Zurich University
of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Safety-Critical Systems Research @IAMP

Martin Rejzek, Christian Hilbes

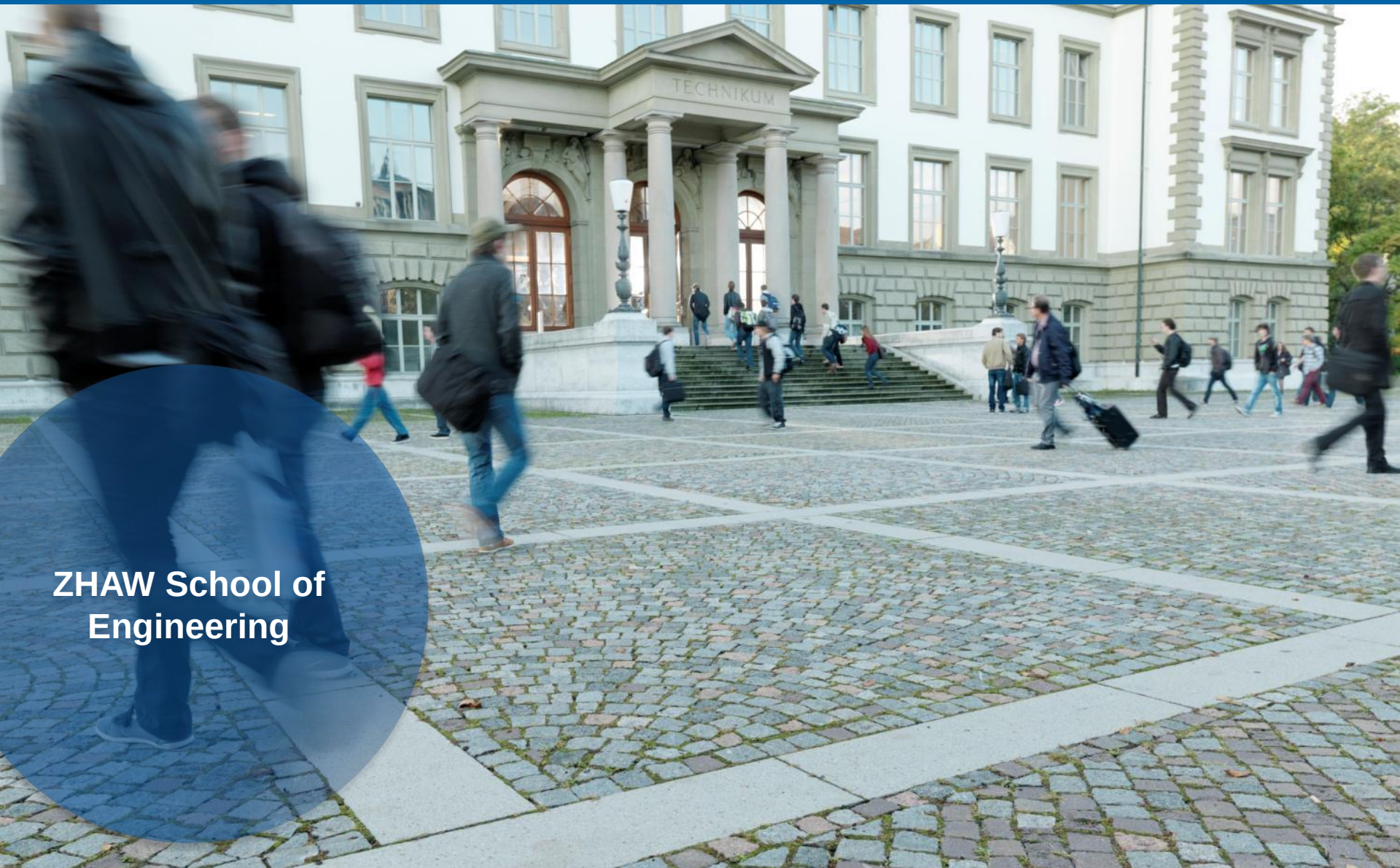
ESS Machine Protection Workshop - CERN 03-04.02.2015

Zurich University
of Applied Sciences

zh
aw

School of
Engineering

IAMP Institute of Applied
Mathematics and Physics



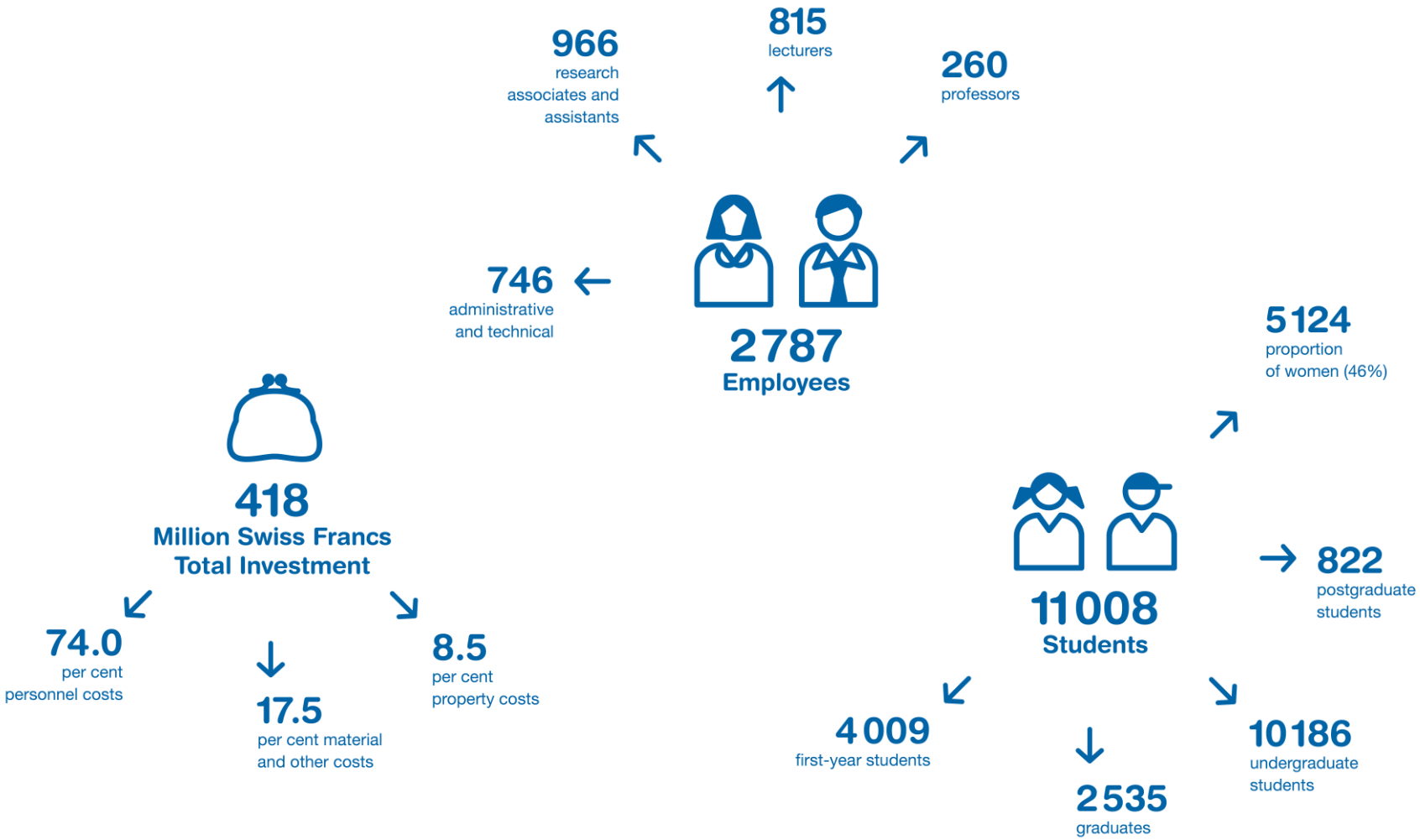
ZHAW School of Engineering

ZHAW in Numbers

Zurich University of Applied Sciences

School of Engineering

IAMP Institute of Applied Mathematics and Physics



ZHAW – Areas of Activity

Zurich University of Applied Sciences

School of Engineering

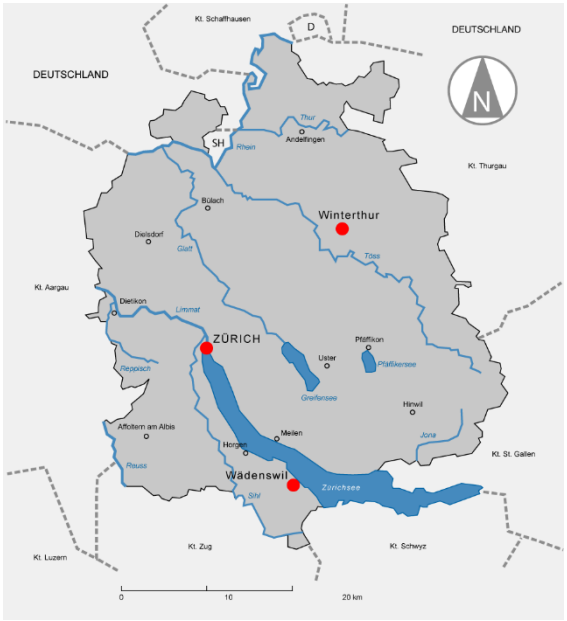
IAMP Institute of Applied Mathematics and Physics

