Mitglied der Helmholtz-Gemeinschaft

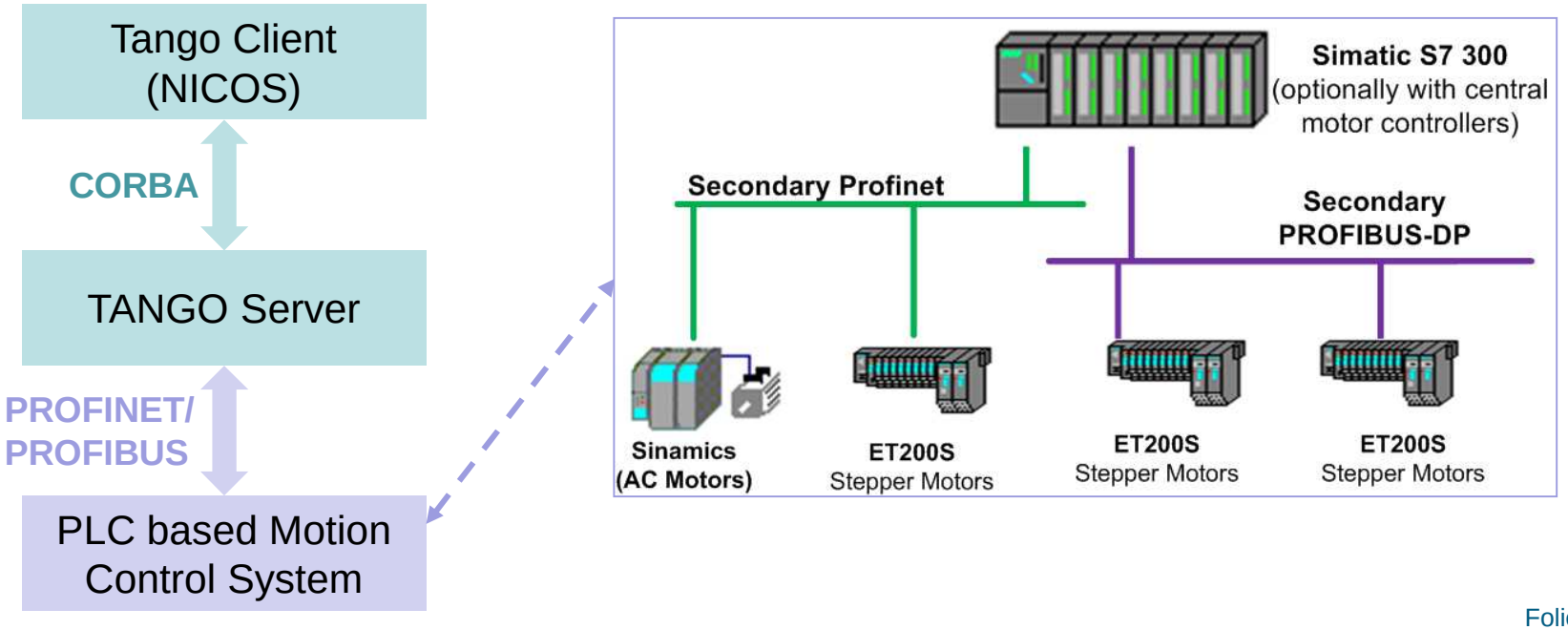
JÜLICH
FORSCHUNGSZENTRUM

Motion Control with Failsafe Requirements

Harald Kleines, Forschungszentrum Jülich, ZEA-2: Electronic Systems

Overall Architecture of JCNS Motion Control Systems

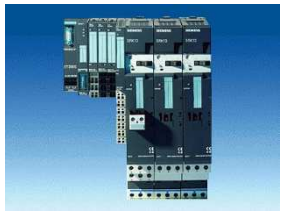
- Application Area: Neutron Scattering
- Jülich Centre of Neutron Science (JCNS) developed and operates numerous neutron instruments at its outstations at FRM-II, ILL and SNS
- ZEA-2 is responsible for the control and data acquisition systems of all JCNS neutron instruments
- Neutron Instruments: comparable to synchrotron beamlines
  - About 30 mechanical axes, mostly stepper motors
  - Relative slow movement due to heavy shielding and low count rates



