Zurich University
of Applied Sciences

School of
Engineering
IAMP Institute of Applied
Mathematics and Physics

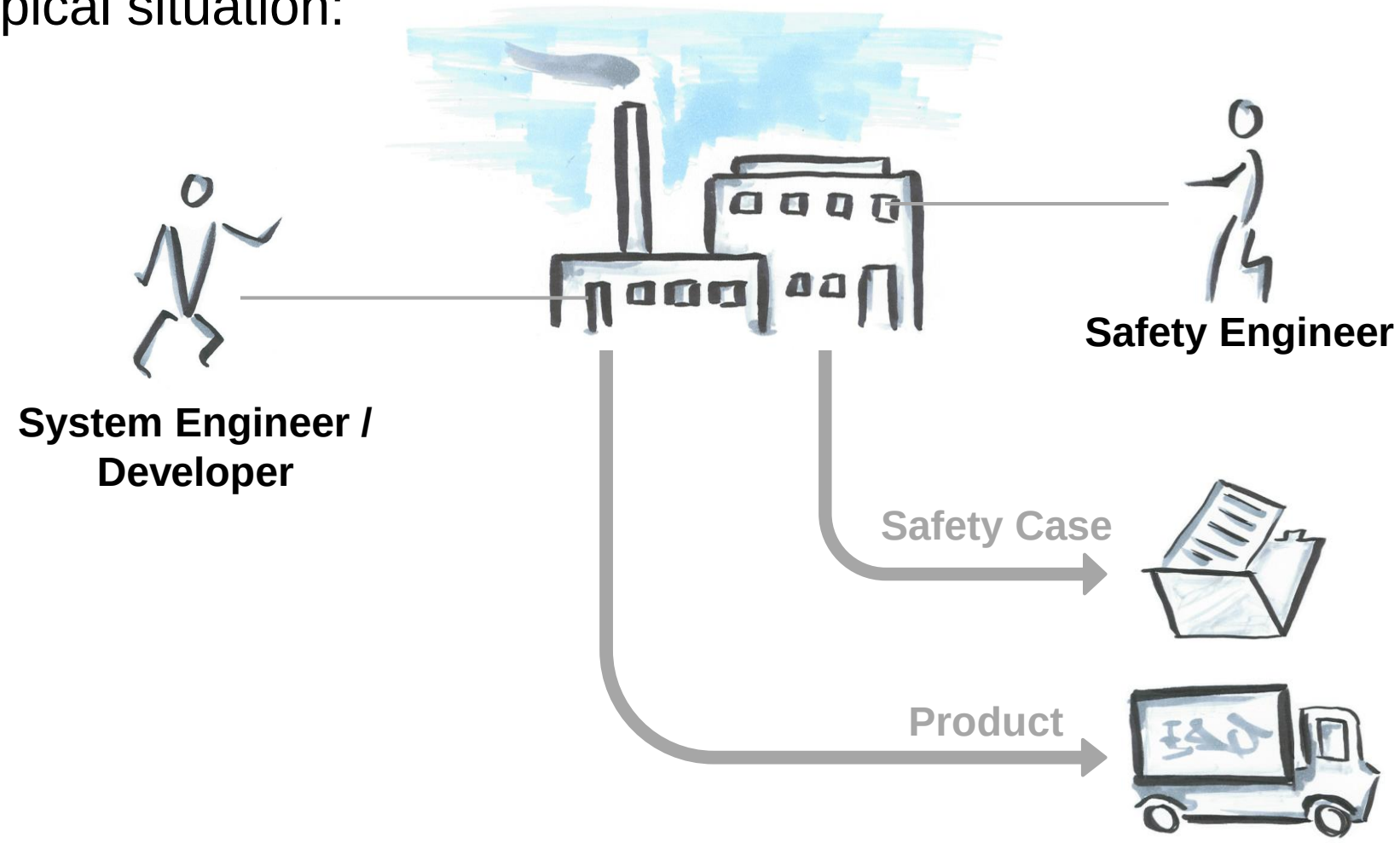
Safety Driven Design with UML and STPA

Martin Rejzek, Sven Krauss, Christian Hilbes

