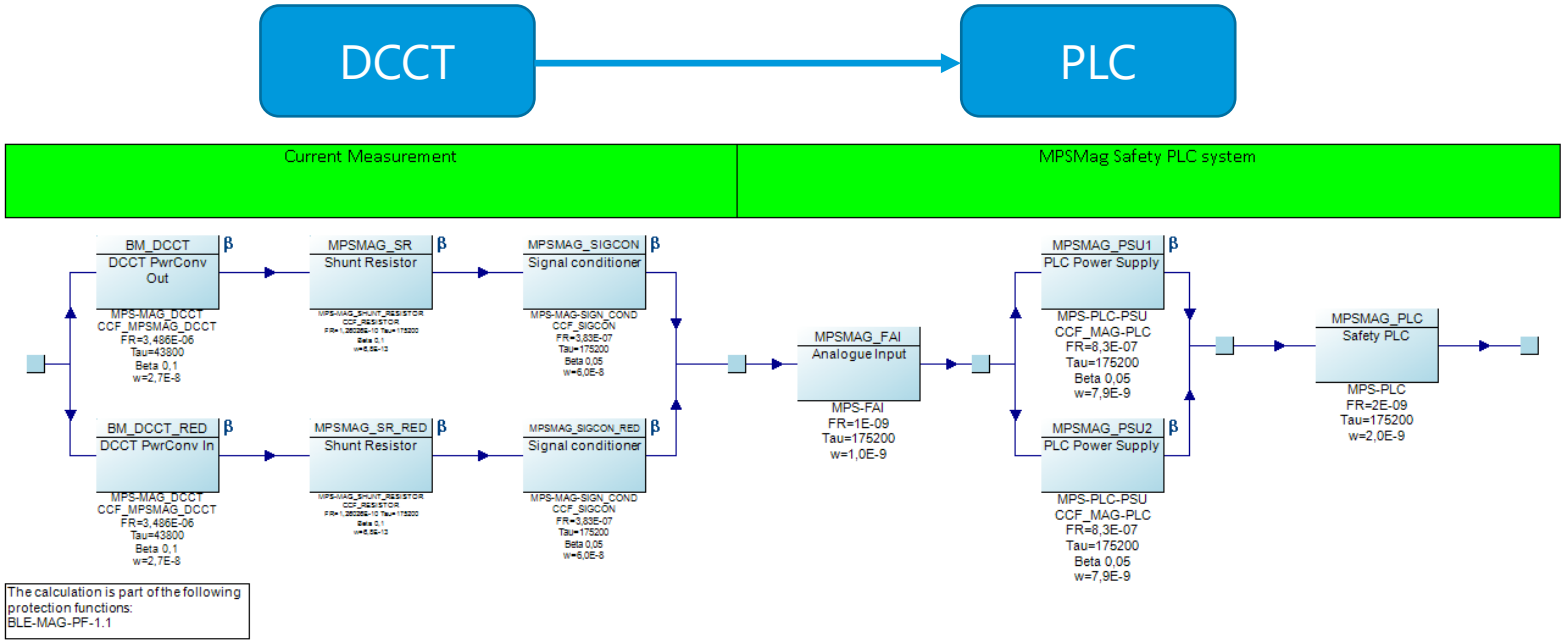


Machine protection reliability analysis

Analysis of sensor system

The machine protection PLC system uses SIL rated components with pre-calculated values from the manufacturer.