ZHAW – Locations and Departments

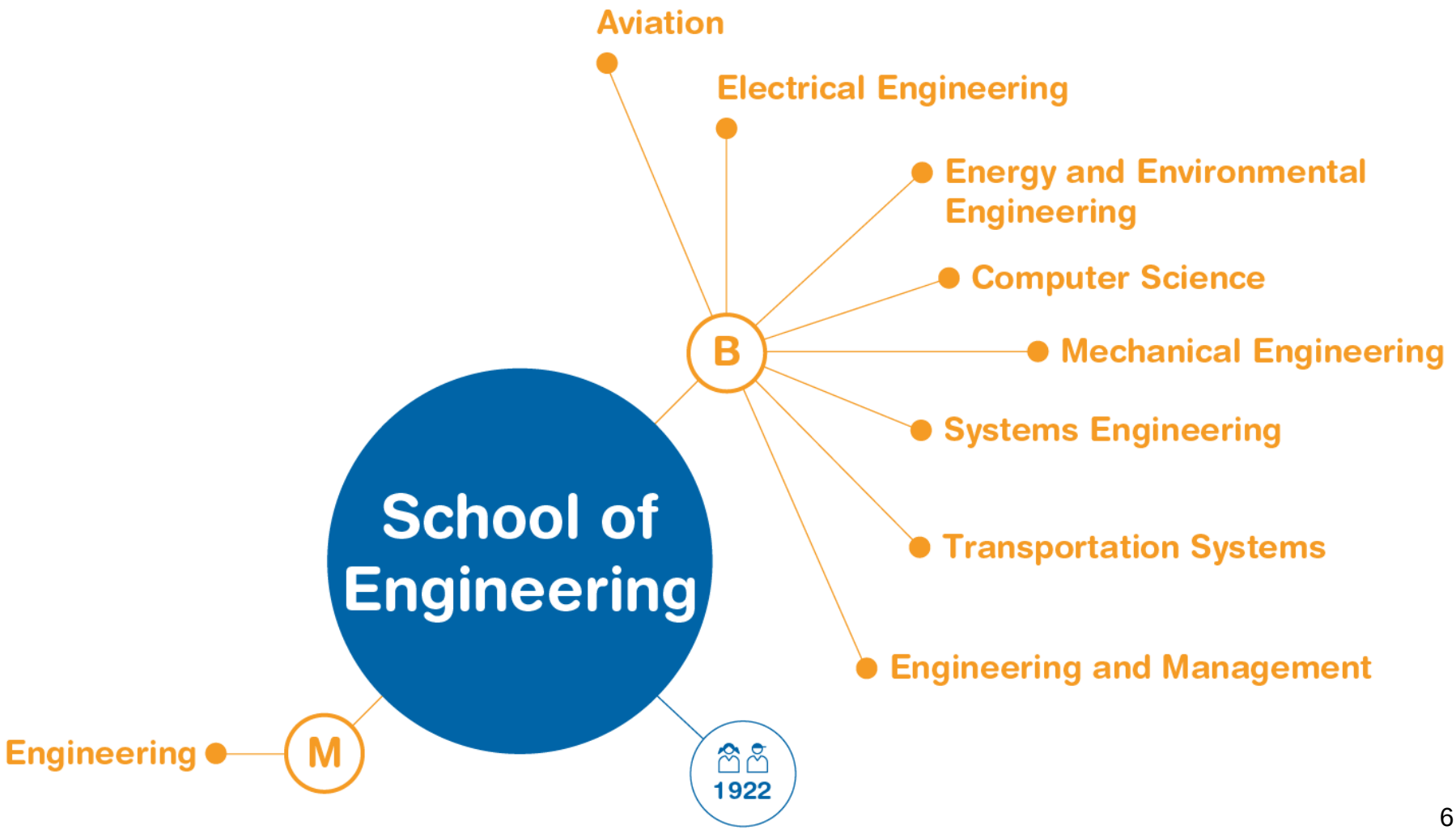
Zurich University of Applied Sciences

School of Engineering

IAMP Institute of Applied Mathematics and Physics



School of Engineering - Education

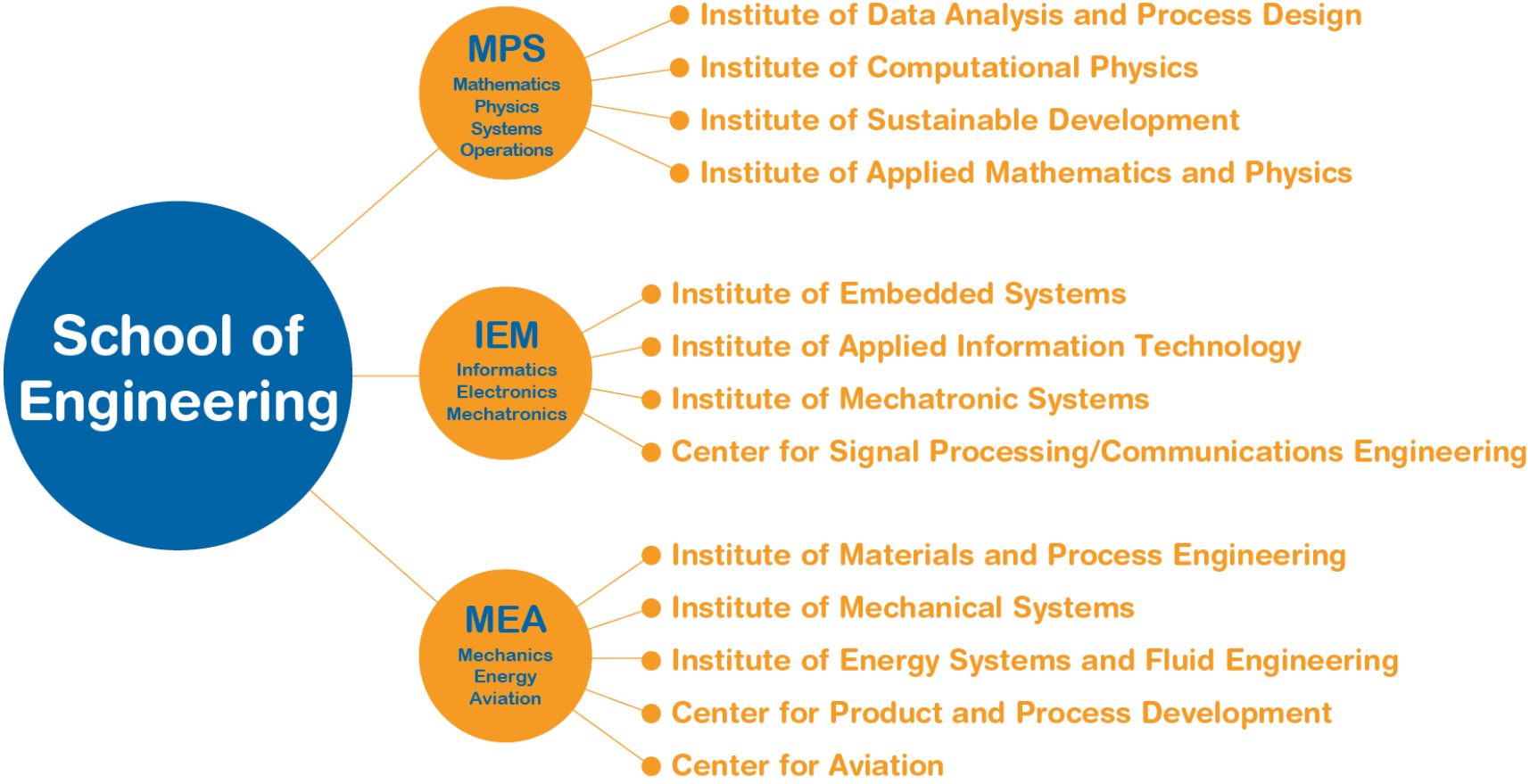