PLC Based Motion Control

- PLCs: Mainly Siemens S7-300

- Decentral Periphery: Mainly ET200S



- Motor Controllers:

1STEPdrive

FM353

Sinamics S120

- PLC hides mechanical and functional specialities
  - Abstract hierarchical controller/axis model independent of the specific motor controller
  - Important information directly mapped into the PROFIBUS/PROFINET IO-Space (similar to EPICS motor record)
  - Additional information/commands via transactions
- **Standard PLCs not sufficient for personal protection!!!**

Functional Safety

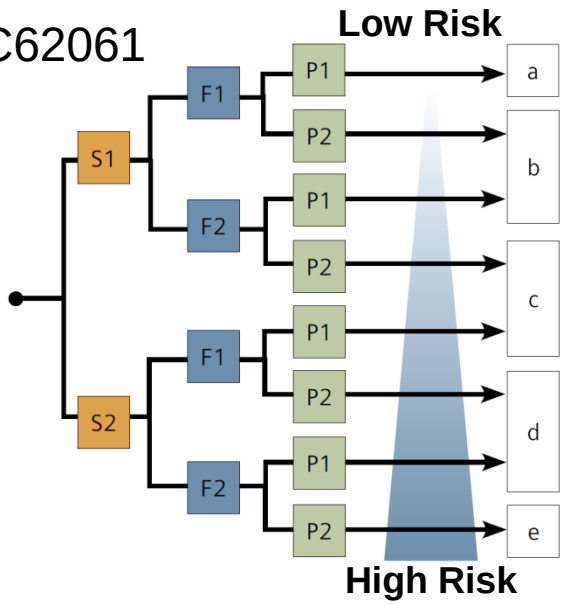
- Safety engineering: Minimization of dangers for humans, environment,….
- Dangers: heat, electrical shock, radioactivity,…
- Variety of international and national regulations (standards, laws, directives,..)
- Automation systems: Functional safety
  - Minimization of system failure

- Possible Solutions: High availability or failsafe
- Failsafe: Switch off leads to a safe system

Functional Safety Standards

- Motion control systems in Europe: Machinery directive of the EU
- IEC 62061: sector specific standard derived from IEC61508
  - Specific for electrical and programmable electronic control systems
  - Quantitative risk classification => Safety Integrated Levels (SIL) 1 – 4
- ISO/EN 13849-1: Successor of EN 954
  - Also applicable to hydraulic and pneumatic systems
  - Determination of Performance Level (PL) a-e by risk graph
  - Also quantitative probability classification (simpler)
  - Based on control system models
  - Easier too use but not as flexible as IEC62061