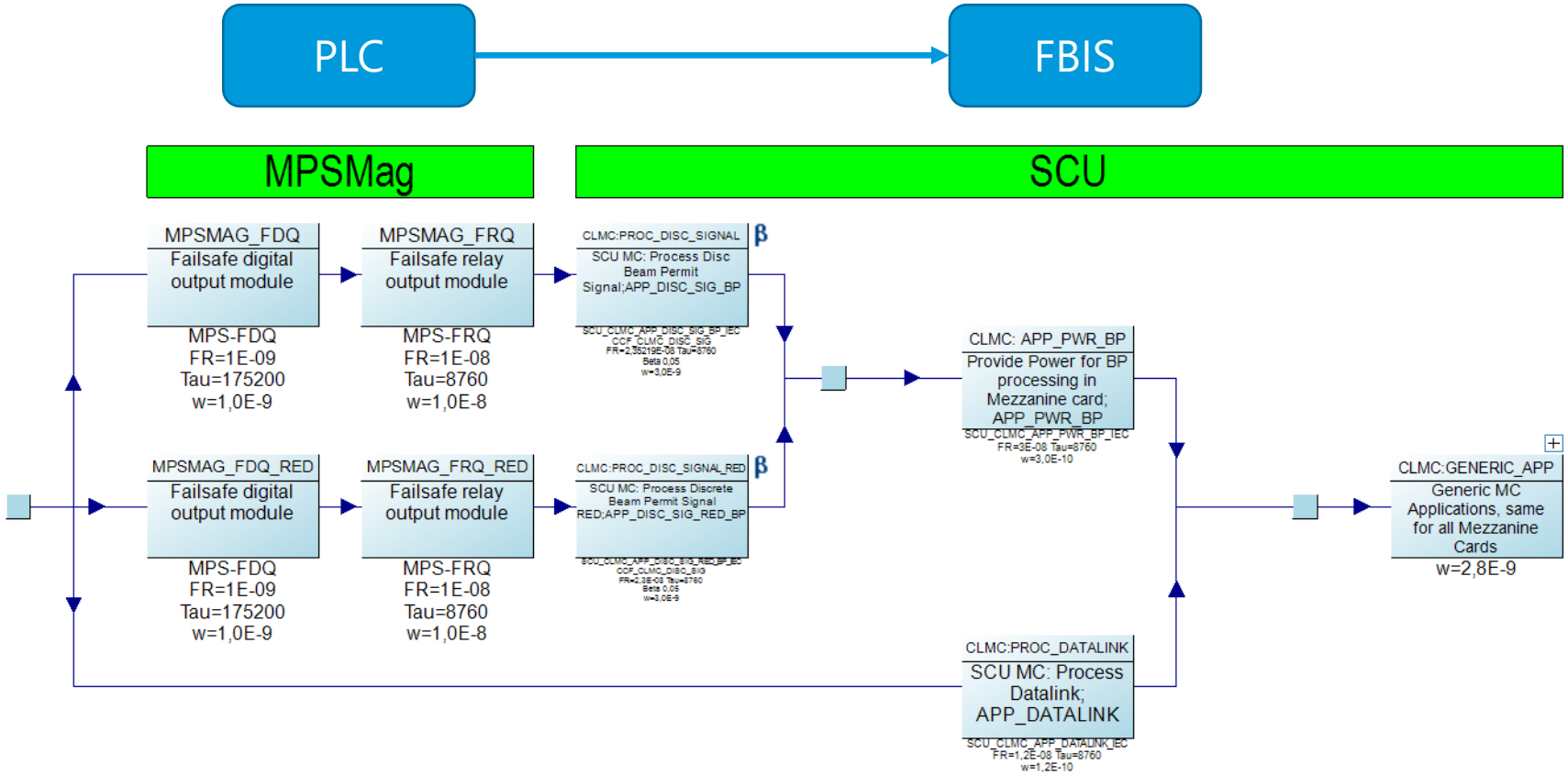
A detailed analysis is performed on the current measurement