Frackumzug

Zurich University
of Applied Sciences

zh aw School of Engineering
IAMP Institute of Applied Mathematics and Physics

School of Engineering – Applied R&D

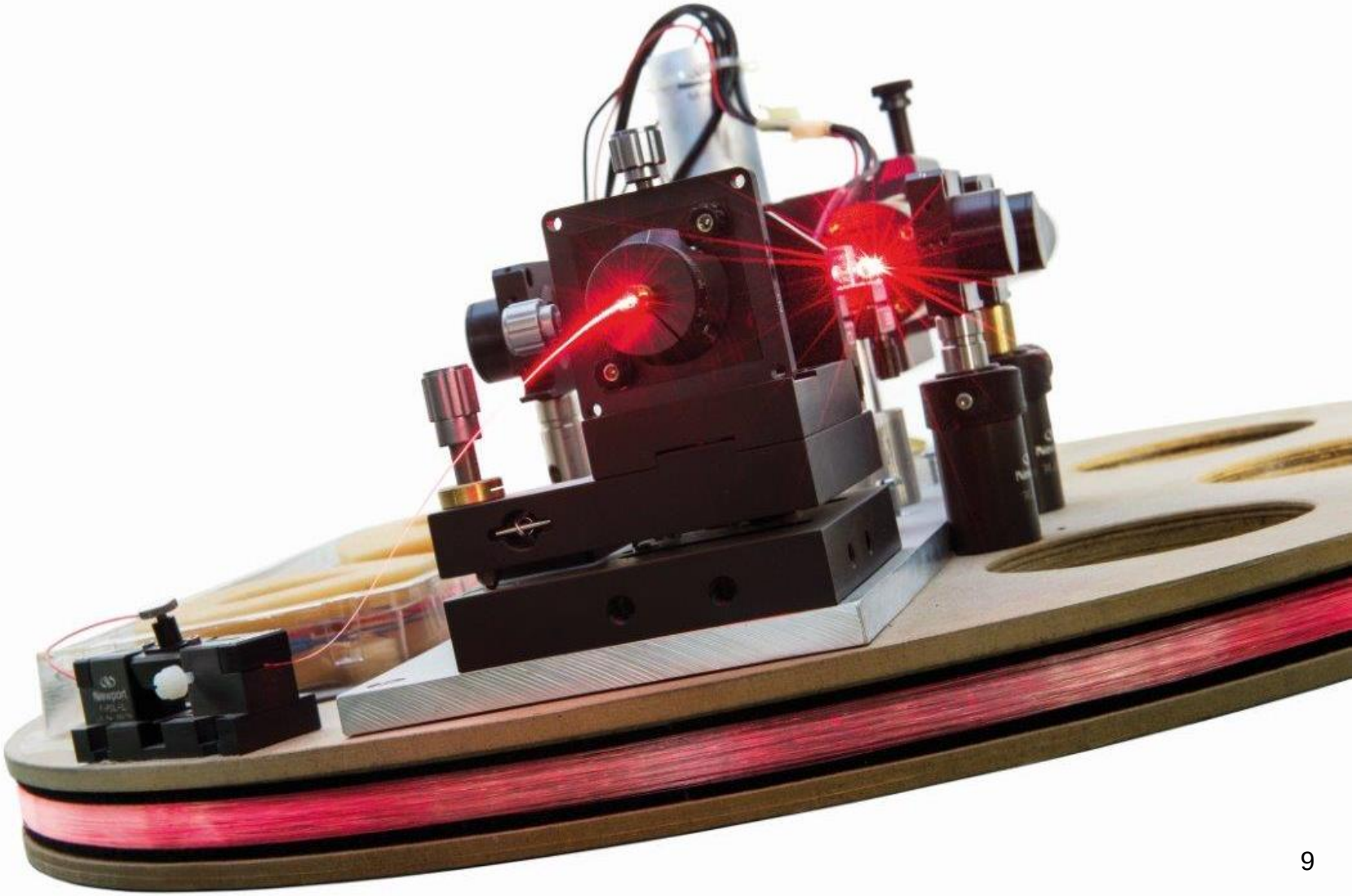


Institut of Applied Mathematics und Physics (IAMP)