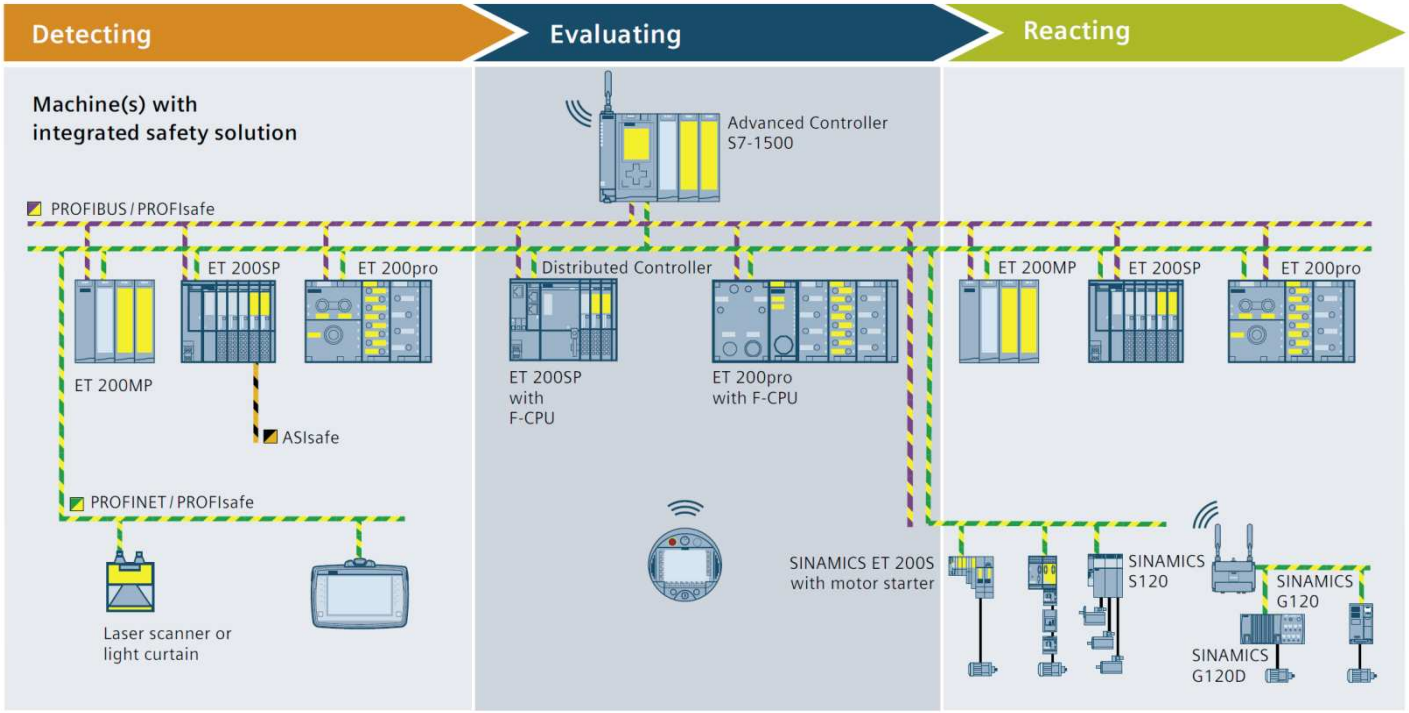
Risk parameters
S = Severity of the injury
S1 = Minor (generally reversible) injury
S2 = Severe (generally irreversible) injury, including death
F = Frequency and/or duration of exposure to the hazard
F1 = Seldom to more often and/or short duration of exposure
F2 = Frequent to constant and/or long duration of exposure
P = Possibilities of avoiding the hazard or limiting the harm
P1 = Possible under certain conditions
P2 = Hardly possible
a, b, c, d, e = Targets of the safety-related Performance Level



Products and Systems

- Certified Sensors (e.g. Switches, Laser Scanner,…)
- Certified Actuators
- Safety relays
- Failsafe and high available logic controllers
  - Specialized companies: PILZ, HIMA
  - Big Players: Siemens, Rockwell Automation,…
- Extension of fieldbus systems: Safetybus p, PROFIsafe, Safety at Work,..
- Safety Integrated: Massive market entrance of Siemens on all of the above areas
  - Extremely scalable and homogenous

