Zurich University
of Applied Sciences

School of
Engineering

IAMP Institute of Applied
Mathematics and Physics

Use of STPA in digital instrumentation and control systems of nuclear power plants

Martin Rejzek

Second European STAMP Workshop
22.09.2013 Stuttgart, Germany

Agenda

- Project background and objectives
- System under consideration
- Analysis approach
  - Process towards the hierarchical control structure
  - STPA step 1 and 2
  - Blended approach
- Conclusion and outlook

Project Background

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

- Replacement of existing instrumentation and control system (I&C system)
- Simultaneous transition from analog to digital system

How can STPA be efficiently applied to an I&C system as it is used in nuclear power plants?

Project Objectives

- Develop process to «transform» an I&C system specification into a hierarchical control structure
- Investigate potential of STPA (with respect to nuclear power plant I&C systems) by performing a case study
- Investigate potential to integrate existing analyses (FTA, ETA, FMEA, ...) into STPA (blended approach)

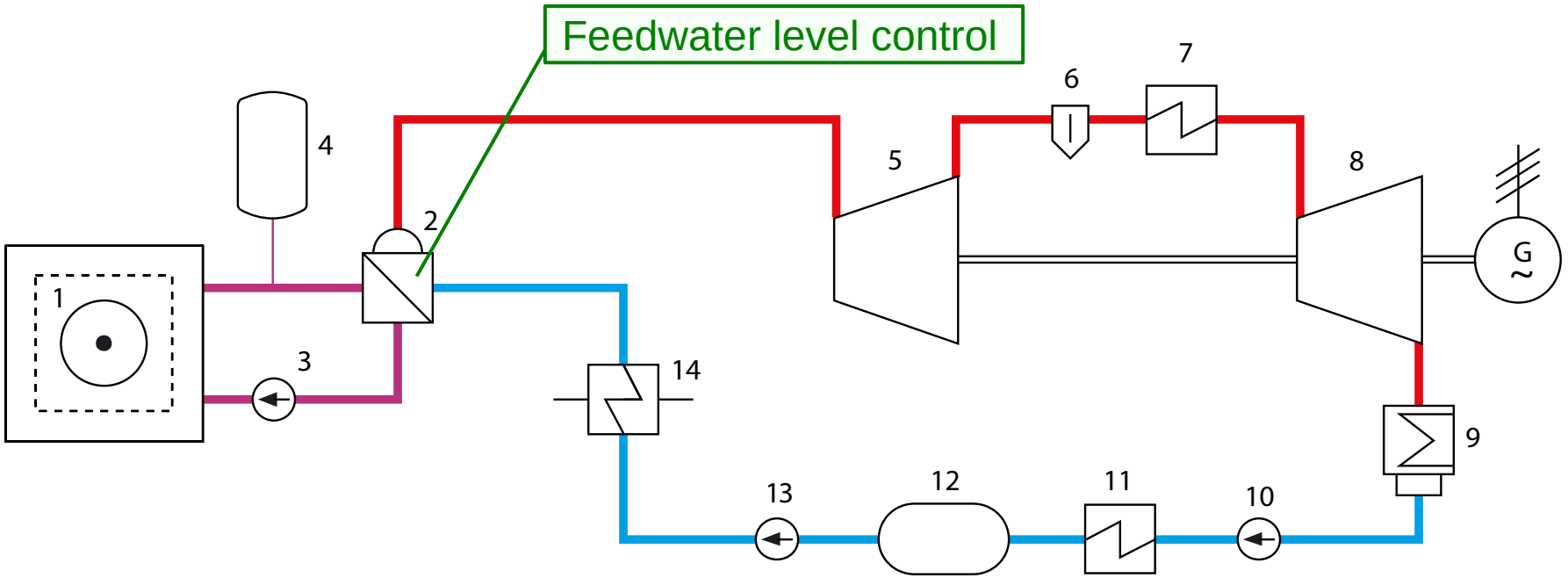
→ Detailed documentation

→ Case study

→ Knowledge transfer

System Under Consideration - Selection of the Case Study

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



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

Exemplary illustration

System Under Consideration – Information Sources Used

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

Information sources used:

- Facility documentation
- System specifications (level 3 & 4 documents)
- Manuals
- Expert knowledge

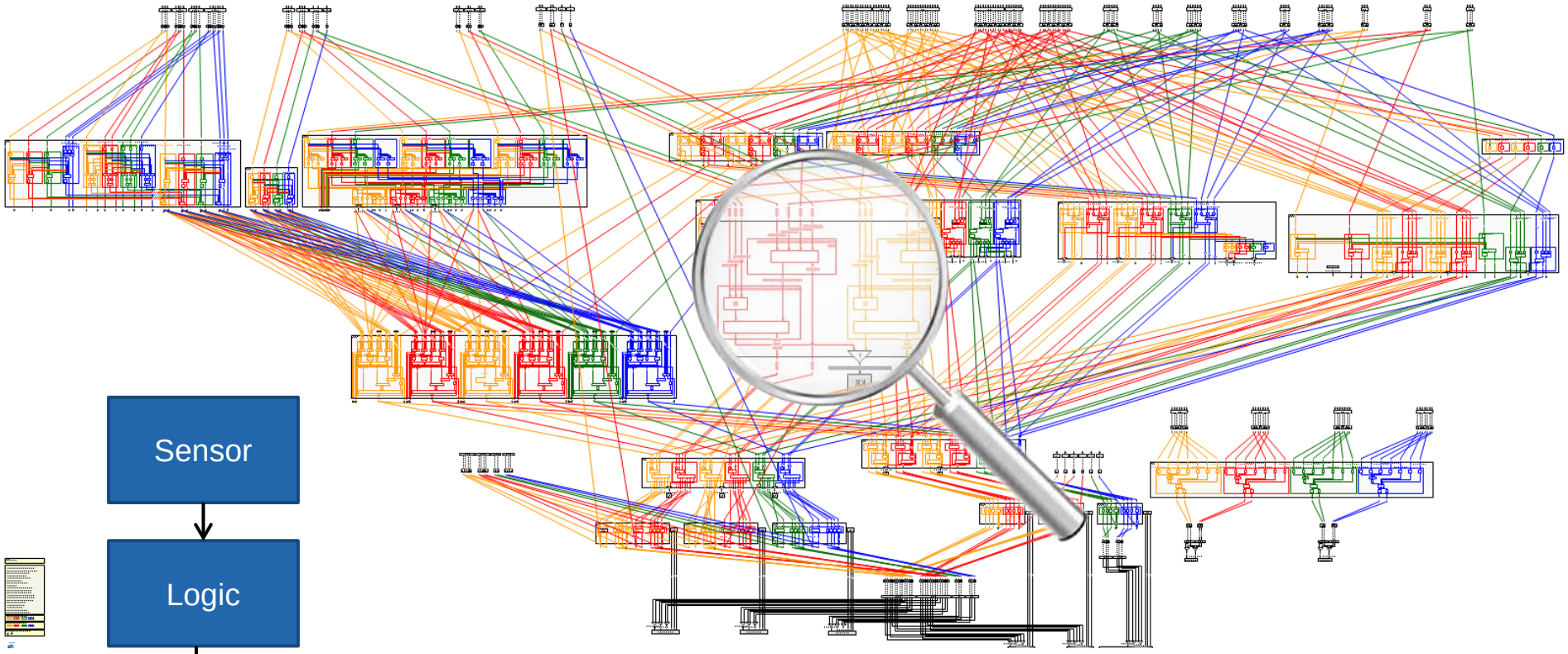
Case Study - System Architecture

A generic way to represent a control function:

Source: IEC 61508 «Functional safety of electrical/electronic/programmable electronic safety-related

Case Study - System Architecture

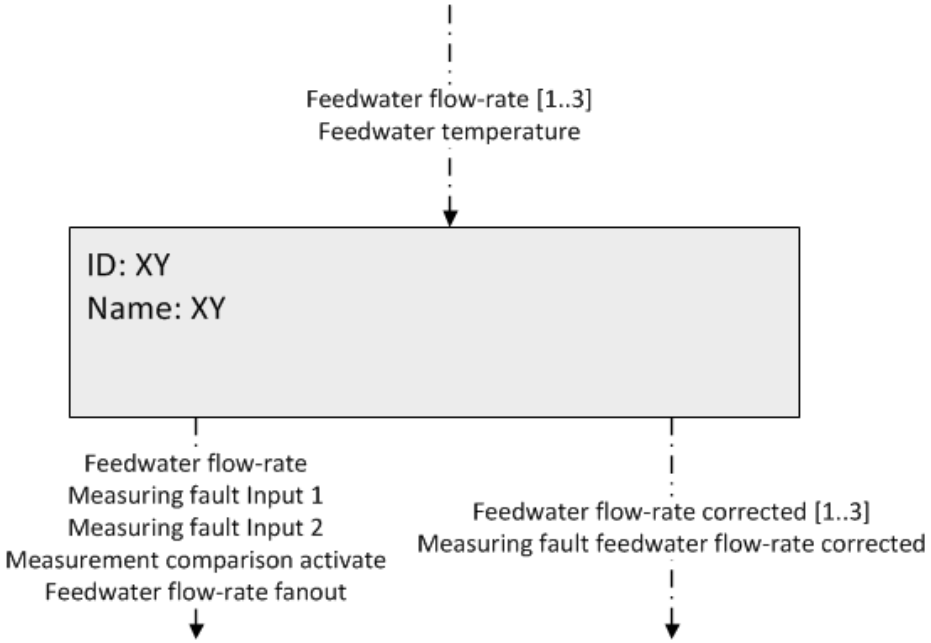
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics



Not what you want to start with!

Problem of Terminology - Functional Entities

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

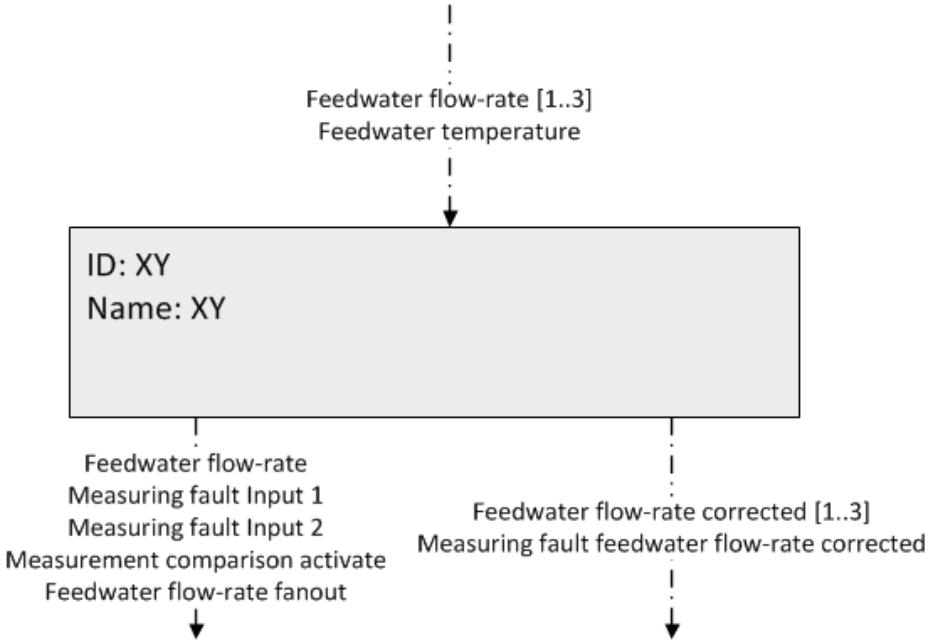


Is this a

- function,
- module,
- sub-system,
- class,
- component, …?

Identification of Controllers - What is a controller in the sense of STPA

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



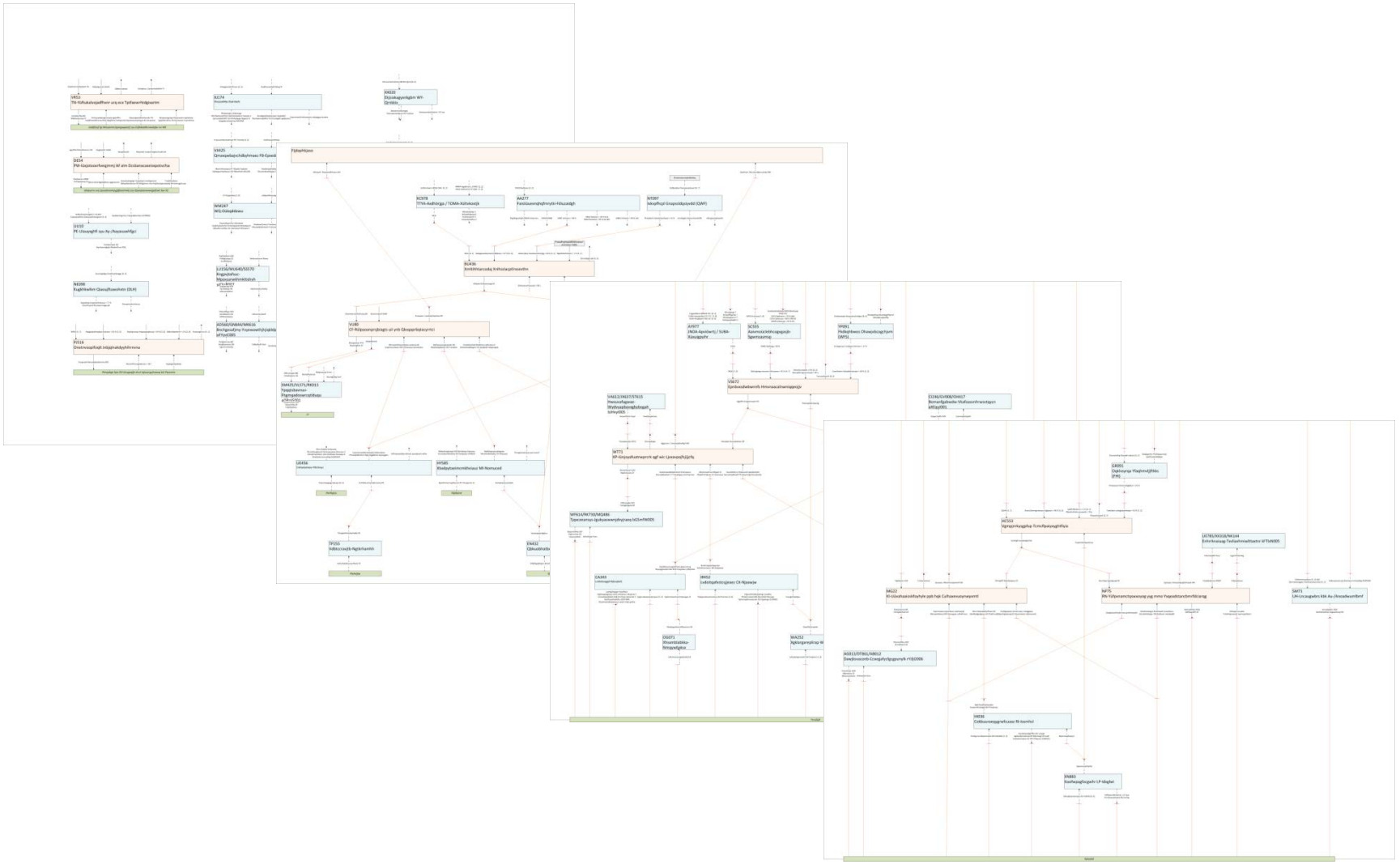
«Controller»?