Zurich University of Applied Sciences

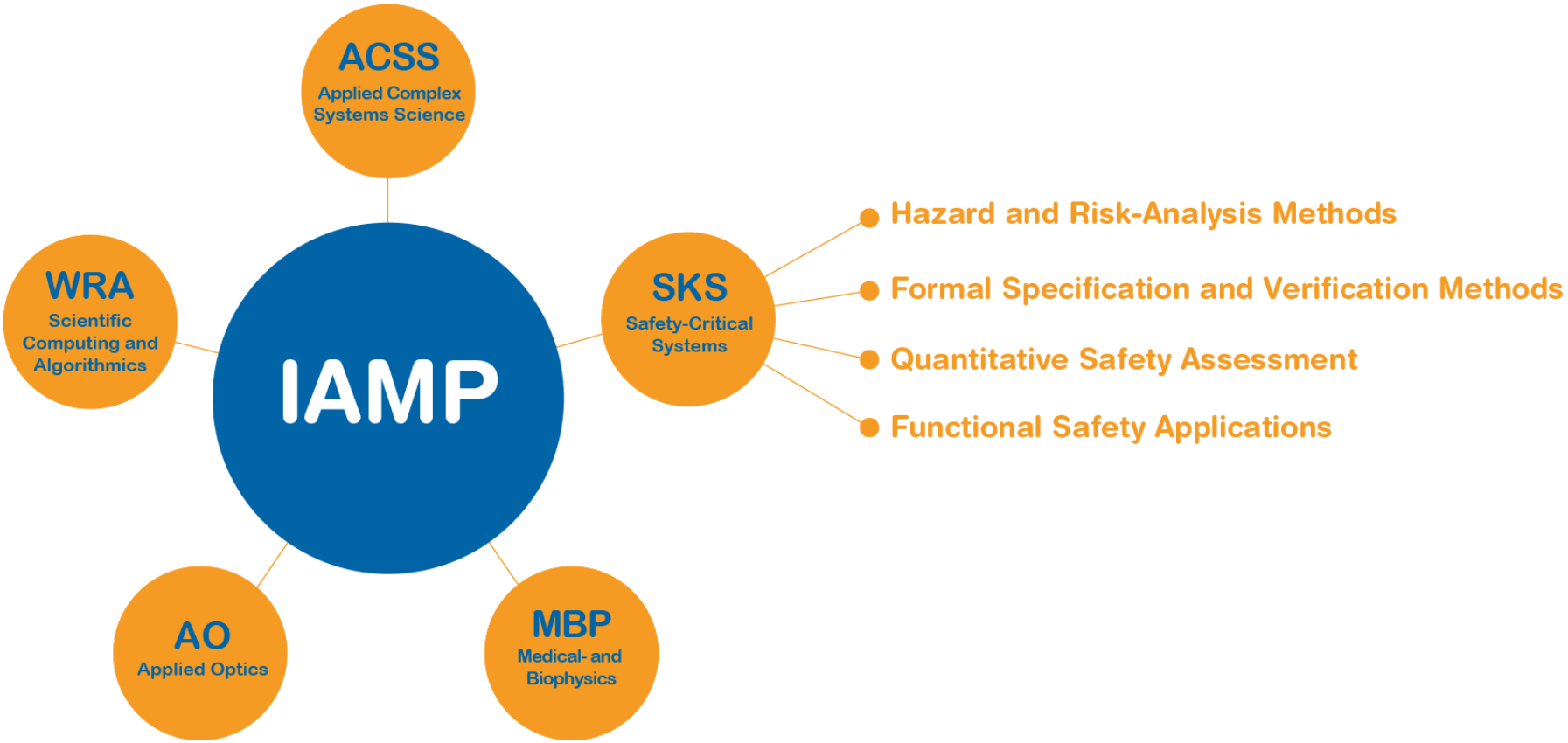
School of Engineering

IAMP Institute of Applied Mathematics and Physics



Safety-Critical Systems Research @IAMP

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics



Safety-Critical Systems Research - Team

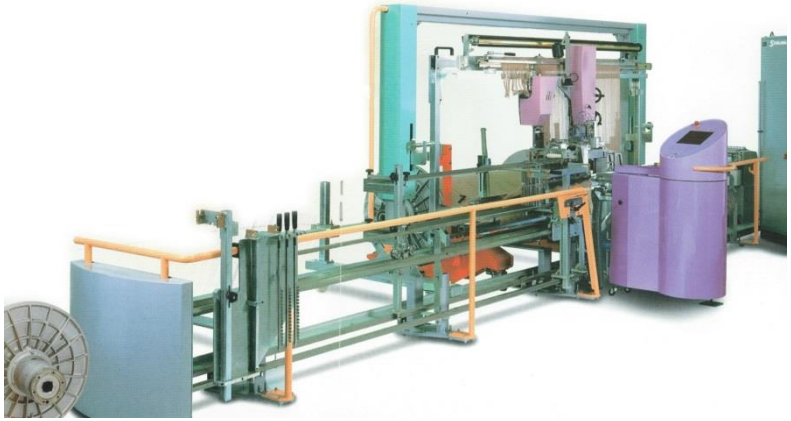
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

- Martin Rejzek
  - Dipl. El.-Ing. FH
  - CAS Project-Management
  - Safety Professional EigV
  - Co-Founder SafeCert Consulting GmbH

Safety-Critical Systems Research - Team

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

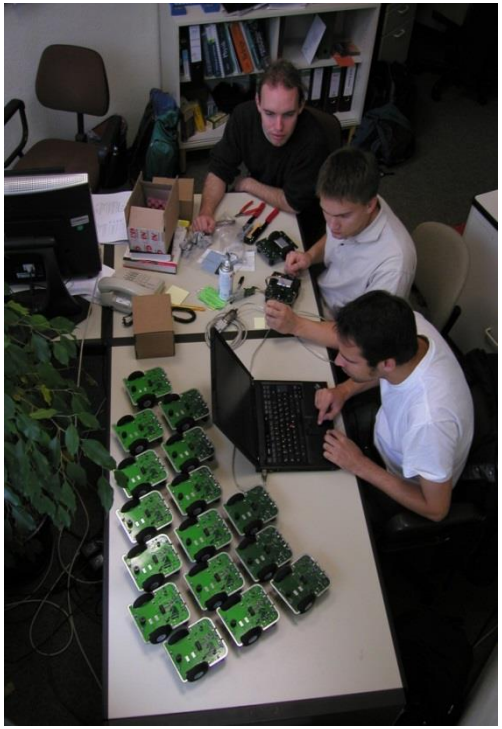
- Martin Rejzek
  - Dipl. El.-Ing. FH
  - CAS Project-Management
  - Safety Professional EigV
  - Co-Founder SafeCert Consulting GmbH
  - Professional Background
    - Stäubli AG Sargans



Safety-Critical Systems Research - Team

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

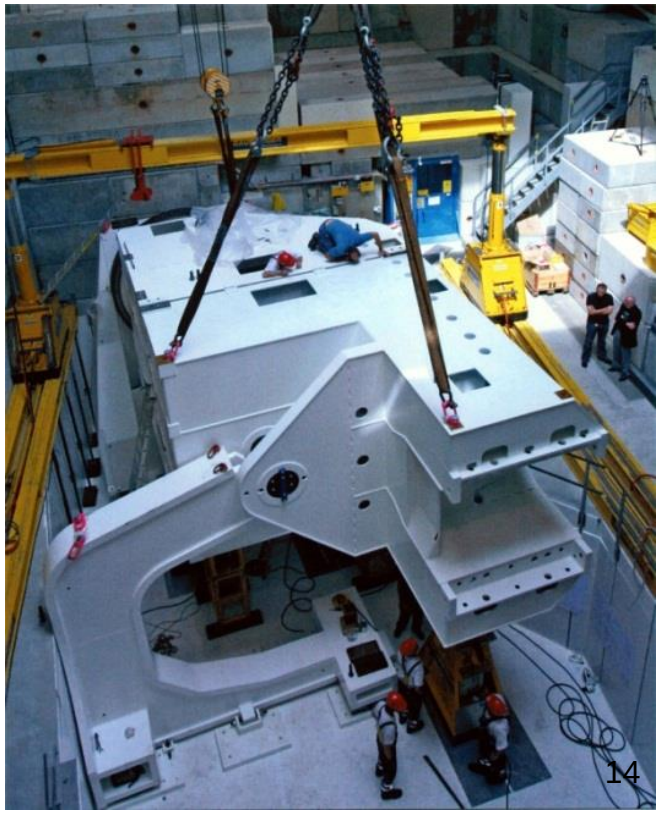
- Martin Rejzek
  - Dipl. El.-Ing. FH
  - CAS Project-Management
  - Safety Professional EigV
  - Co-Founder SafeCert Consulting GmbH
  - Professional Background
    - Stäubli AG Sargans
    - Fraunhofer Gesellschaft



Safety-Critical Systems Research - Team

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

- Martin Rejzek
  - Dipl. El.-Ing. FH
  - CAS Project-Management
  - Safety Professional EigV
  - Co-Founder SafeCert Consulting GmbH
  - Professional Background
    - Stäubli AG Sargans
    - Fraunhofer Gesellschaft
    - Paul Scherrer Institute



Safety-Critical Systems Research - Team

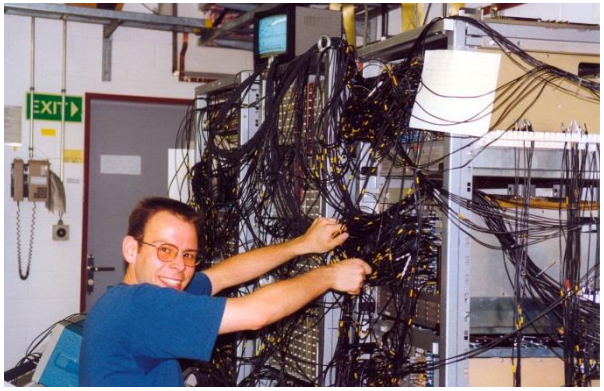
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

- Martin Rejzek
  - Dipl. El.-Ing. FH
  - CAS Project-Management
  - Safety Professional EigV
  - Co-Founder SafeCert Consulting GmbH
  - Professional Background
    - Stäubli AG Sargans
    - Fraunhofer Gesellschaft
    - Paul Scherrer Institute
    - Senior Research Associate IAMP

Safety-Critical Systems Research - Team

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

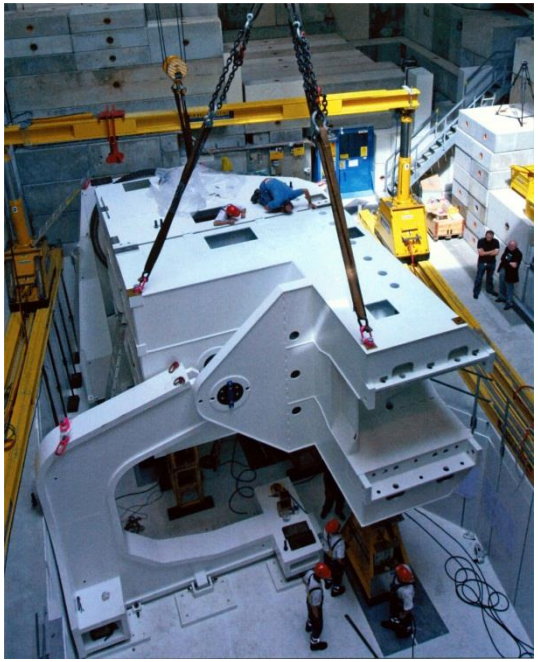
- Dr. Christian Hilbes
  - Physics Diploma ETH Zürich (1997)
  - PhD Experimental Particle Physics ETH / PSI (2001)