Machine protection reliability analysis

Interface between PLC based system and FBIS

Analysis of the interface between the PLC based system and FBIS SCU

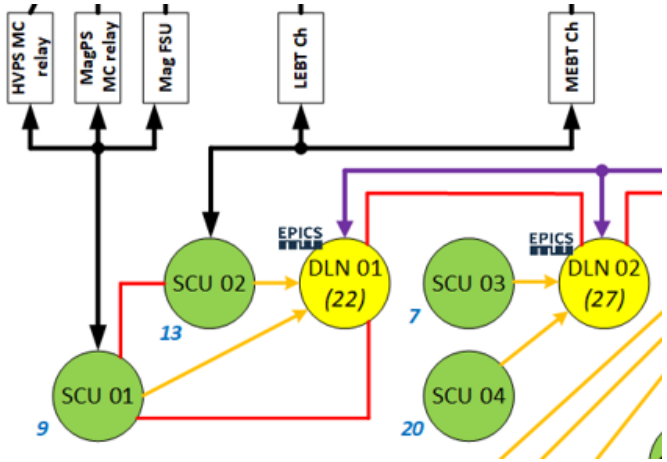


Machine protection reliability analysis

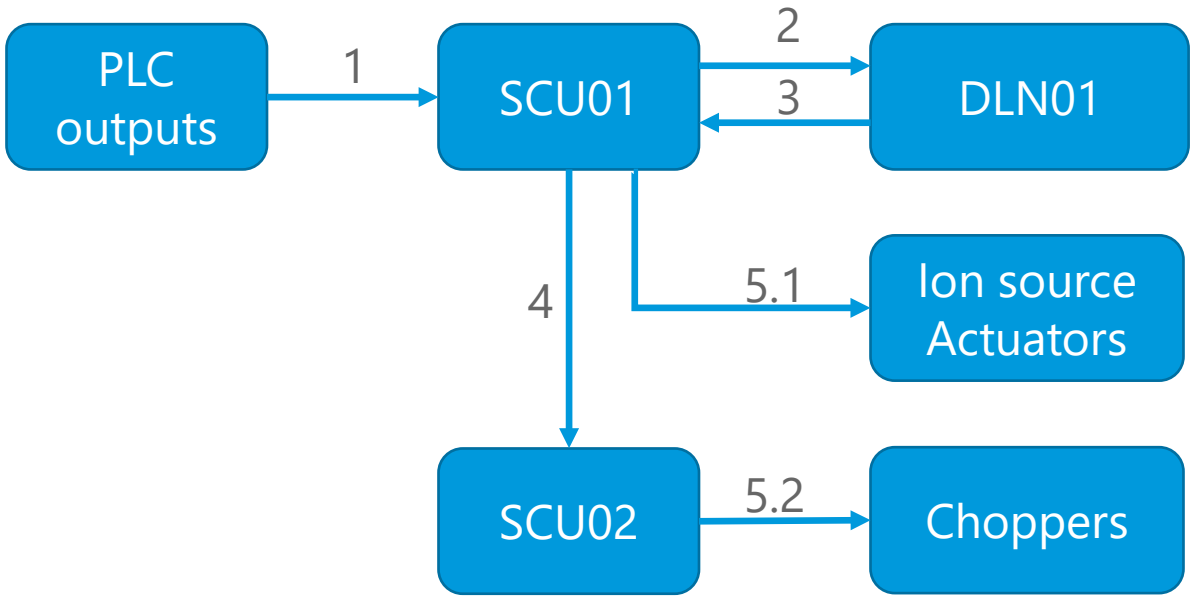
Modification of FBIS model based on input

FBIS architecture must be modified depending on what SCU the input signal is connected to and what actuators that can be used.

In this example the input signals are connected to SCU01 and all actuators can be used.



Signal chain in order 1 to 5



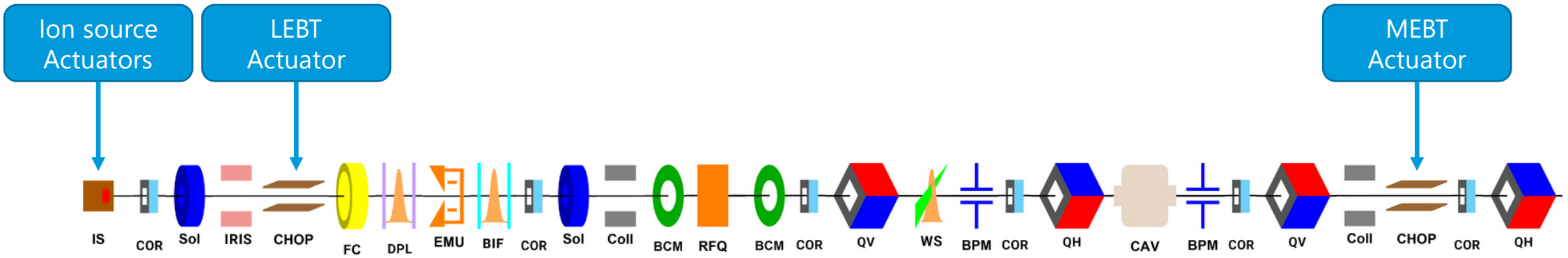
Machine protection reliability analysis

Modification of actuator side

Not all protection functions can use all actuators.