Zurich University of Applied Sciences, Switzerland

System and Safety Engineering

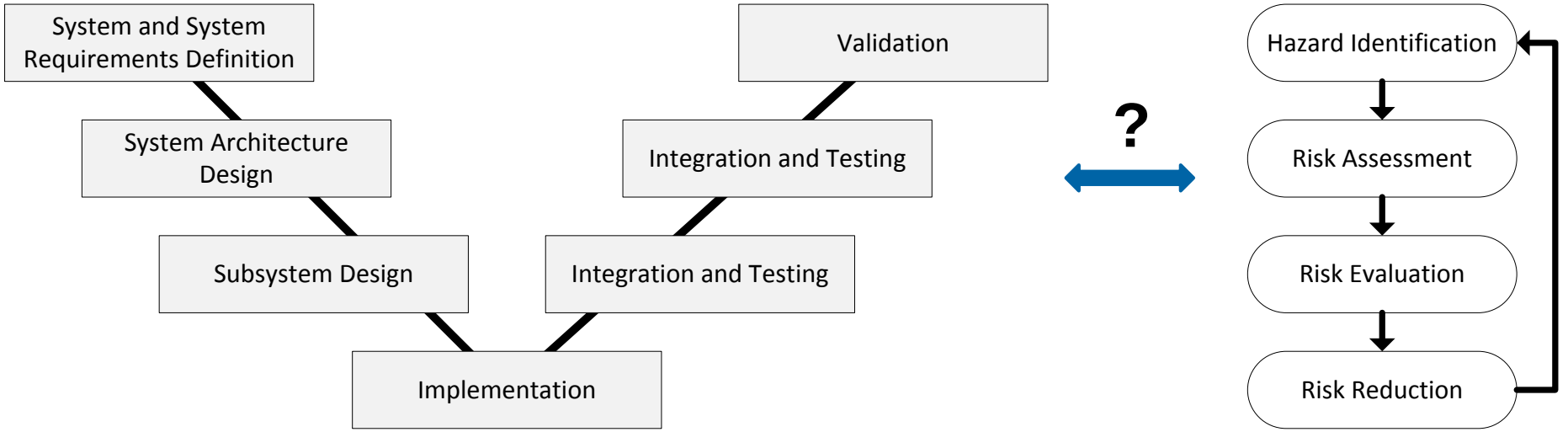
A typical situation:



System and Safety Engineering

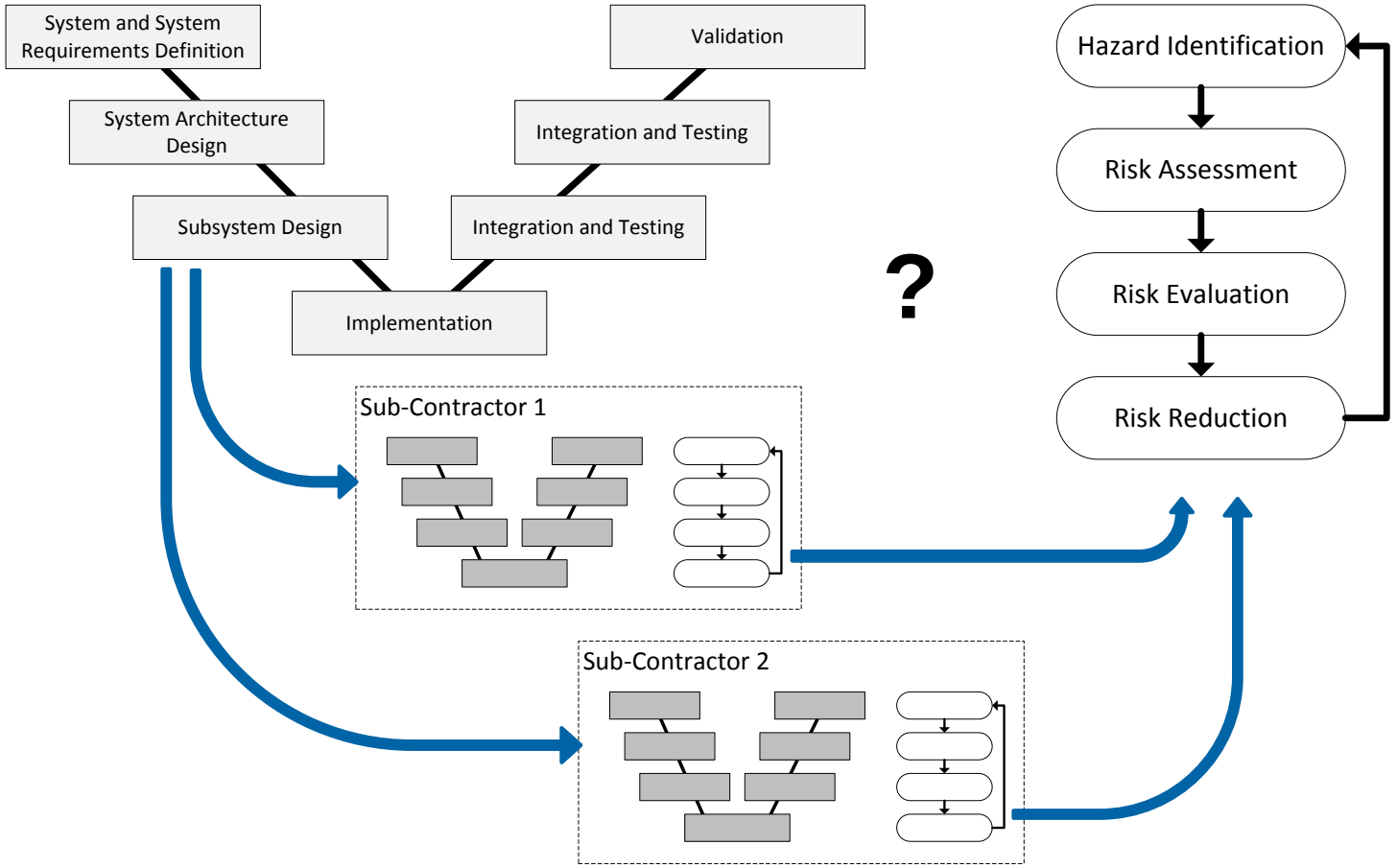
The challenges with this situation:

- Product development and safety management separated
- Different teams, methods, terminology
- Different processes and mindset



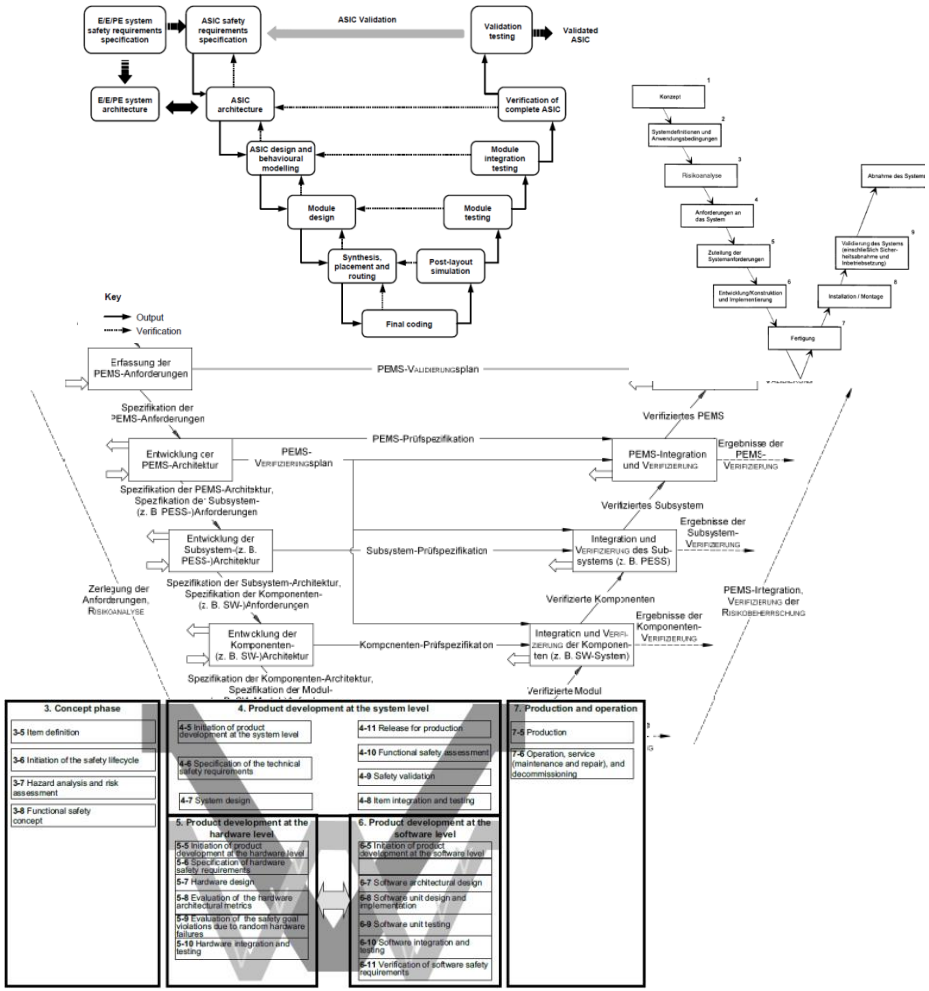
System and Safety Engineering

The challenge is even more severe for complex systems involving sub-contractors:

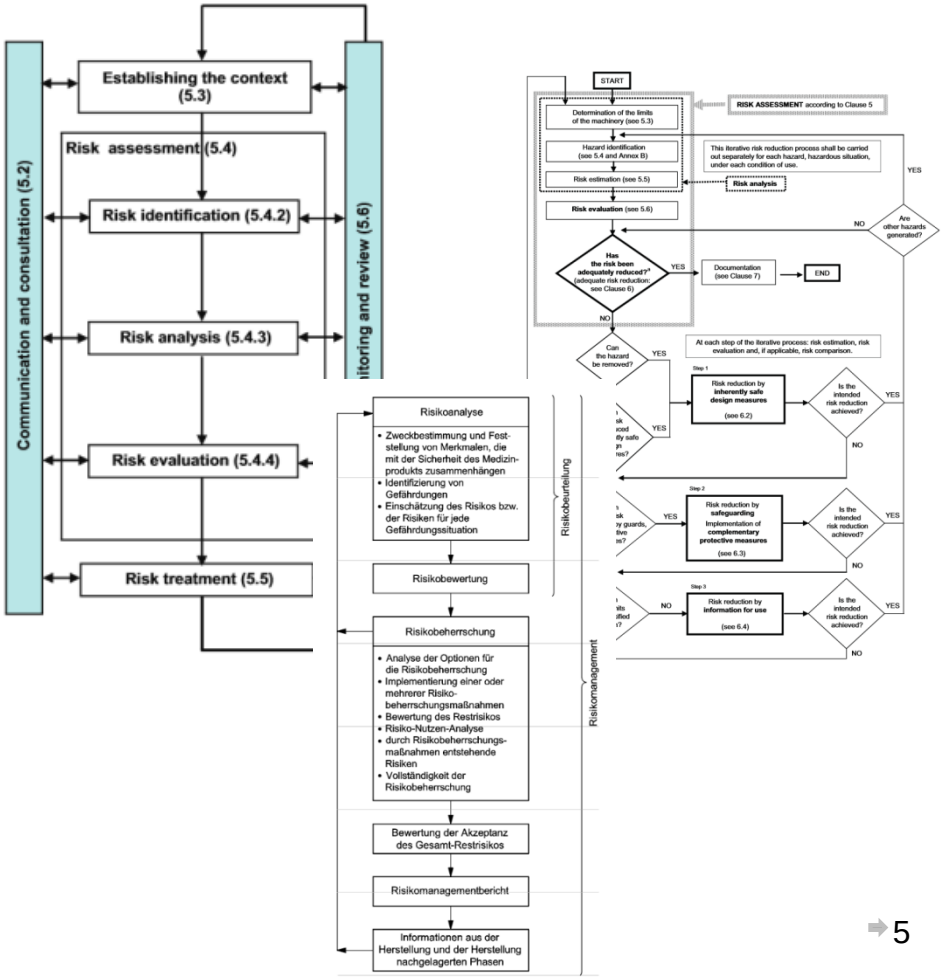


Processes

V-Model Zoo:

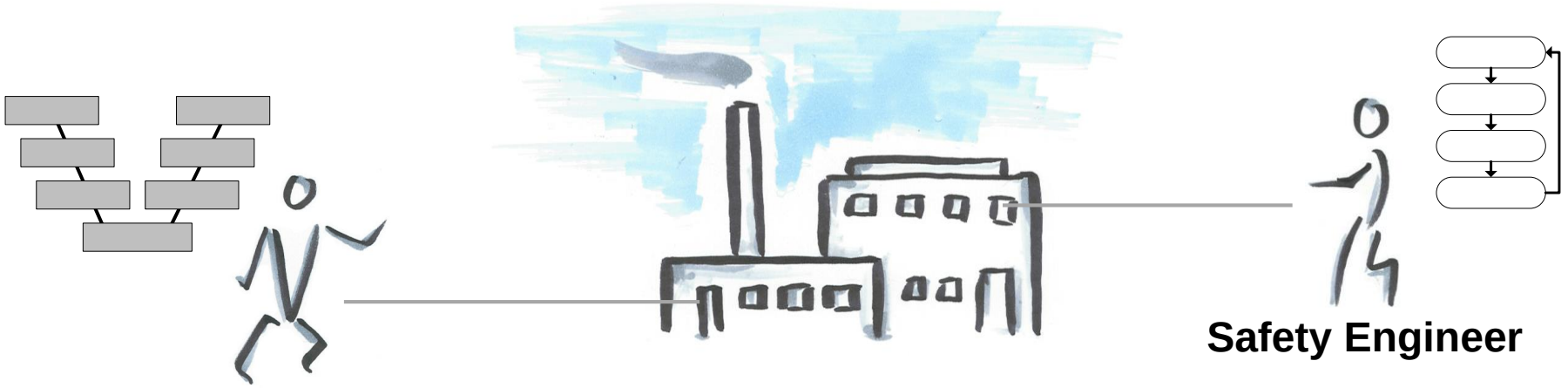


Risk Management Processes:



System and Safety Engineering

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



System Engineer / Developer

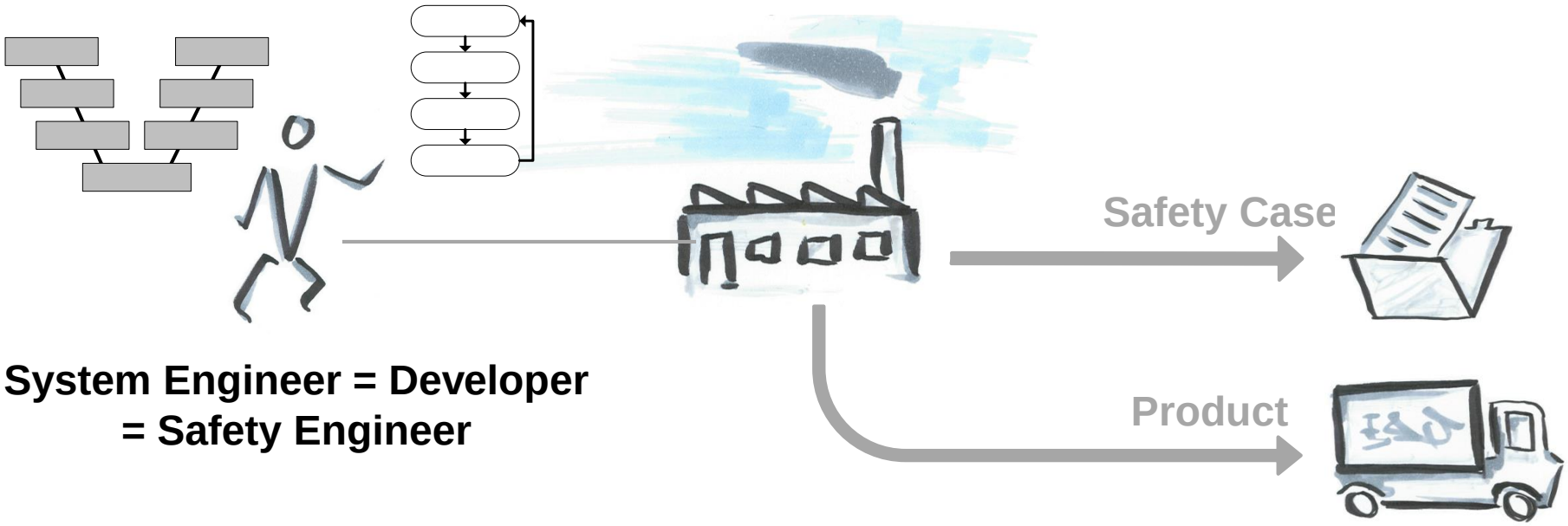
- Model based development with UML
- UML Case Tools
- Automated Code Generation

Safety Engineer

- FTA, FMEA, HAZOP, …
- Dedicated Tools

System and Safety Engineering

A typical situation in smaller companies:



System Engineer = Developer
= Safety Engineer

Developer wants to do a good job but has no chance to cope with “everything” …

Solution: Empower developer to incorporate the safety aspects right into system development

State of the Art in Systems Engineering: Model Based Development with UML

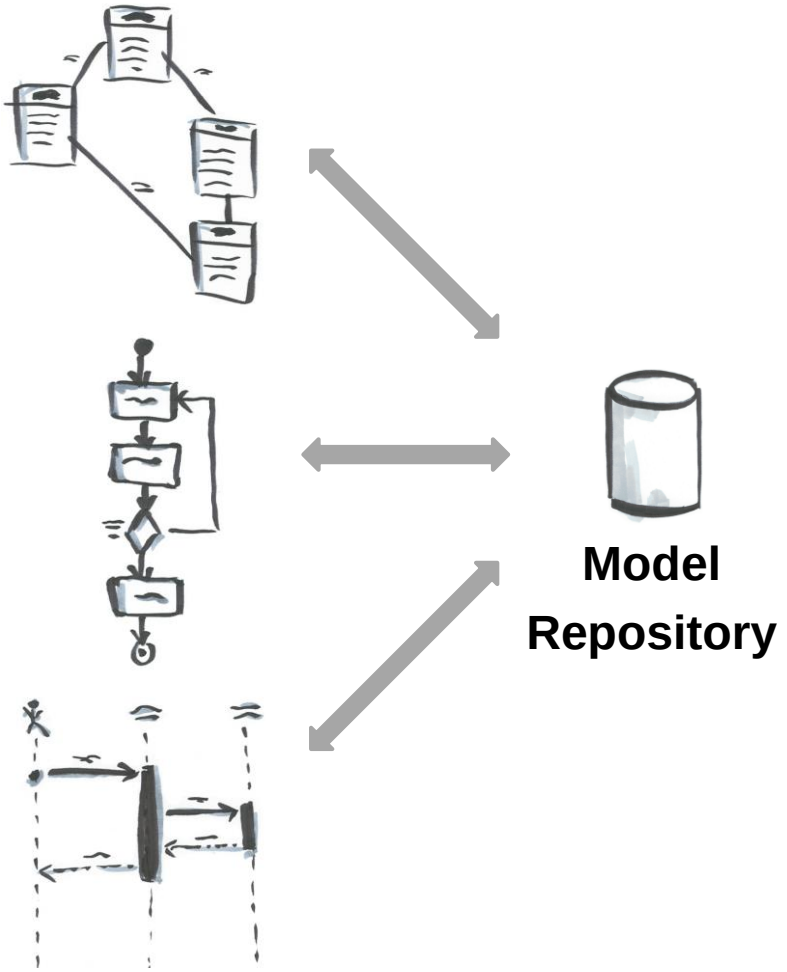
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Structural:

- Class Diagram
- Object Diagram
- Package Diagram
- Component Diagram
- Composite Structure Diagram
- Deployment Diagram

Behavioral:

- UseCase Diagram
- Sequence Diagram
- Activity Diagram
- StateMachine Diagram
- Interaction (Overview) Diagram
- Communication Diagram
- Timing Diagram



Example

Fictitious example (examples from our industry partners are confidential):