Safety-Critical Systems Research - Team

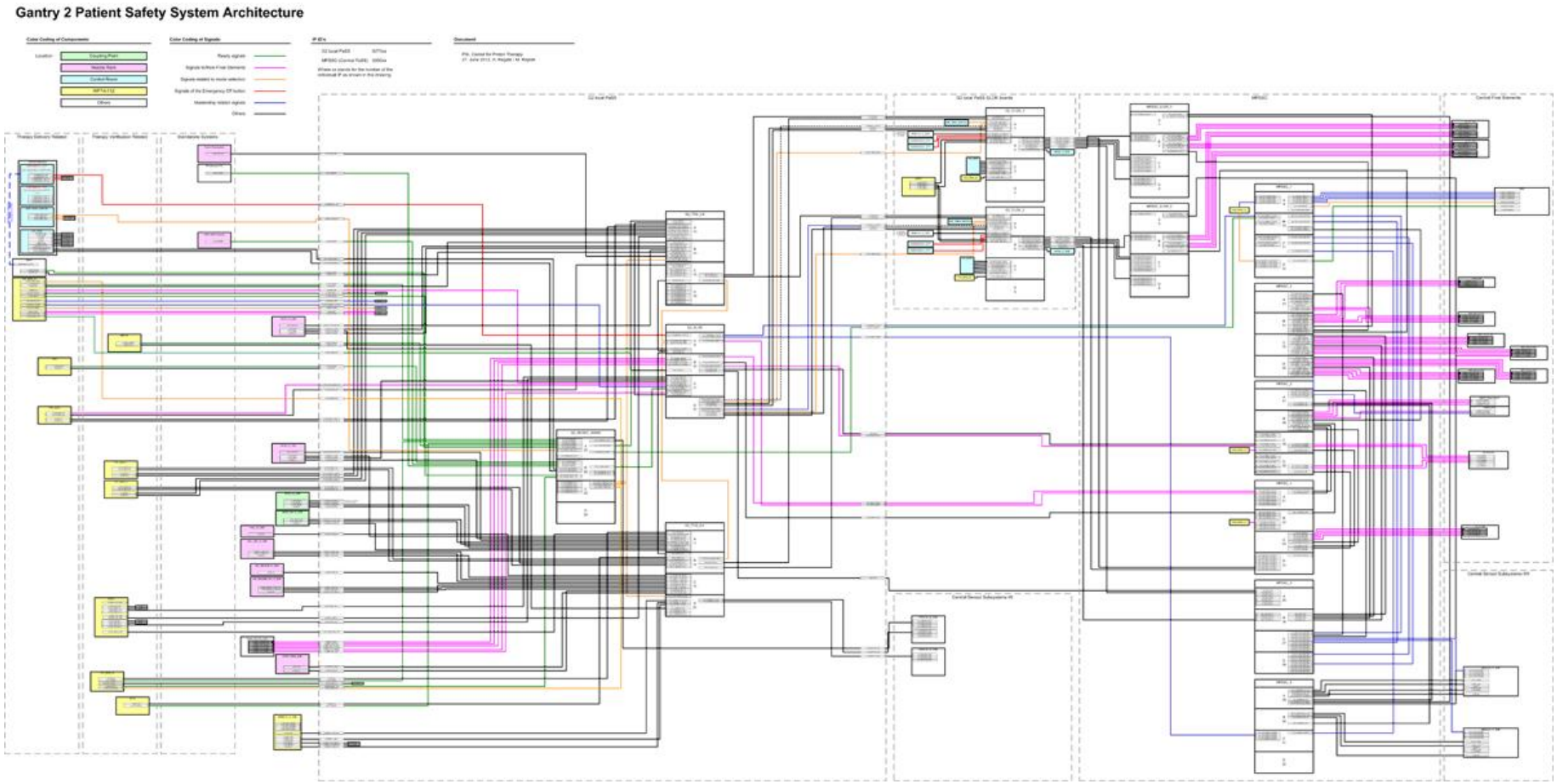
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

- Dr. Christian Hilbes
  - Physics Diploma ETH Zürich
  - PhD Experimental Particle Physics
    ETH / PSI
  - Research Associate Center for Proton Therapy - PSI
  - Head Therapy-Control and Patient-Safety-Systems
    CPT - PSI



Unnecessary Complex? - !

Zurich University
of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics



Safety-Critical Systems Research - Team

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

- Dr. Christian Hilbes
  - Physics Diploma ETH Zürich
  - PhD Experimental Particle Physics ETH / PSI
  - Research Associate Center for Proton Therapy - PSI
  - Head Therapy-Control and Patient-Safety-Systems CPT - PSI
  - Product Safety Manager Rheinmetall Air Defence AG
  - Co-Founder SafeCert Consulting GmbH

Safety-Critical Systems Research - Team

- Dr. Christian Hilbes

  - Physics Diploma ETH Zürich
  - PhD Experimental Particle Physics ETH / PSI
  - Research Associate Center for Proton Therapy - PSI
  - 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
  - IAMP Head Applied Research & Development, Head Safety-Critical Systems Research
  - CAS Risk and Safety ETH Zürich
  - Safety Engineer EiV
  - Medical Products Expert CH/EU IPQ
  - TÜV Süd Certified Functional Safety Professional IEC 61508/IEC61511

Safety-Critical Systems Research - Team

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Dr. Karl Lermer

- Dipl. and PhD Mathematics
- Research Associate Institute for Informatics University Zürich
- Research Fellow Software Verification Research Centre University of Queensland, Brisbane, Australia
- Lecturer IAMP

Dr. Monika Reif

- Dipl. Ing. Mechanical Engineering, PhD Reliability Engineering
- Research Associate University Stuttgart
- Development Engineer Functional Safety BMW
- Safety Engineer Bombardier
- Lecturer IAMP

Sven Krauss

- Technical School Precision Engineering, Dipl. Inf. FH Computer Engineering
- Functional Safety Engineer TÜV Rheinland
- Executive Master in International Business Management
- Senior Research Associate IAMP

Safety-Critical Systems Research @IAMP

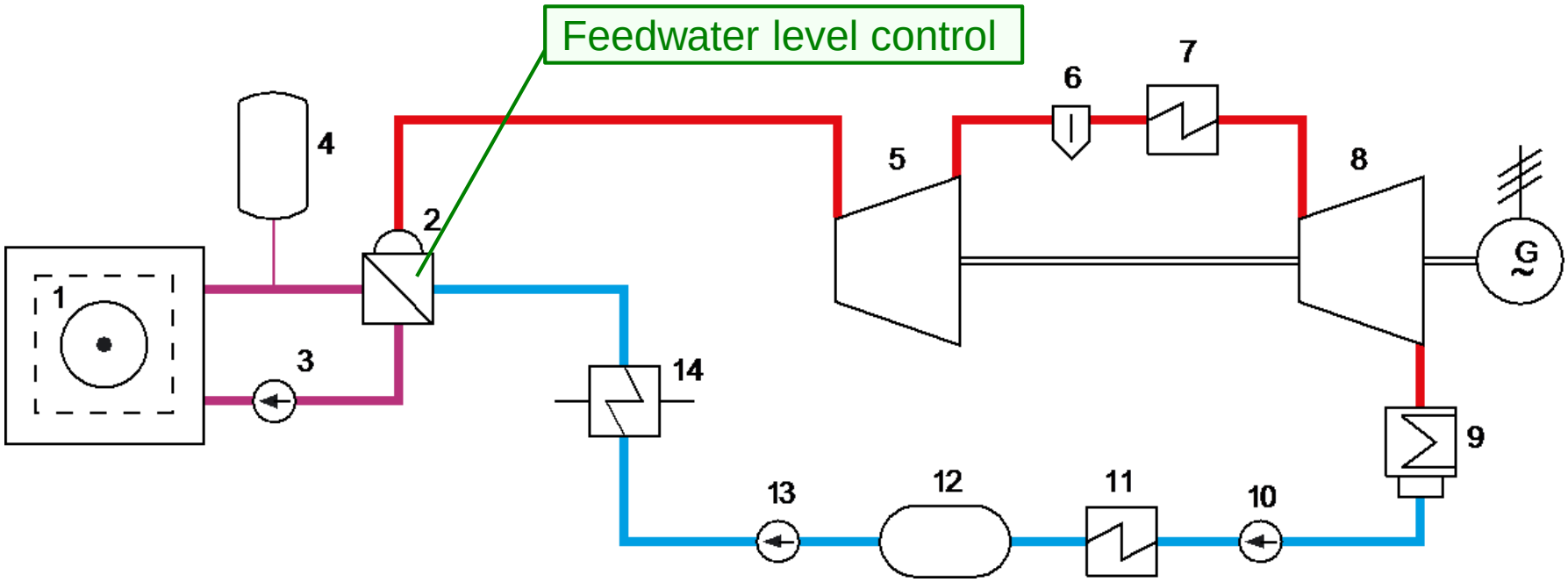
- Project Examples
  - Quantitative Software-Reliability Modeling of digital I&C Systems
    - Nuclear Power Plant Gösgen
  - FPGA based Railway Control Centre Development
    - Super-Computing-Systems Zürich, SBB, DB, ÖBB