Does functional entity …

- bear responsibility for a part of the process?
- possess necessary means to interact with process?
- receive necessary feedback for adequate control?

Recombination of Functional Entities - First Step towards the HCS

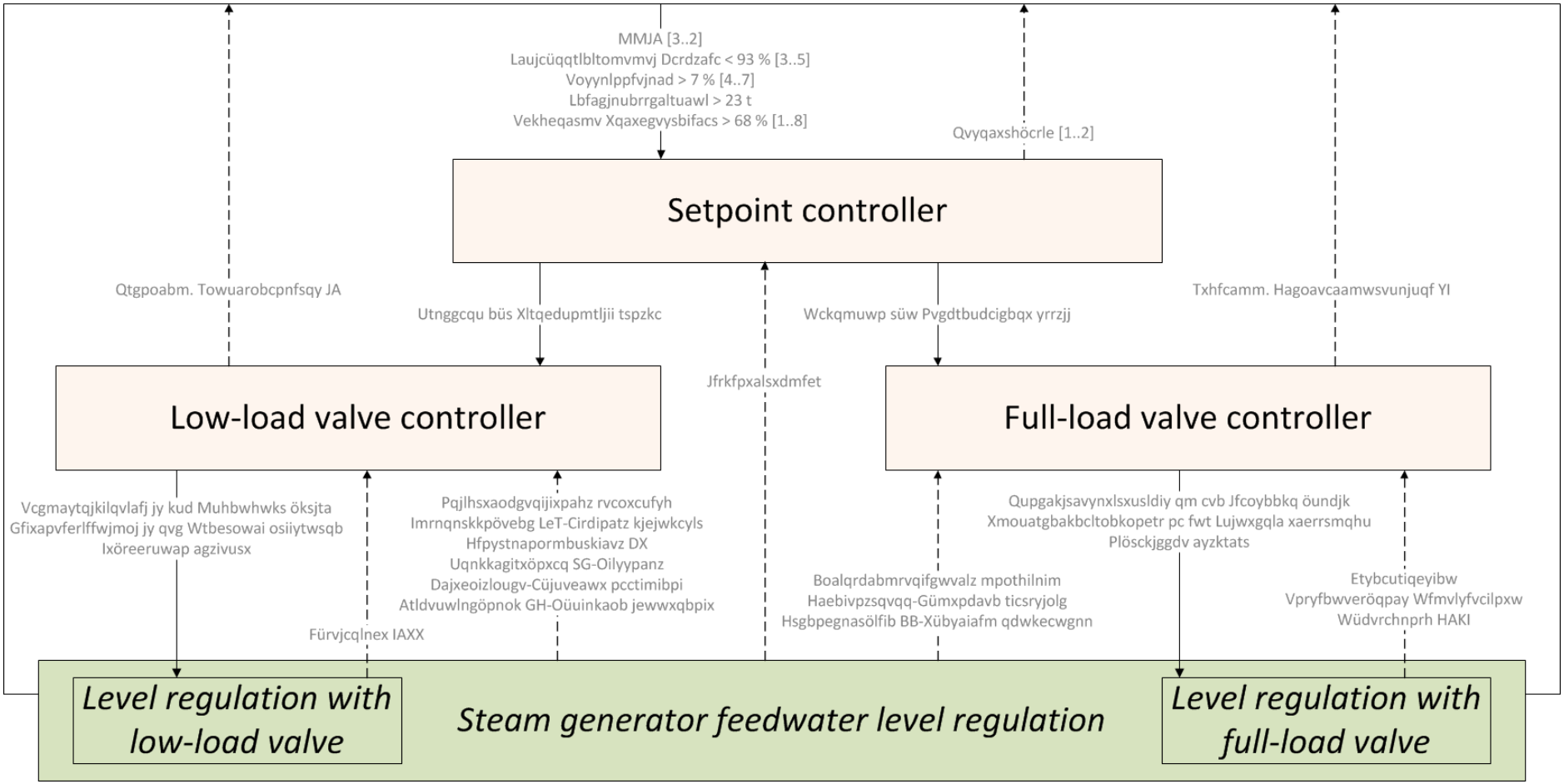
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics



Exemplary illustration

Hierarchical Control Structure

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



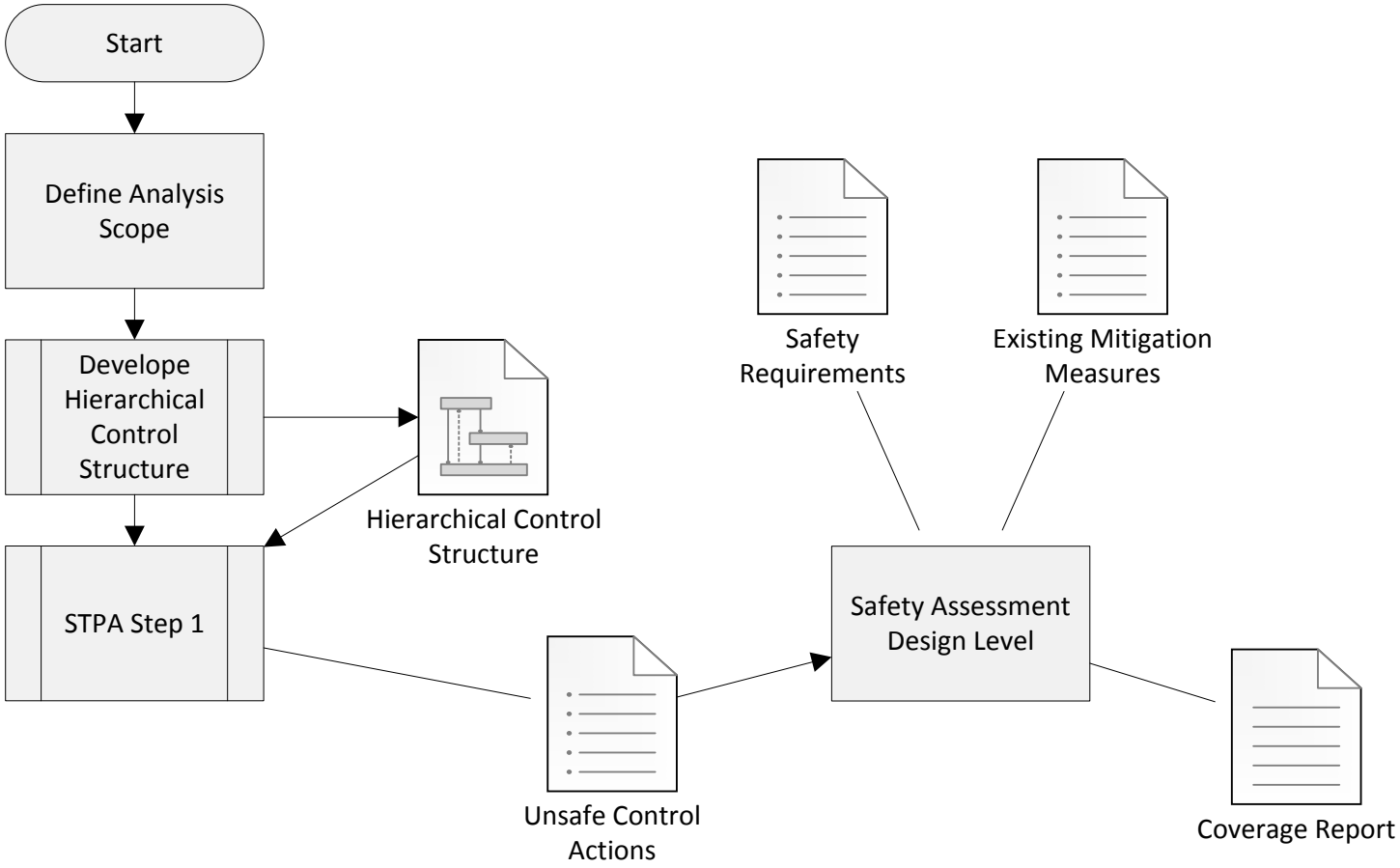
Exemplary illustration

Project Objectives - A First Conclusion

- ✓ Develop process to «transform» an I&C system specification into a hierarchical control structure
  - Systematic and reproducible process
  - Could be partially automated
  - Basis: System Specification with additions
- Investigate potential of STPA by performing a case study
- Investigate potential to integrate existing analyses (FTA, ETA, FMEA, ...) into STPA (blended approach)