Each protection function needs to be evaluated depending on:

- Location of protected element in accelerator
- Required reaction time.



Machine protection reliability analysis

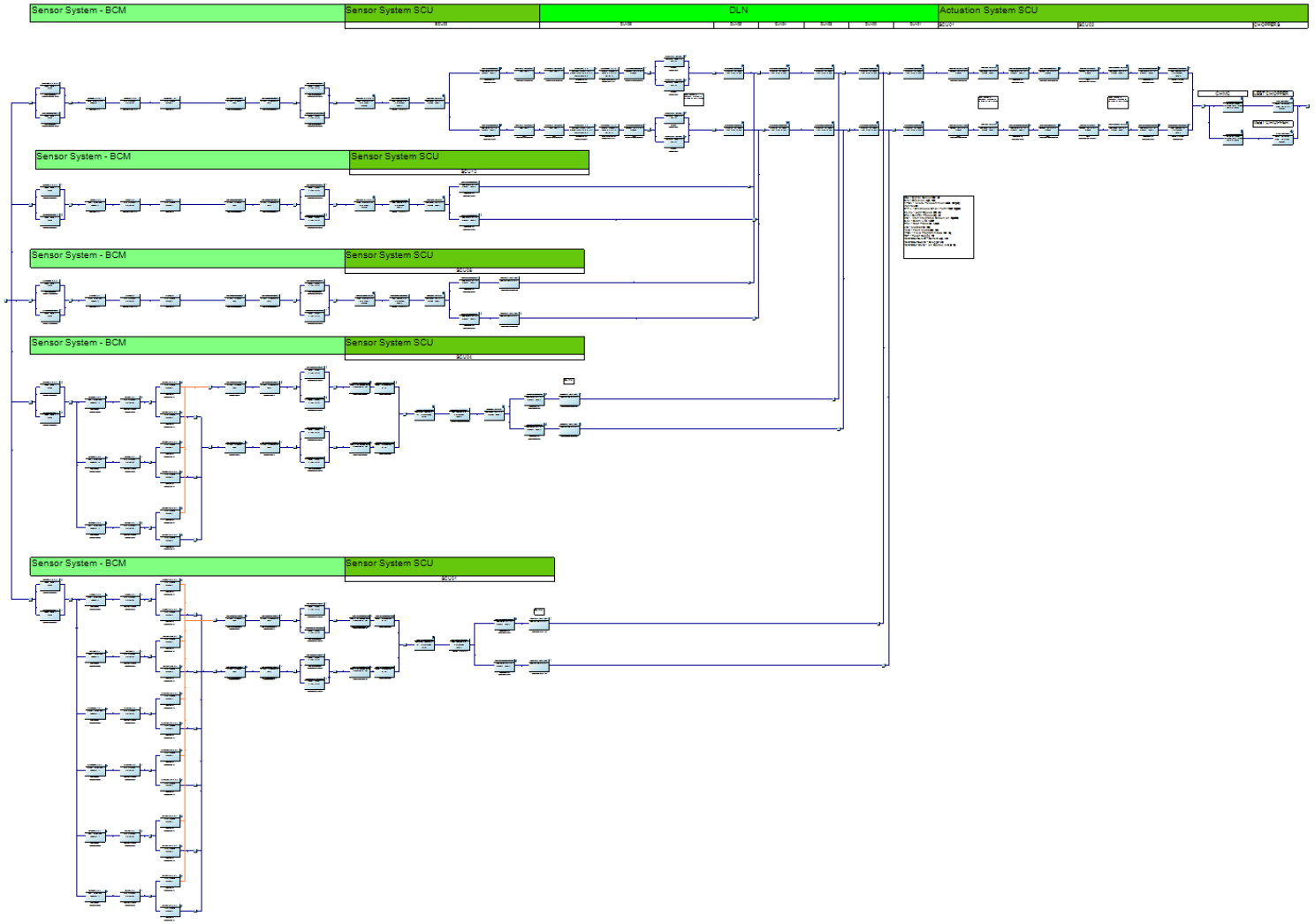
Example Results for full protection function