Safety-Critical Systems Research @IAMP

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

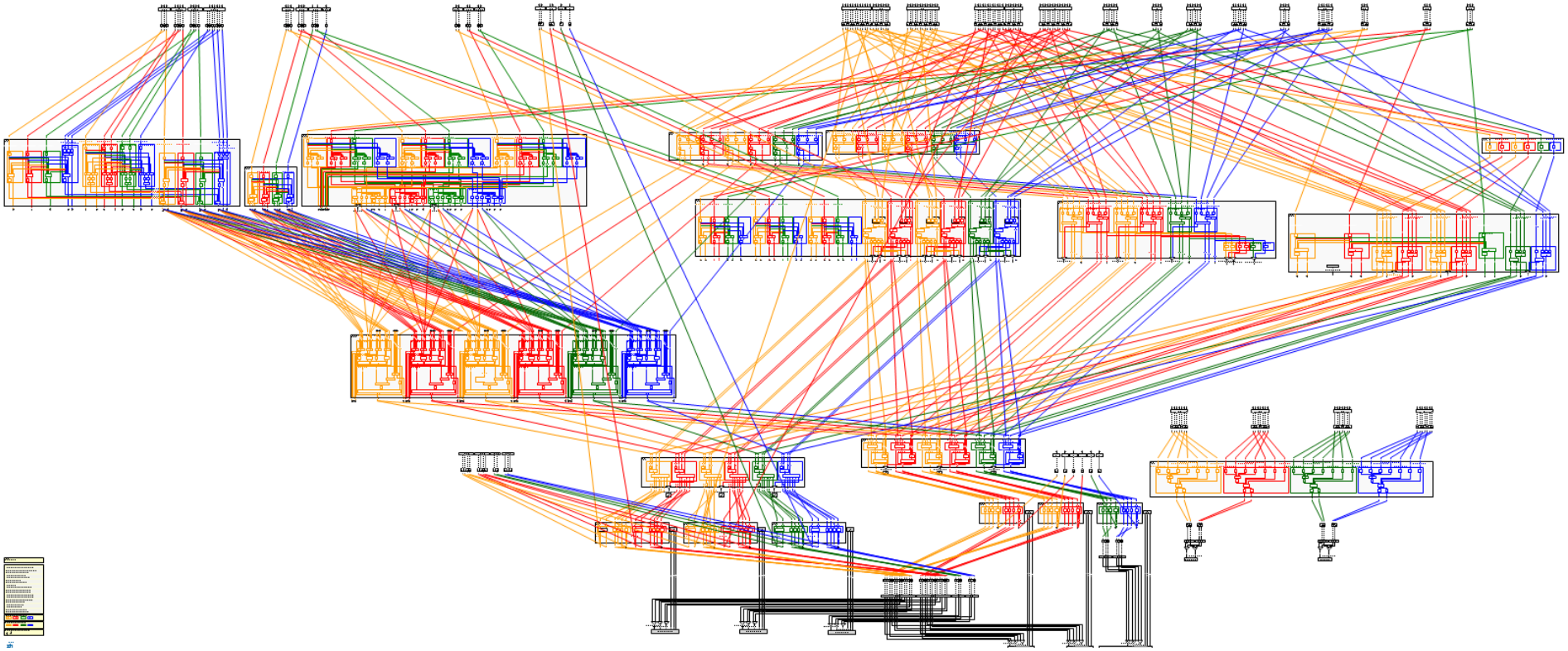
- Project Examples
  - Quantitative Software-Reliability Modeling of digital I&C Systems
    - Nuclear Power Plant Gösgen
  - FPGA based Railway Control Centre Development
    - Super-Computing-Systems Zürich, SBB, DB, ÖBB
  - STPA for Safety Assessment of Complex Medical Systems
    - PSI, MIT
  - Risk Analysis of digital I&C Systems with STPA
    - Swissnuclear
  - Safety-Driven-Design with STPA in the Context of the EU Machinery Directive
    - CurtissWright Drive Technologies

Feedwater Control Example



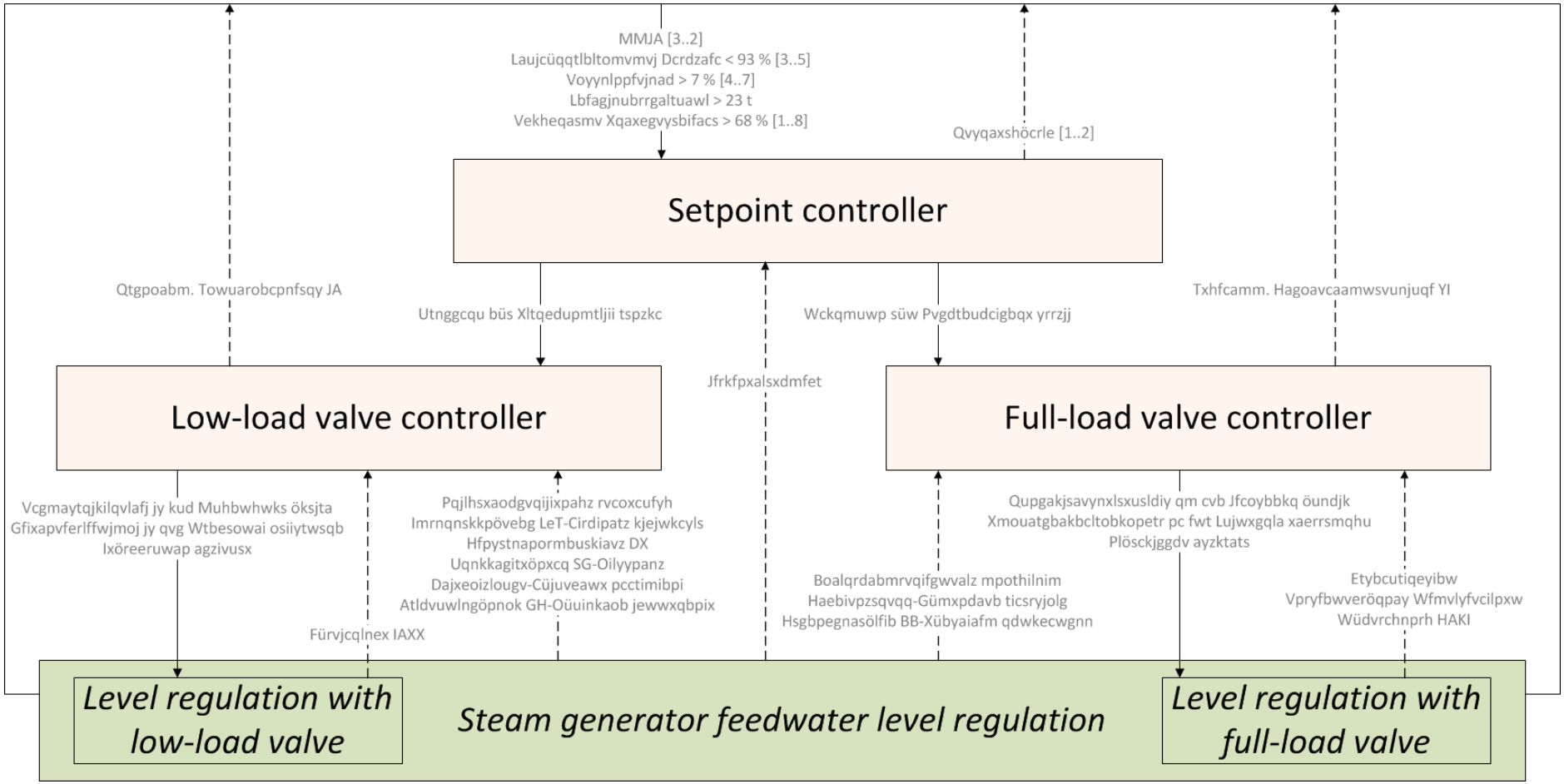
1 Reactor
2 Steam generator
3 Reactor coolant pump
4 Pressuriser
5 High-presure turbine
6 Water separator
7 Superheater
8 Low-pressure turbine
9 Condenser
10 Condensate pump
11 Low-pressure preheater
12 Feedwater tank
13 Feedwater pump
14 High-pressure preheater