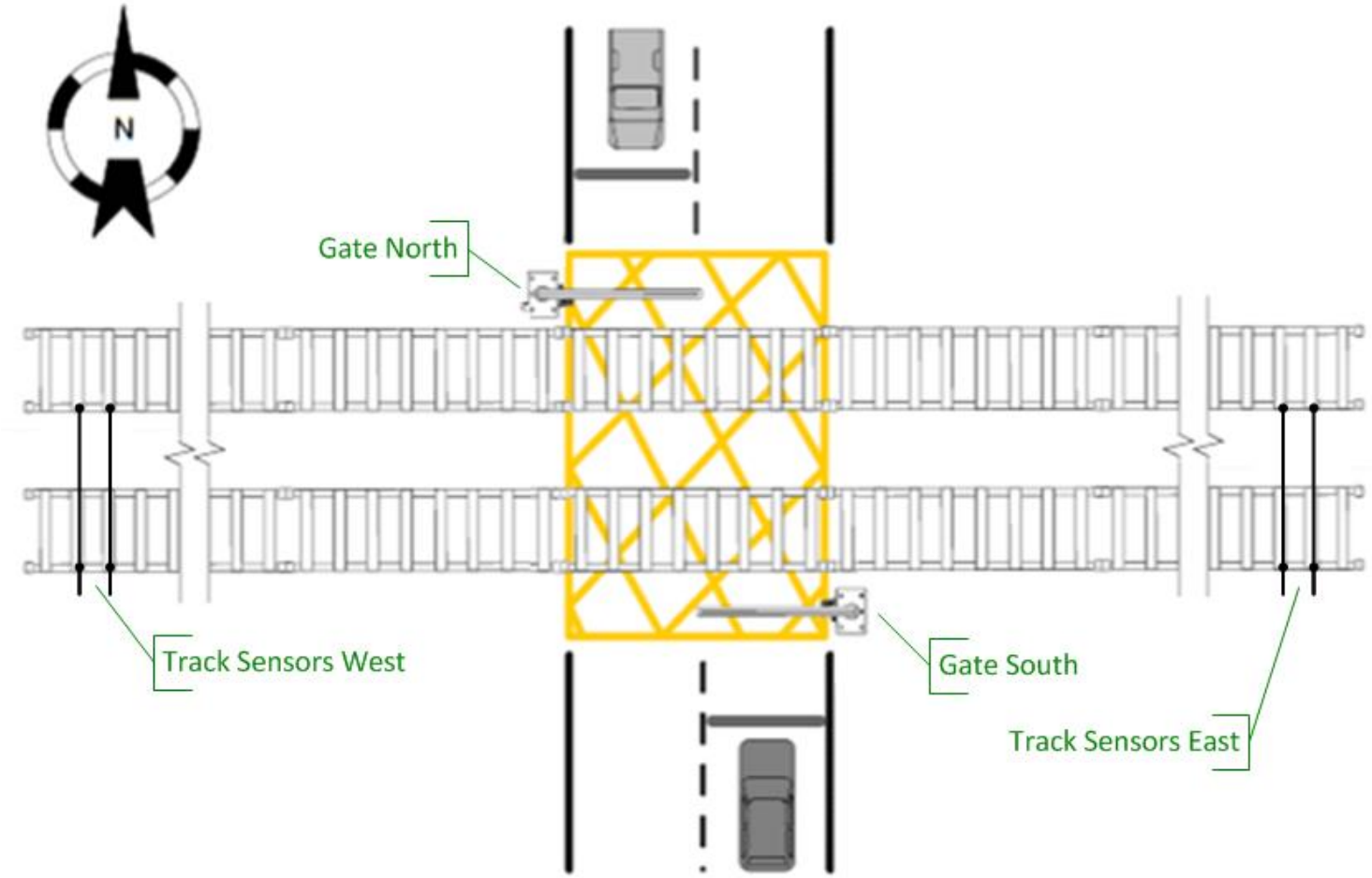