PF Tag	Required PIL	Required PFH	Achieved PFH	Max allowable PIL (Architectural Constraints)	Result
BLE-MAG-PF-1.1	PIL 1	<= $1 * 10^{-5}$	$4{,}8 * 10^{-7}$	PIL 1	Passed

Analysis of all Protection Functions and update of FBIS analysis is currently ongoing

Machine protection reliability analysis

Example of complex protection function calculation



5

Benefits of detailed reliability studies

Benefits of detailed reliability studies

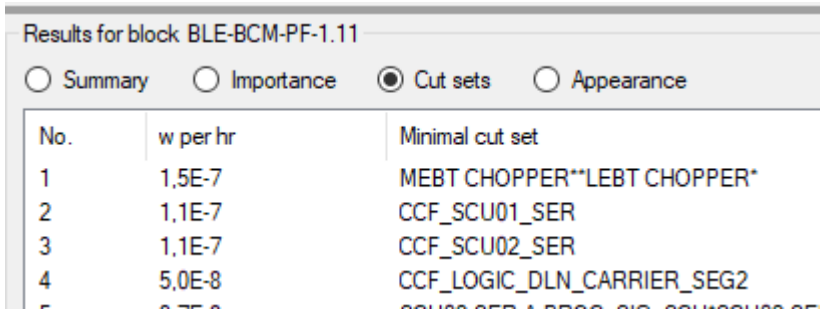
Compliance with requirements

- The calculated results show if a protection function complies with the set requirements, which is defined by the risk assessment.
- Provides a unified way of classifying how reliable all protection functions are
- Ensures that you have a robust system
- Justifies cost and effort for additional protection functions if required
- Can prevent over-engineering
  - ✓ Decreased cost
  - ✓ Less components
  - ✓ Less maintenance
  - ✓ More availability
- Helps define diagnostic functions and regular testing of the MP systems

Benefits of detailed reliability studies

Finding the weakest links

Each calculation provides the “Minimal cut sets”, which provides inputs on what parts of a complex system benefits most of improvements.


Results for block BLE-BCM-PF-1.11

Summary Importance Cut sets Appearance

No.	w per hr	Minimal cut set
1	1,5E-7	MEBT CHOPPER**LEBT CHOPPER*
2	1,1E-7	CCF_SCU01_SER
3	1,1E-7	CCF_SCU02_SER
4	5,0E-8	CCF_LOGIC_DLN_CARRIER_SEG2

This helps defining where we should put our design efforts.

Discussion

2022-10-20

Contact

Dr. Joanna Weng
- Senior Lecturer
- Certified Functional Safety Engineer
  FS Eng (TÜV Rheinland)
- Project Manger (Nuclear)