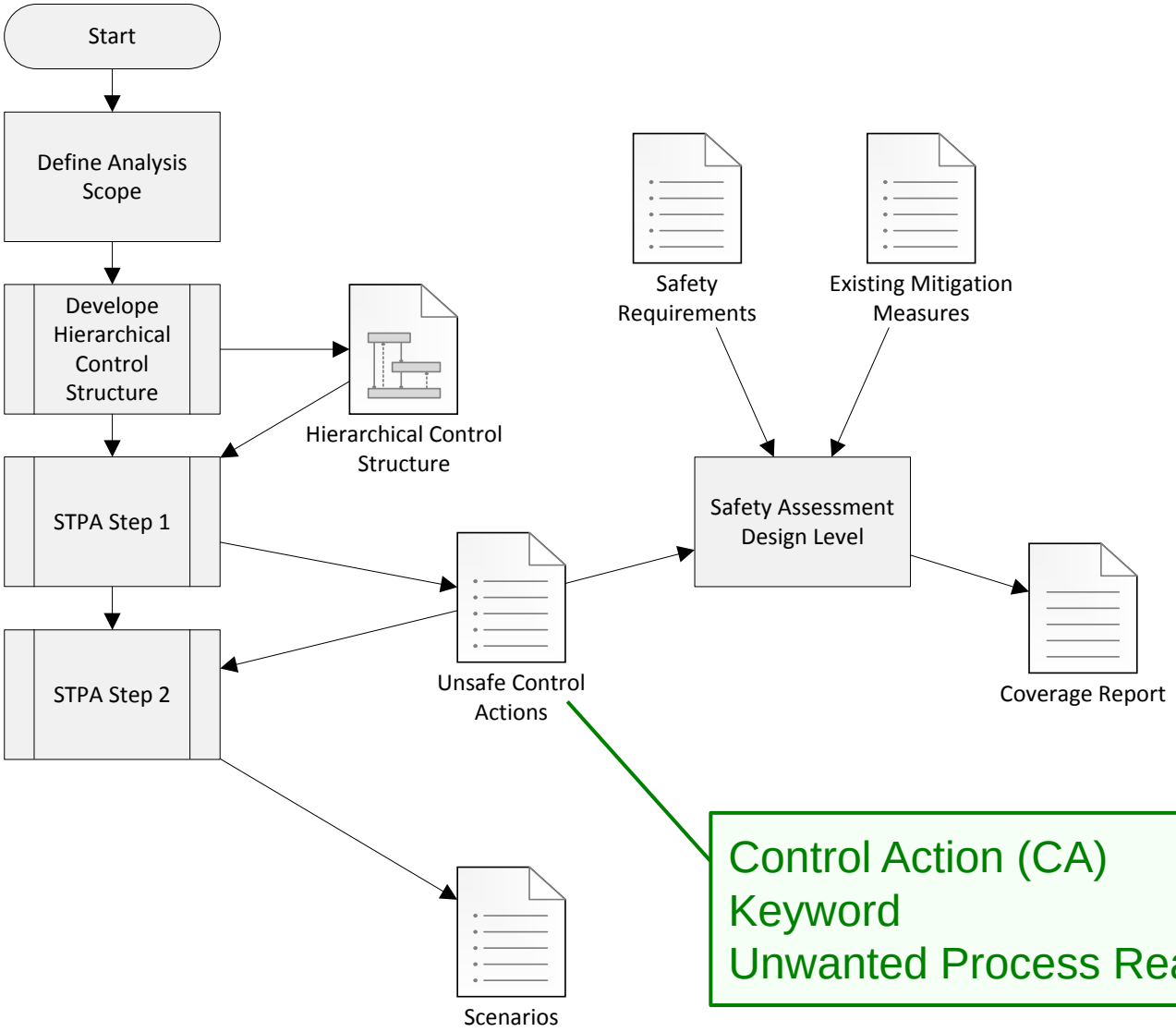
STPA Process - Step 1

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



STPA Process - Step 2

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

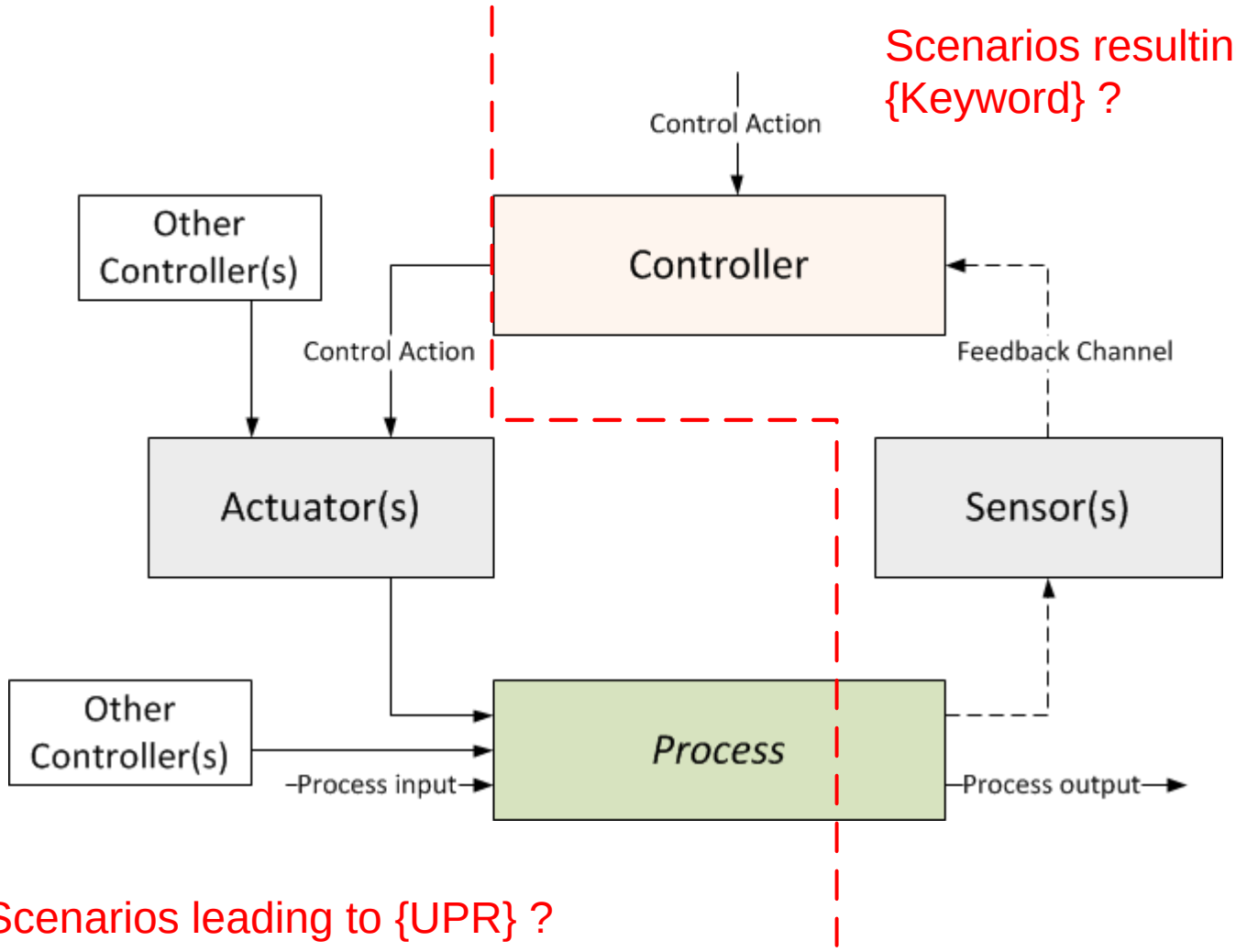


Control Action (CA)
Keyword
Unwanted Process Reaction (UPR)

STPA Step 2 - Generic Control Loop

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

Scenarios resulting in {CA} {Keyword} ?

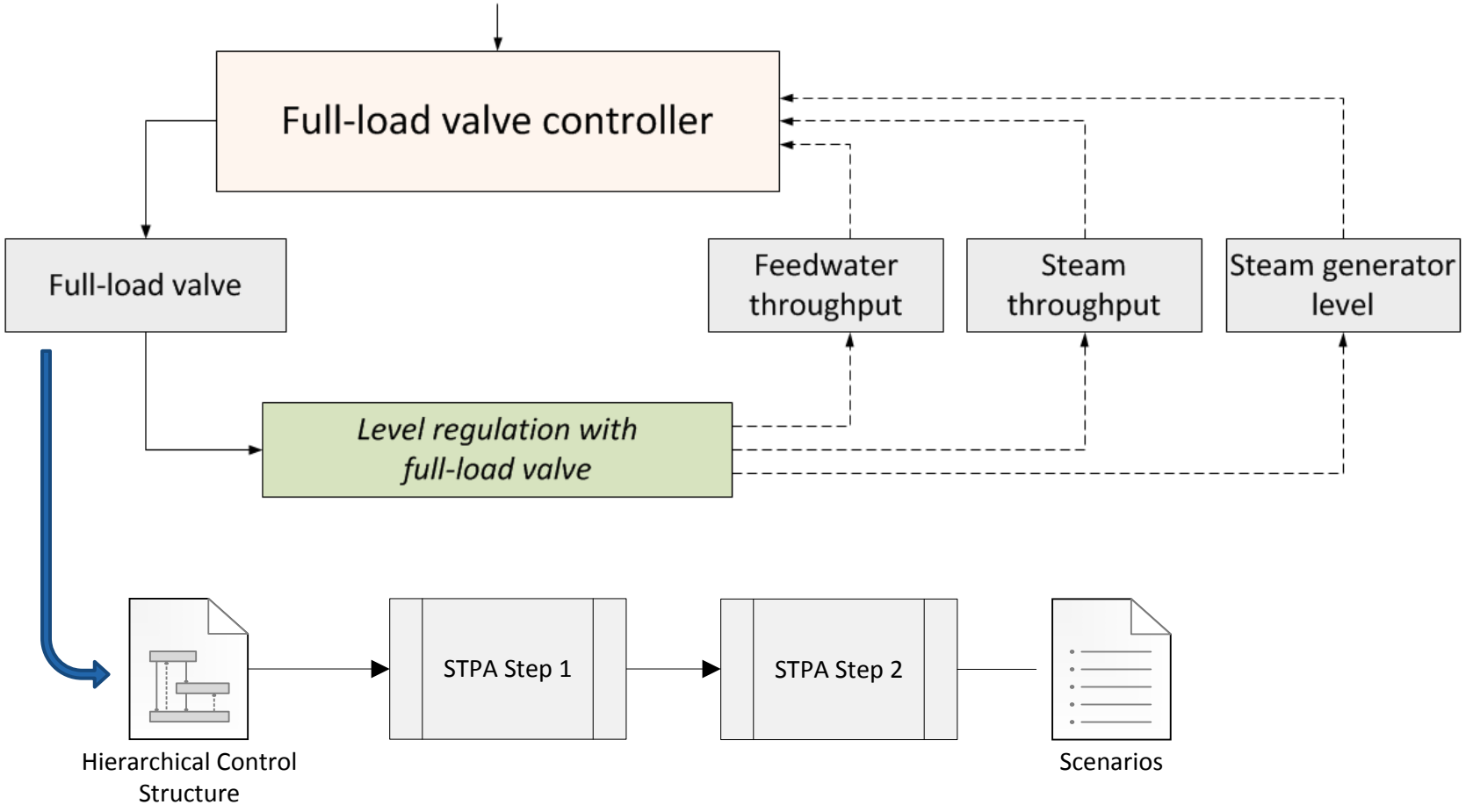


Scenarios leading to {UPR} ?