Feedwater Control Example – Physical Deployment



Feedwater Control Example - HCS

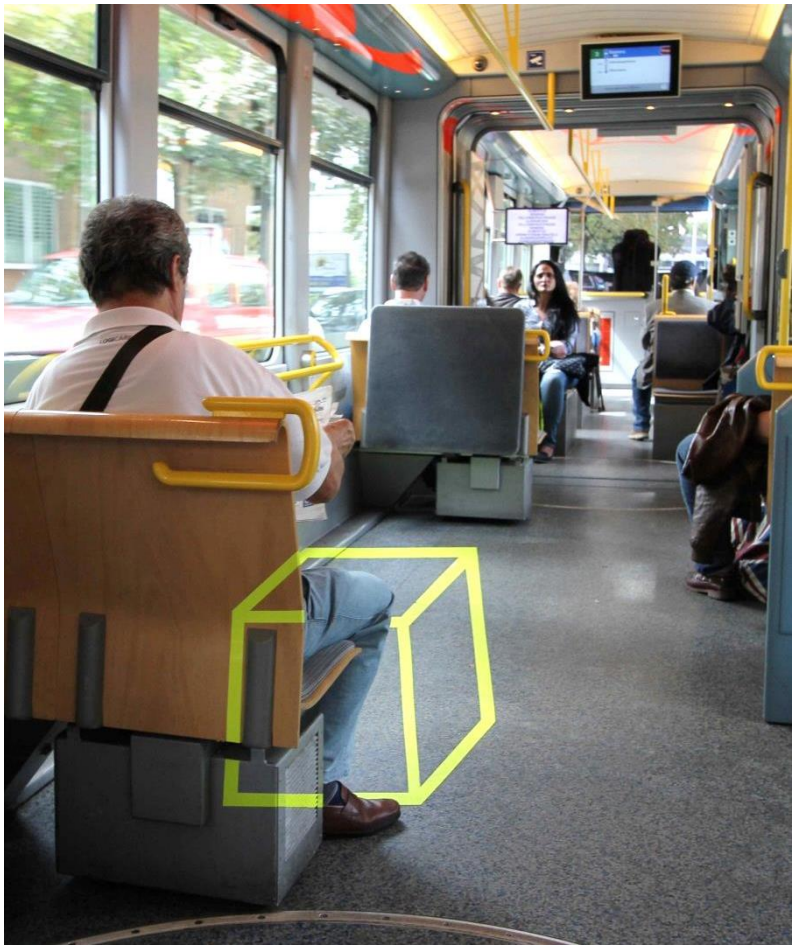
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics



Exemplary illustration

Anamorphosis

Anamorphosis



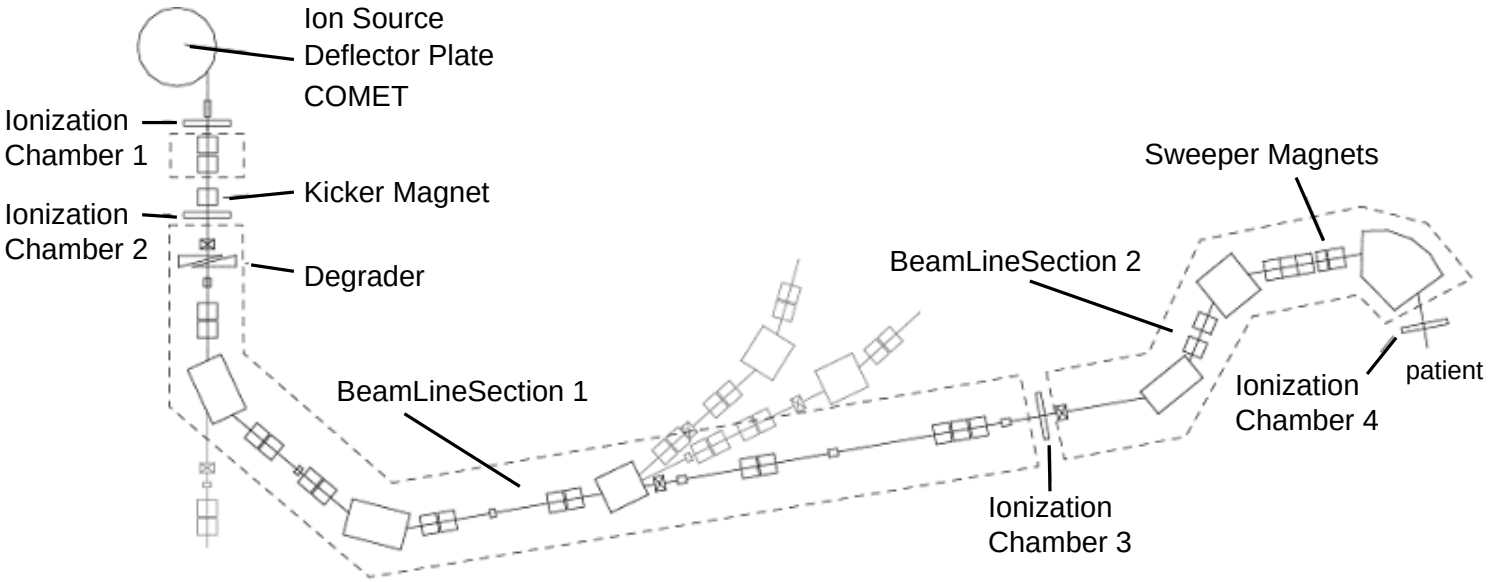
Safety-Critical Systems Research @IAMP

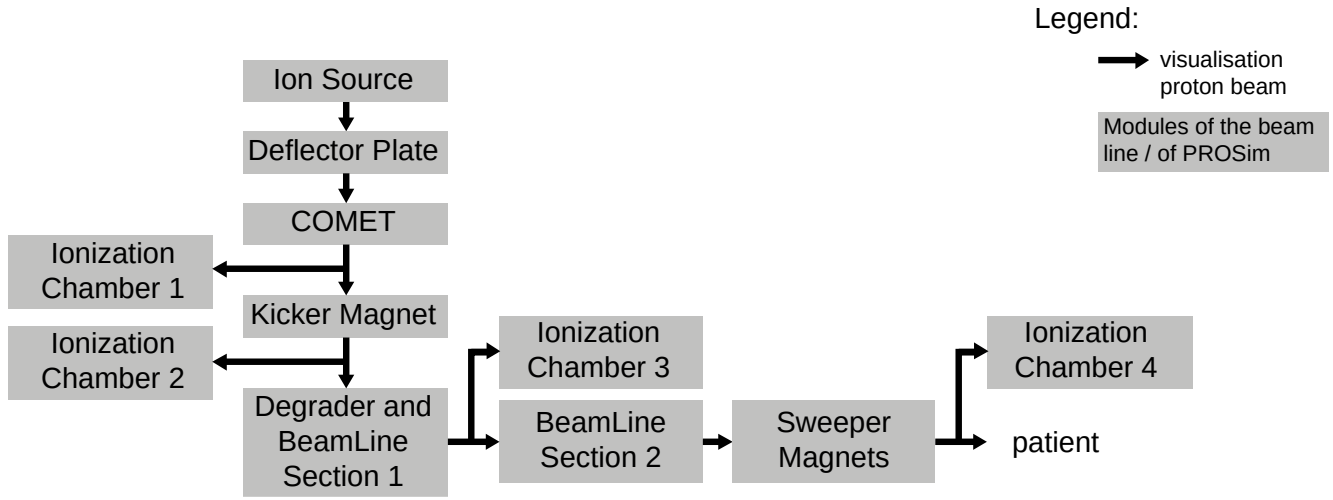
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

- Project Examples
  - Quantitative Software-Reliability Modeling of digital I&C Systems
    - Nuclear Power Plant Gösgen
  - FPGA based Railway Control Centre Development
    - Super-Computing-Systems Zürich, SBB, DB, ÖBB
  - STPA for Safety Assessment of Complex Medical Systems
    - PSI, MIT
  - Risk Analysis of digital I&C Systems with STPA
    - Swissnuclear
  - Safety-Driven-Design with STPA in the Context of the EU Machinery Directive
    - CurtissWright Drive Technologies
- Ongoing Activities
  - Education in Reliability and Safety Engineering at Master Level
  - Integrated Safety Engineering with STPA and UML
  - HIL Functional-Safety Testing Lab