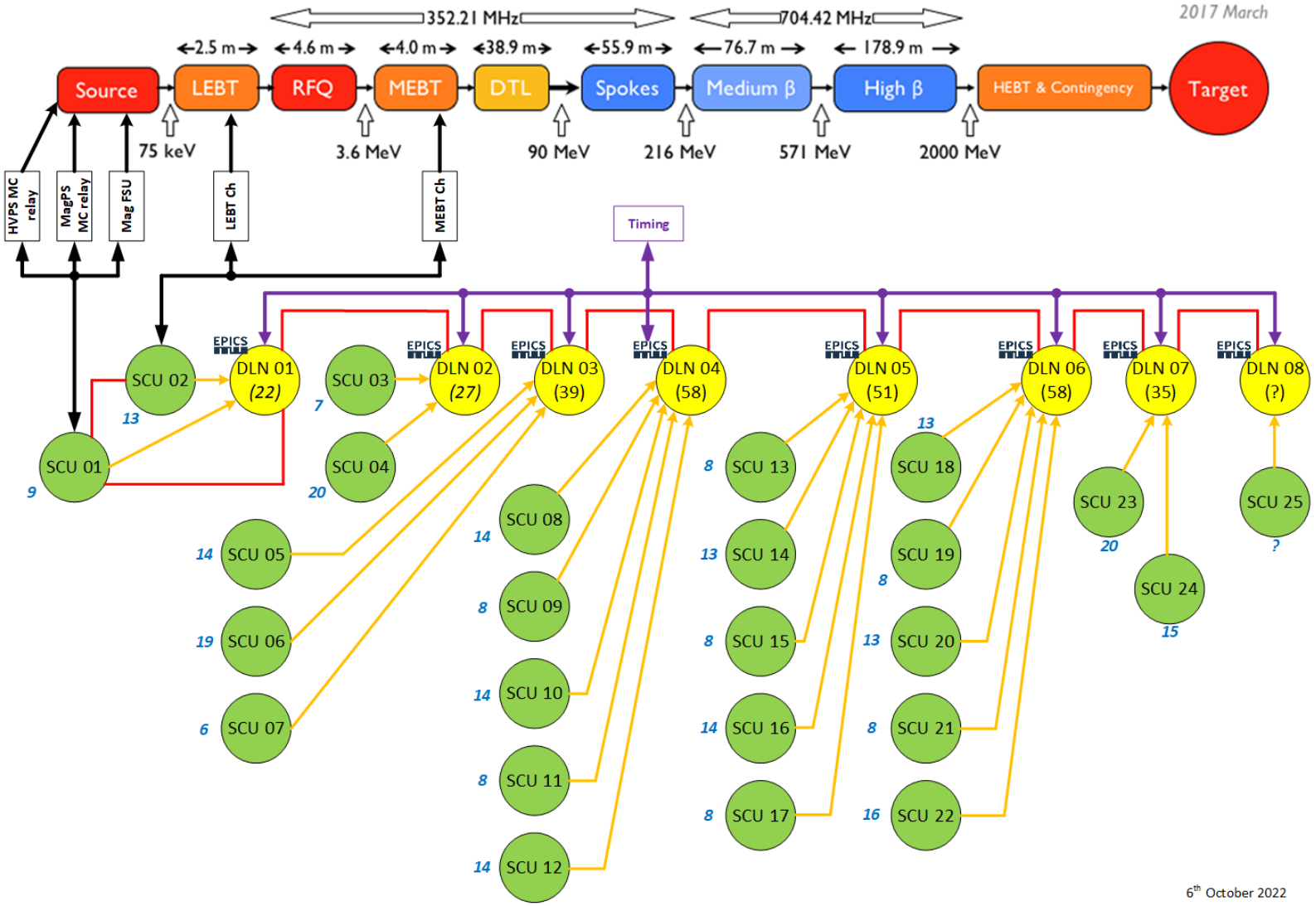
Safety Critical Systems Lab
Zurich University of Applied Sciences (ZHAW)
wenj@zhaw.ch

6

Additional slides

FBIS architecture

Layout and scope of the Fast Beam Interlock System (FBIS)



General Analysis Assumptions

- The analysis assumes constant failure rates and therefore the effects of early failures are expected to be removed by appropriate processes;
- Components are not operated beyond their useful life (no wear-out)
- It is assumed that the requirements stated in equipment safety manuals (if applicable) have been adhered to.
- When a diagnostic coverage is assigned to the dangerous failures (λ_{DD}), it must be ensured that the diagnostic coverage is properly analyzed, so that the failure is detected and hazard mitigated within acceptable time period. Where this is not possible it should be assumed that we have 0% diagnostic coverage.

Benefits of detailed reliability studies

Diagnostic functions

The analysis can provide valuable feedback for diagnostic functions, such as:

- How effective is the diagnostic function?
- How should the function be implemented?
- How often should the diagnostic function run?

Benefits of detailed reliability studies

Proof testing

The analysis can provide valuable feedback for “proof testing”, that ensures that the machine protection systems works “as good as new”, such as:

- What parts of a system needs to be tested?
- How should these tests be done?
- How often should the tests be done?