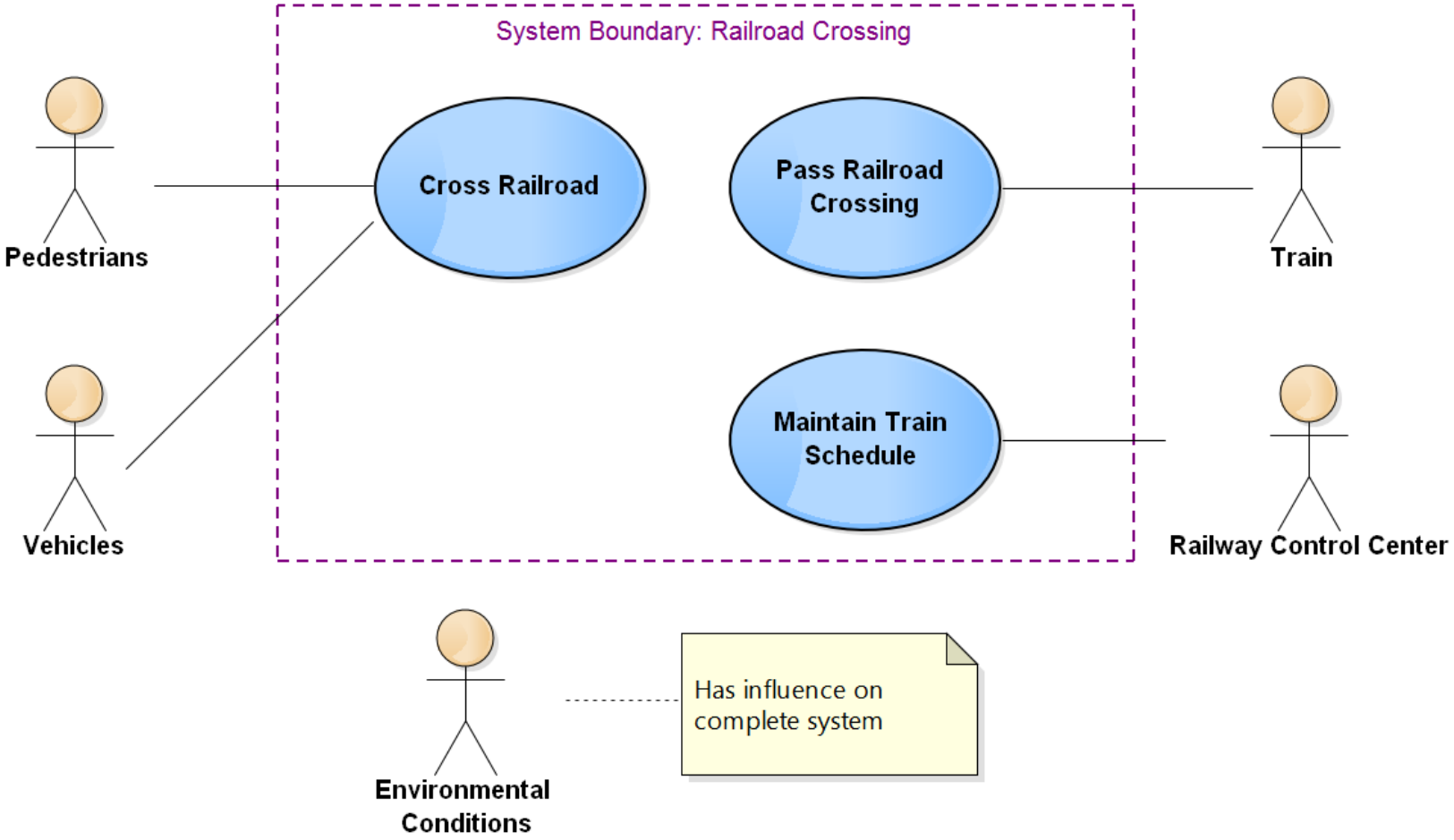