Example Synthetic HIL Environment

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics



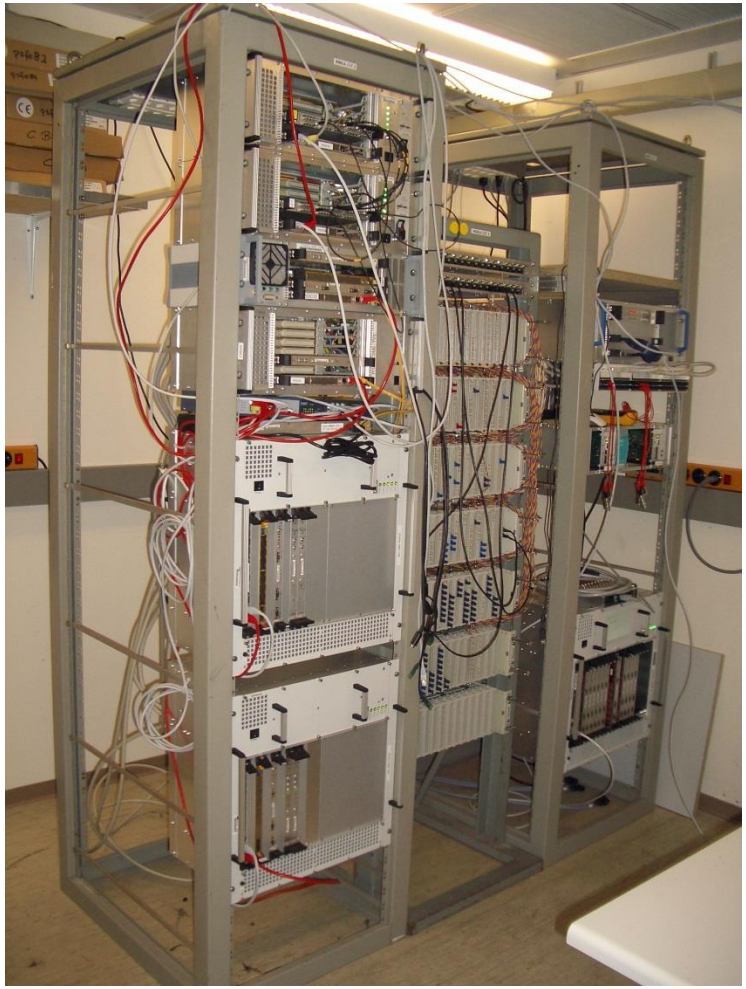


Example Synthetic HIL Environment

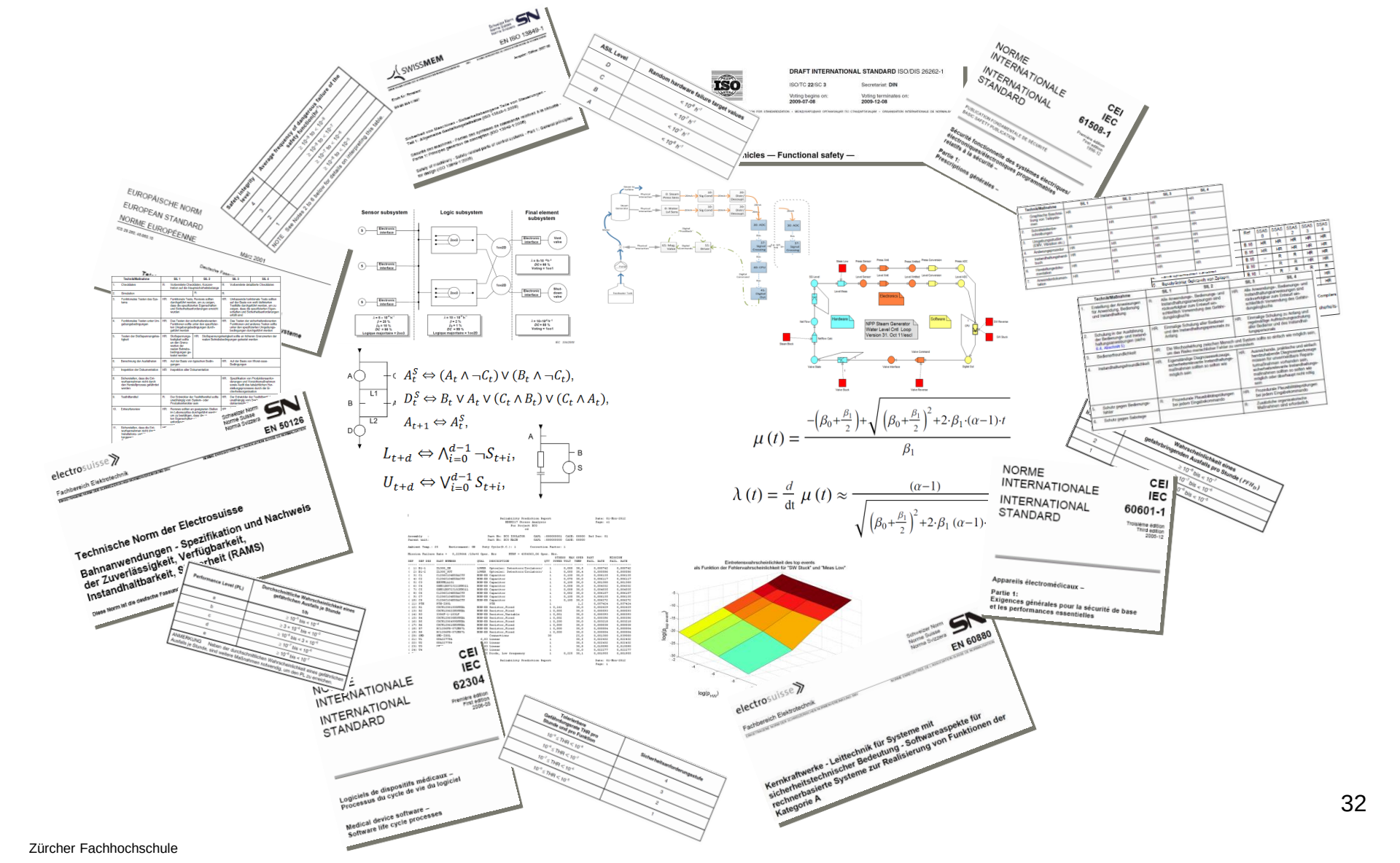
Example: PROSim at PSI

Realtime simulation (1µs cycle time) of actuators, beam current, beam position and sensors of PROSCAN Gantry-2 beamline.

- Simulation implemented on FPGA (PMC Module on VME carrier) in VHDL.
- Interfacing to real control system through custom DA/AD converters and DIO cards directly connected to FPGA.
- Control and configuration of simulation with Motorola MVME6100 PPC running VxWorks implemented in c++
- System behaviour and fault-injection runs settable through scripts and Qt-GUI
- Developed as part of a diploma thesis of two SoE students... Some years ago...



From Principles to Regulatory Context



From Principles to Product

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

From a bachelors thesis to a finished product.

Detection Method, Algorithm and Design @IAMP

Analog Signal Processing Electronics @ZSN

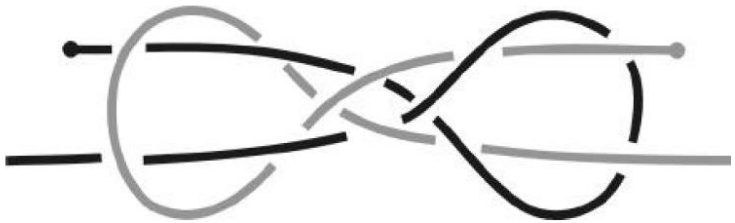
Embedded Computer System @InES

Application Software @InIT

Mechanical Construction @ZPP

To summarize…

- Our competencies for this collaboration
  - Accelerator based research facility experience.
  - Systems Engineering and RAMS methods, established and “beyond”.
  - The principles of functional safety as well as the standards and their application to complex and large systems.
    - From process to design and to implementation of hard- and software.
  - Experience working with people from research, industry and regulatory bodies.
  - Strong network at SoE.




CFA Productions, TV
303-555-6140