STPA Step 2 - Control Loop Example

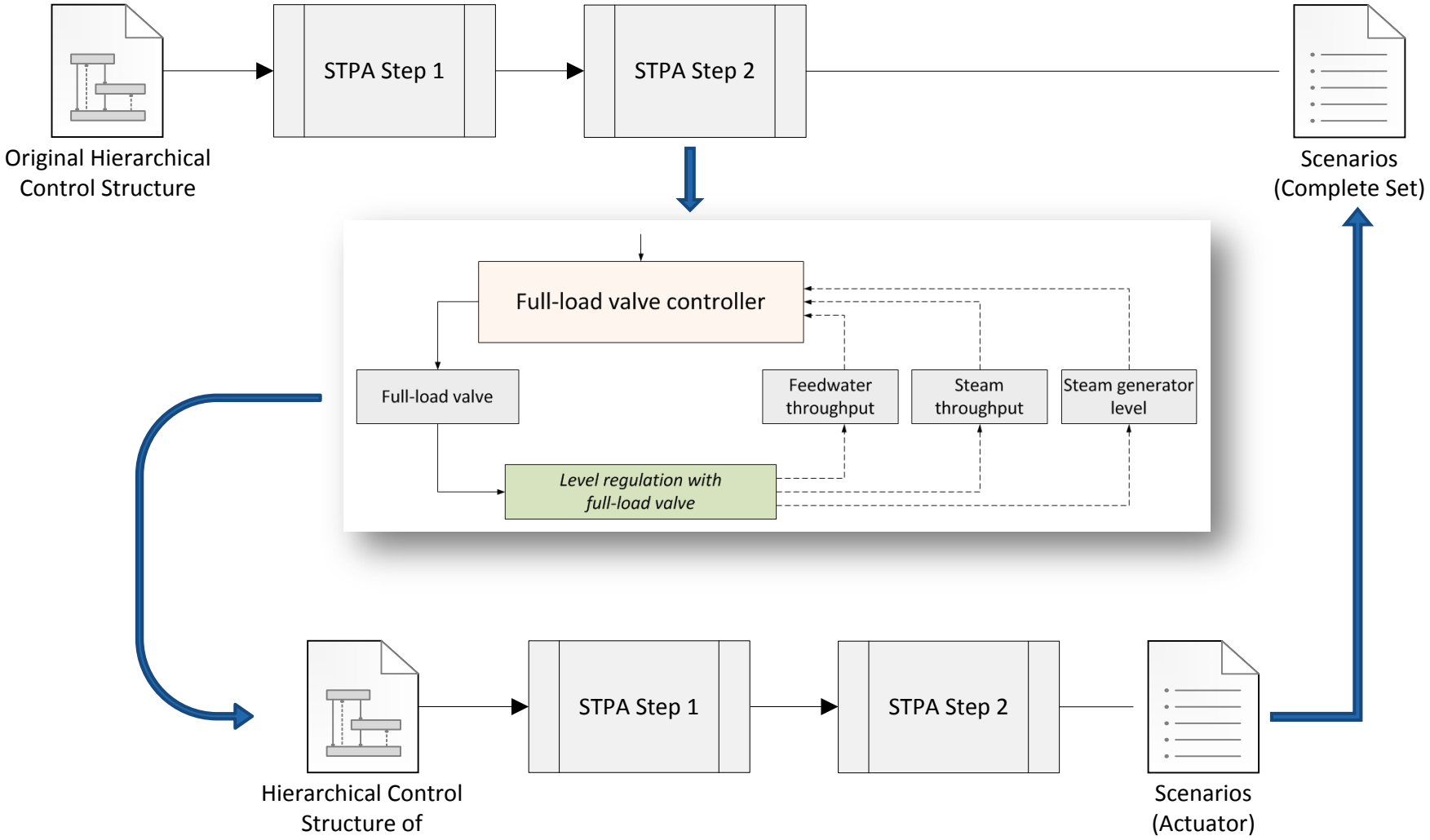
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

UCA: Command to open full-load valve by one increment is not given



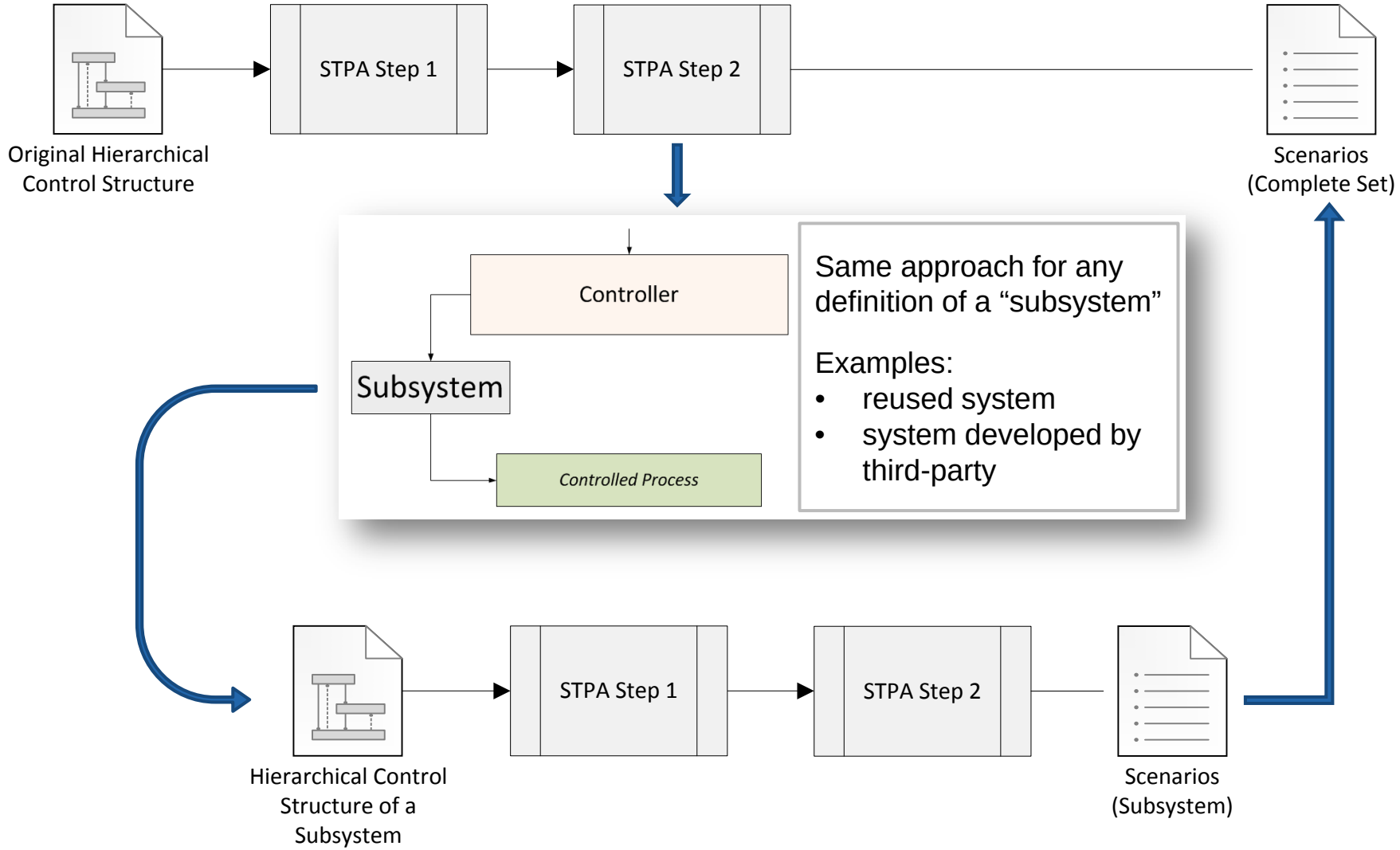
Bridge between STPA Step 2 and Step 1 - Analyzing Subsystems