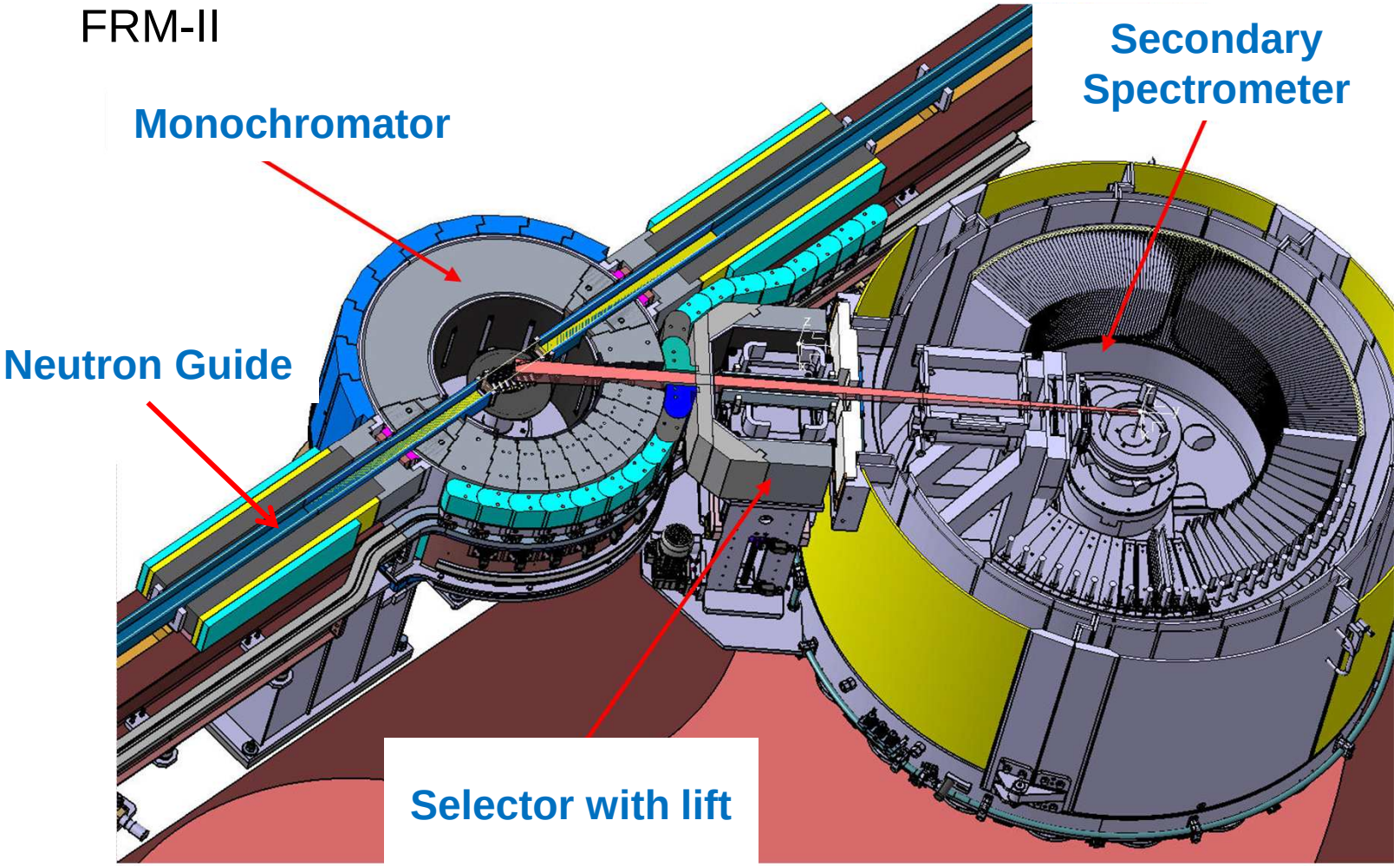
Siemens Safety Integrated



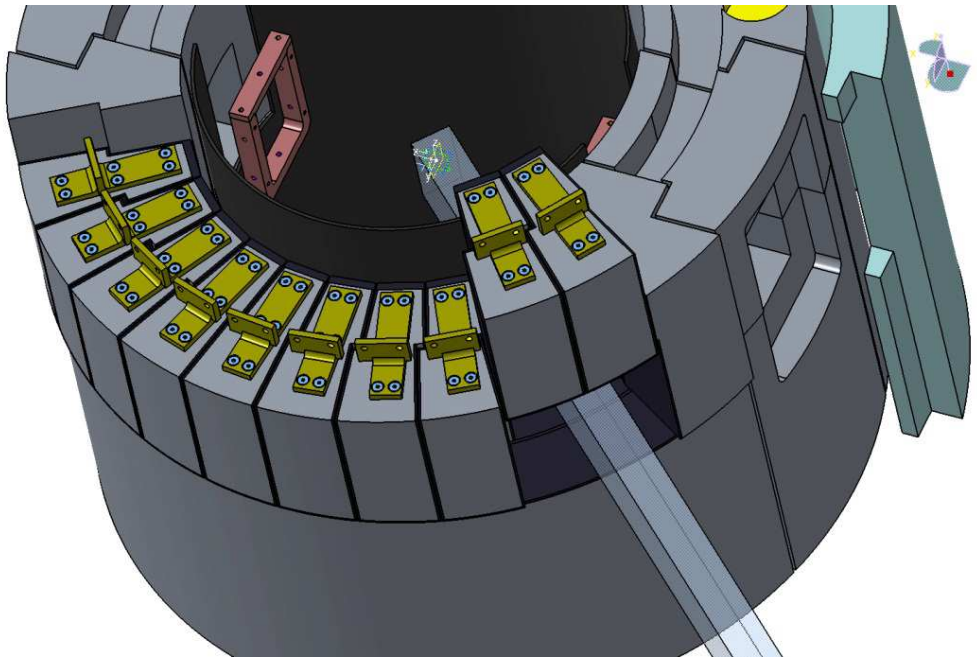
- Special failsafe CPUs (F-CPUs; S7-400 provides even high availability)
- Standard PROFIBUS/PROFINET hardware extended by application layer protocol to implement PROFIsafe
- Special failsafe peripheral modules can be mixed with standard peripheral modules
- Failsafe Program can coexist with standard program on the same CPU
- Engineering: Add-on to Step7 or TIA Portal
- Up to IEC61508 SIL3 and ISO 13849 PLe