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



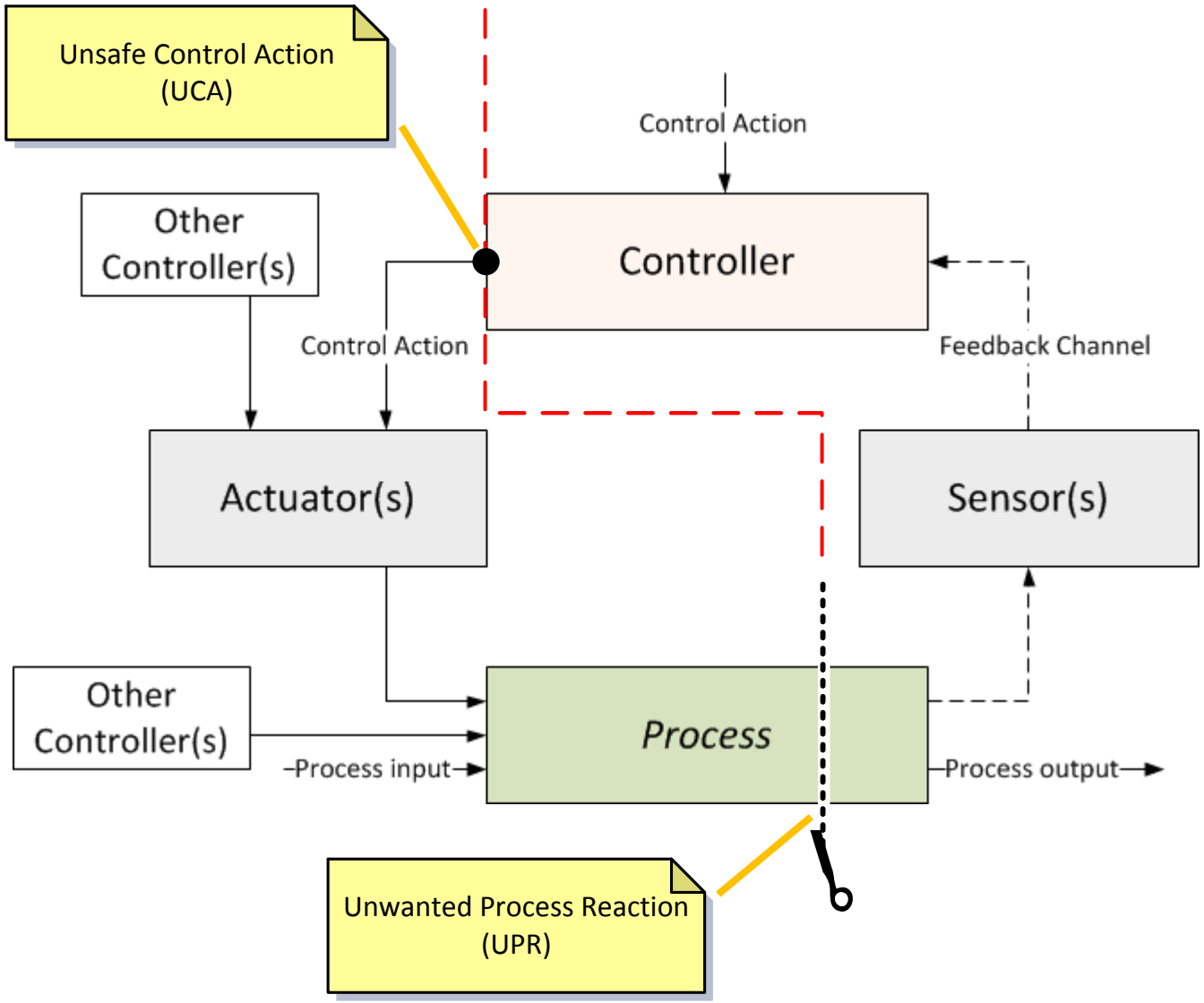
Bridge between STPA Step 2 and Step 1 - Analyzing Subsystems

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



STPA Step 2 - Generic Control Loop

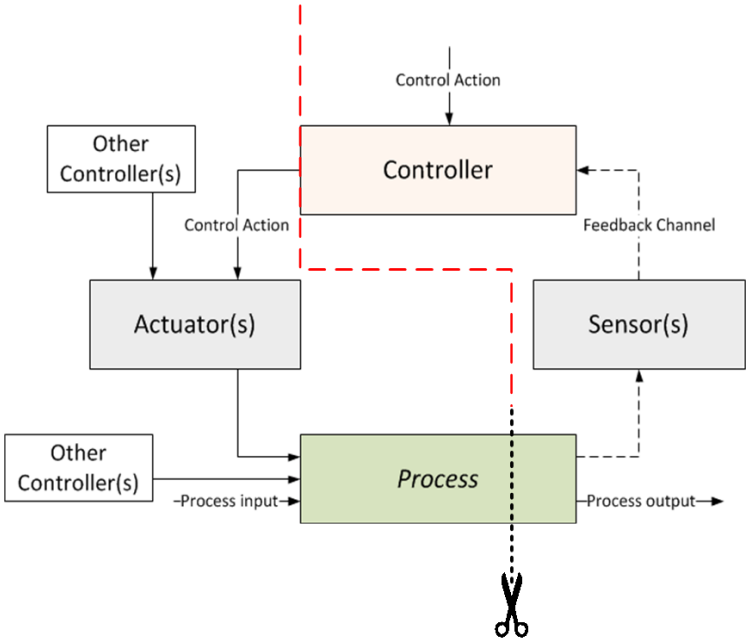
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

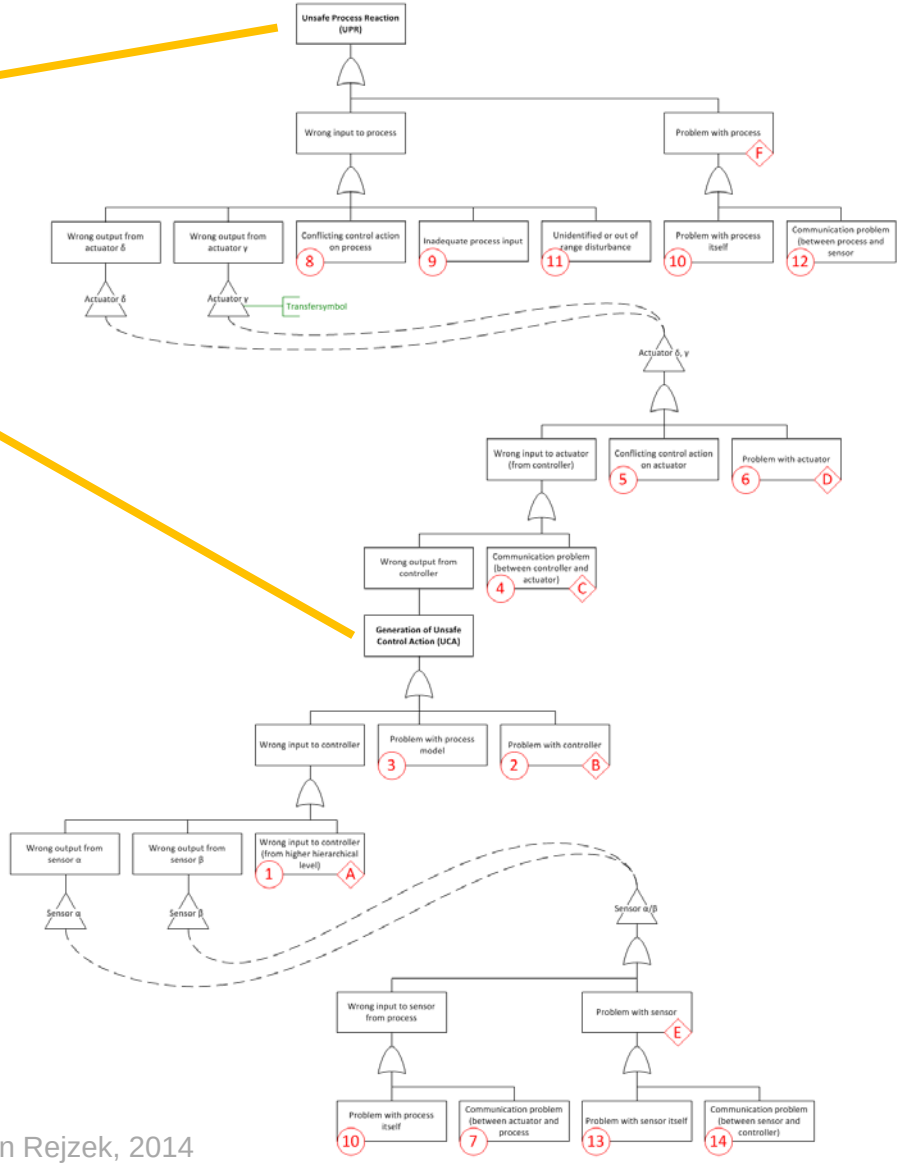


STPA Step 2 - Scenario Organization

Unwanted Process Reaction (UPR)

Unsafe Control Action (UCA)





Conclusion

- Process to «transform» an I&C system specification into a hierarchical control structure
  - Found a systematic and reproducible process
  - Generation of HCS could be partially automated
  - Based on system specification with (little) additions
- Formalization of the STPA step 2 questions:
  - «Scenarios resulting in {CA} {Keyword}»
  - «Scenarios leading to {UPR}»
- Explicit process to handle «subsystems»
  - Prioritization possible at each level
  - Organization of the scenarios in a generic fault tree
  - Link to results from other hazard analyses (FTA, ETA, …)

Current Activities

- Advance the case study
  - Complete STPA step 1 for all control actions
  - Continue with STPA step 2 for selected UCA's
- Advance investigation of "blended-approach"
  - With respect to systems and subsystems
  - With respect to different analysis methods

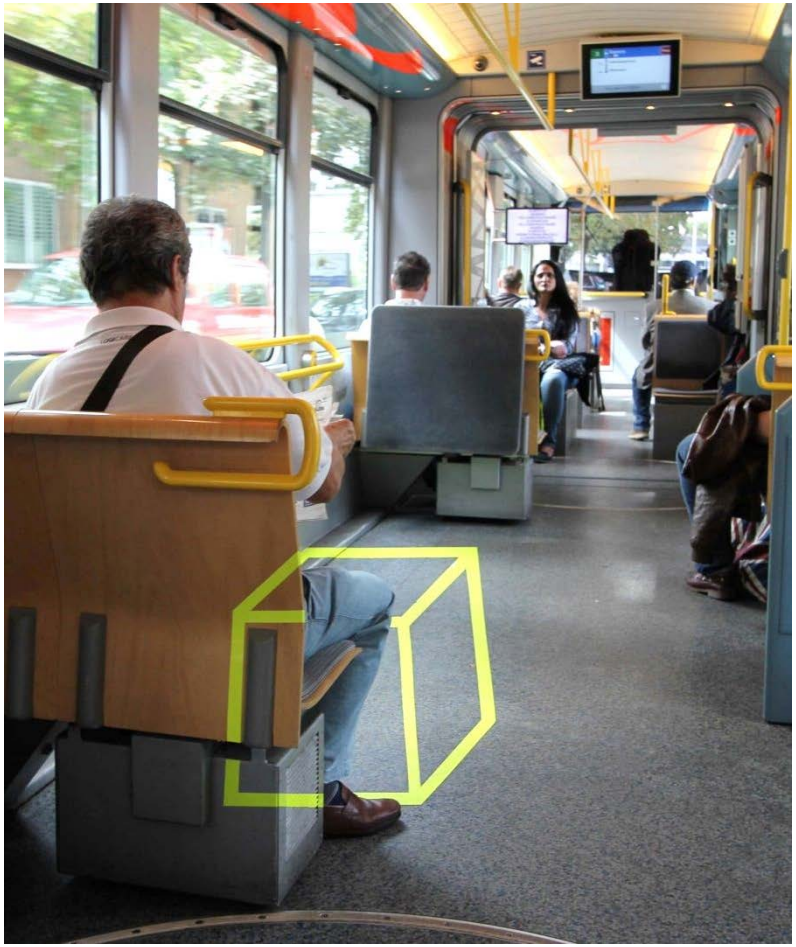
Anamorphosis

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

Certain things can only be seen
from a different standpoint!

Anamorphosis

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



Contact:

Dipl. el. Ing. FH Martin Rejzek
E-mail: martin.rejzek@zhaw.ch
http://www.iamp.zhaw.ch/sks