Example Application: Monochromator at DNS

- DNS (Diffuse Neutron Scattering): Cold time-of-flight neutron spectrometer with polarization analysis operated by JCNS at FRM-II



Lead Block Movement and Interlock

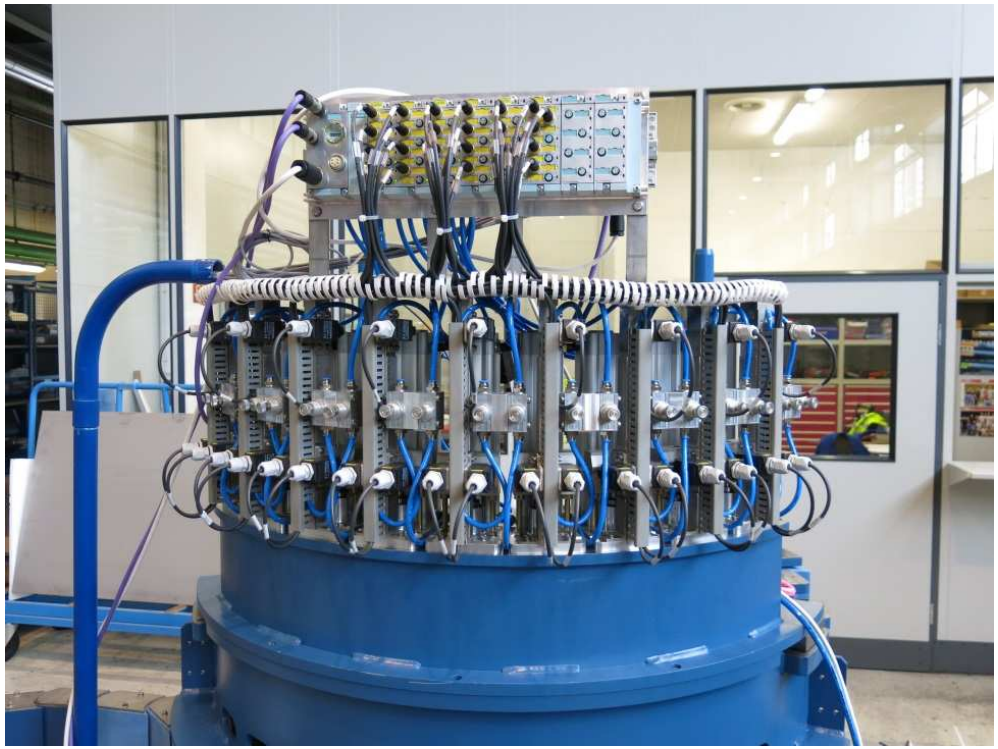


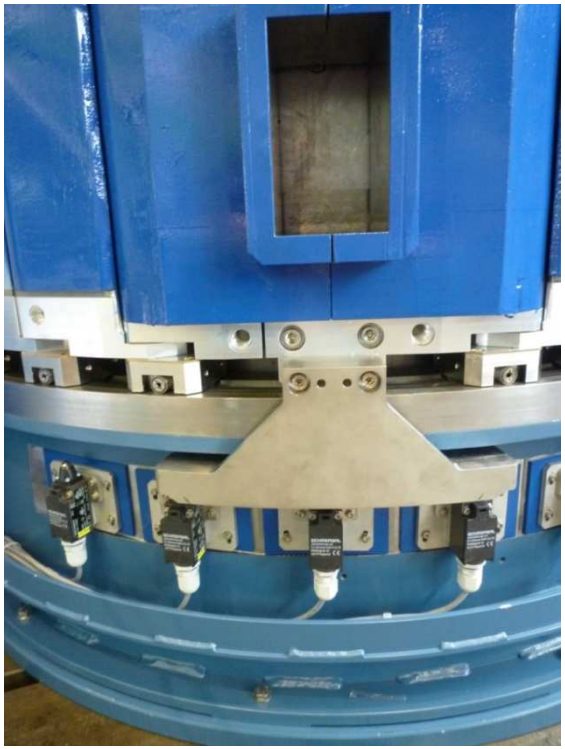
- Monochromator crystal position dependent on the position of the secondary spectrometer
- A maximum number of 2 lead blocks is allowed to open
- Only lead blocks at the position of the secondary spectrometer are allowed to open
- Interlock between lead block movement and beam shutter control

Lead Block Movement

- Lead alock movement by pneumatic cylinders
- Controlled by Festo CPX decentral IO system with valve manifold
  - IP67
  - Interface to PLC via PROFIBUS

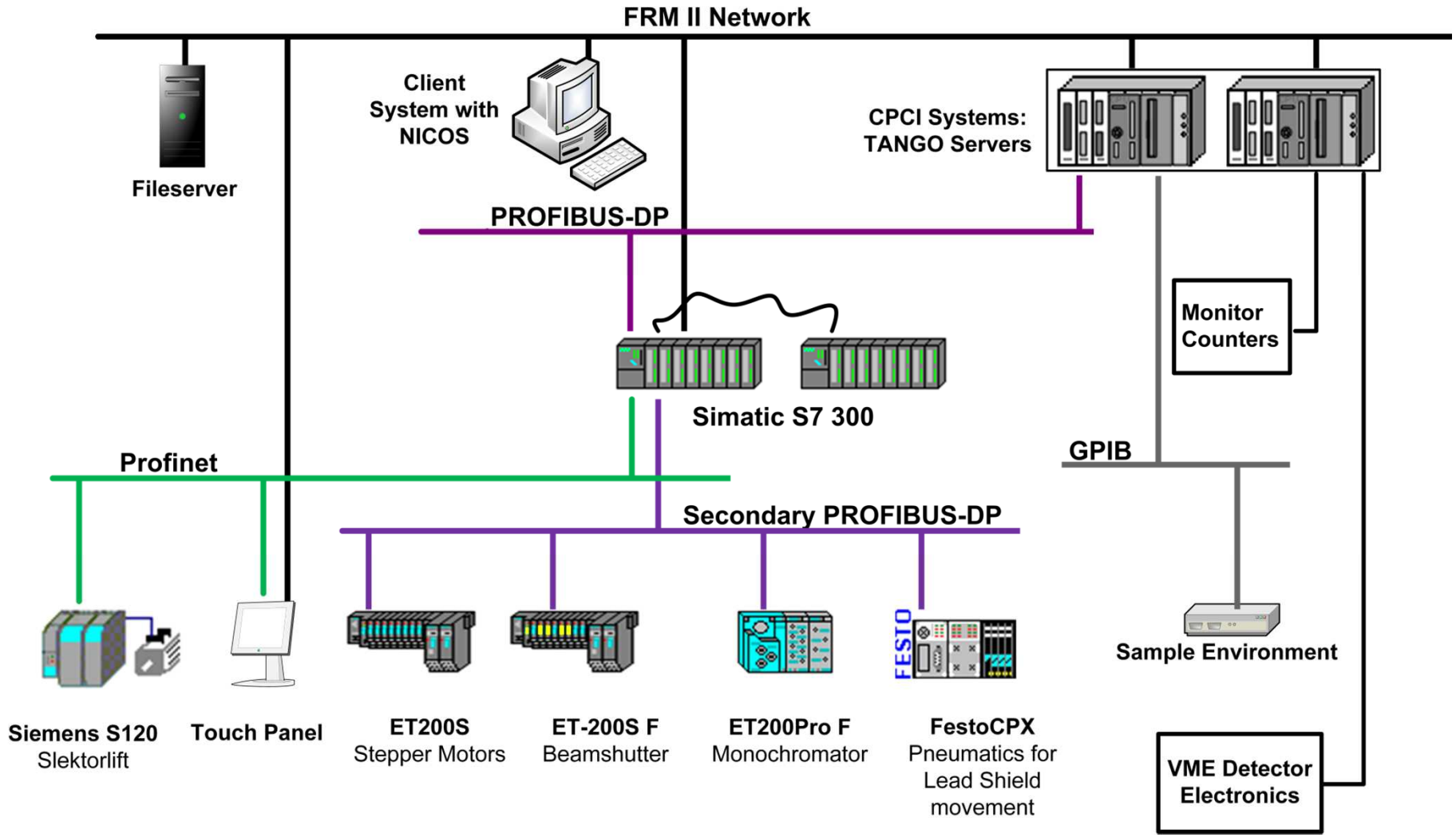
Position Detection





- Safety interlock relies only on limit switches for the lead block position and rotation of the secondary spectrometer
- Safety limit switches with internal redundancy
- Readout of limit switches with ET200pro F (failsafe, IP67) and PROFIsafe
- Encoder on rotation axis only informative

Physical Architecture of the Control and DAQ System

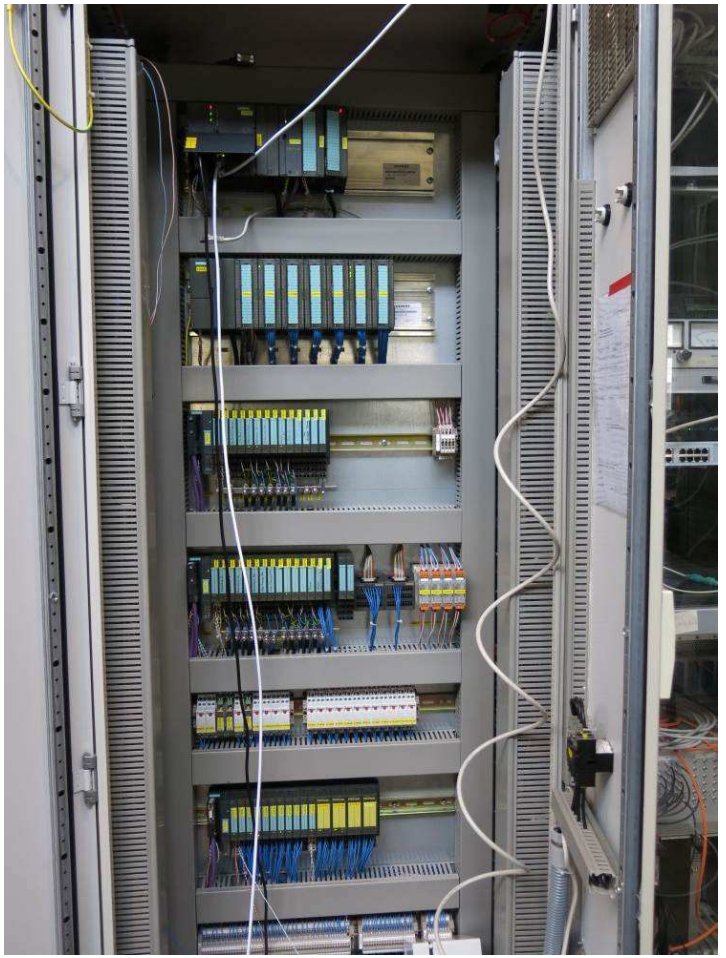


System Overview

Secondary Spectrometer

Selector with lift

Mono-chromator



Main cabinet with PLC

Conclusion

- Failsafe approach in the case of a system failure
  - Stop Movement
  - Block opening of shutters
  - Emergency close of shutters and lead blocks
- Siemens Safety Integrated:
  - Powerful
  - Scalable
  - Homogeneous (Extension of standard HW and engineering tools)
- Important: Use proper sensors and actuators (e.g. safe switches)

Figures on slides 5 and 7 by Siemens AG,
Figures on slides 8 and 9 by Romuald Hanslik