Illustration adapted from Y.S. Weng, et al., *Design of Traffic Safety Control Systems for Railroads and Roadways Using Timed Petri Nets*

System Concept Development: System Definition

Model system requirements as UML UseCase diagram

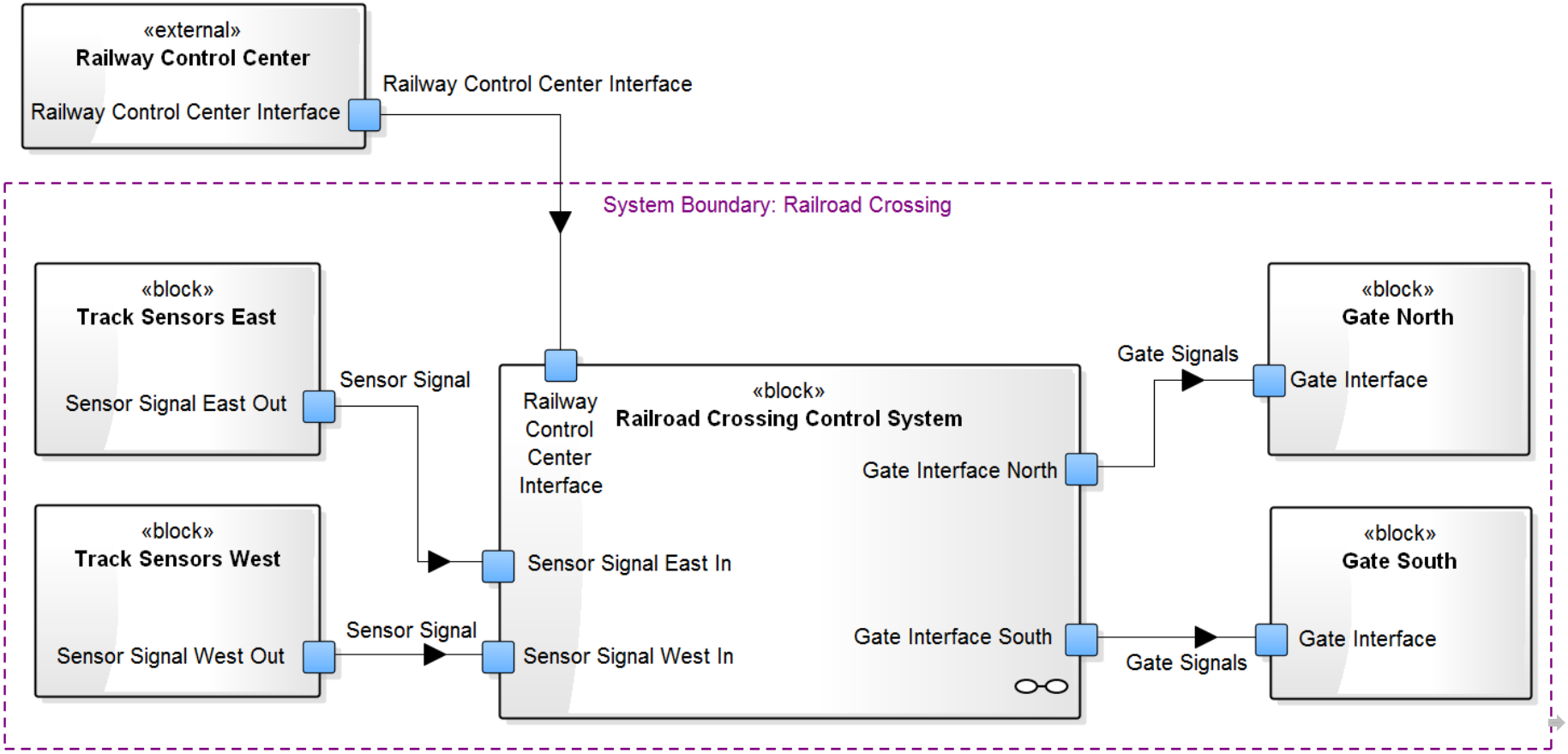


System Concept Development: System Architecture

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

Initial architecture concept as SysML Block diagram

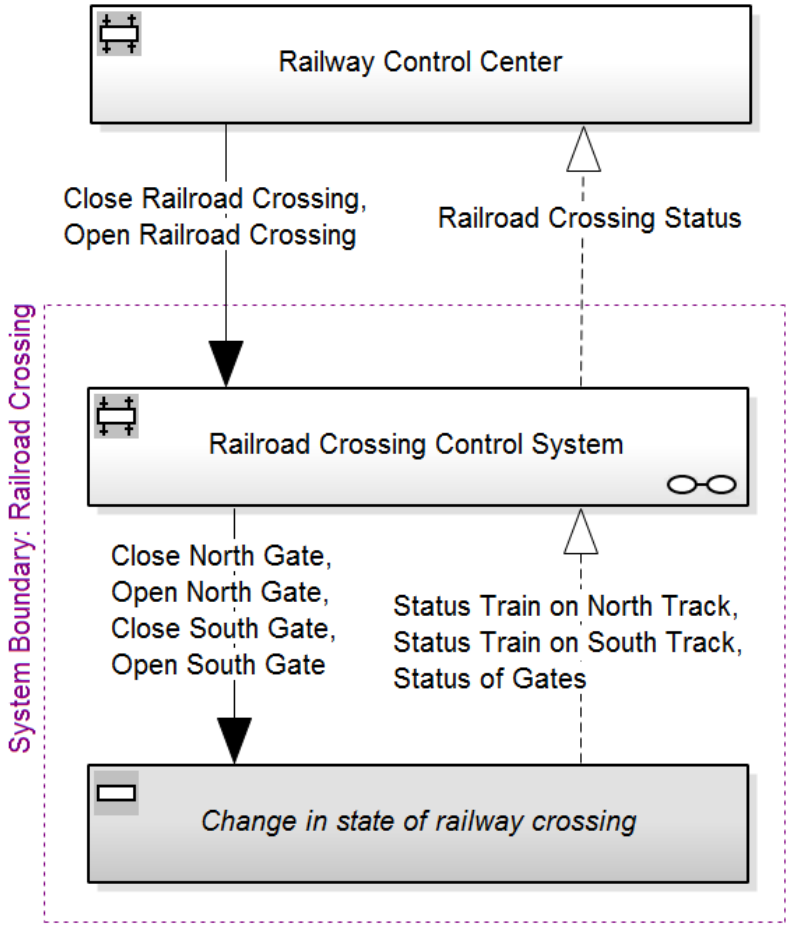
- Suitable for a systematic safety analysis? … No



STPA Hierarchical Control Structure for System Concept Development

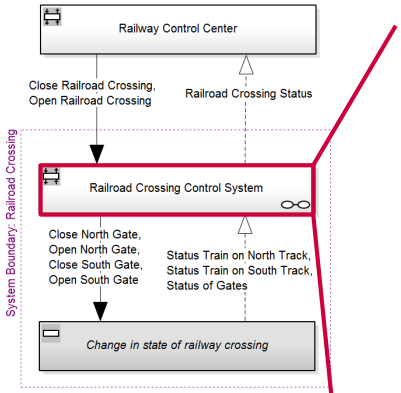
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

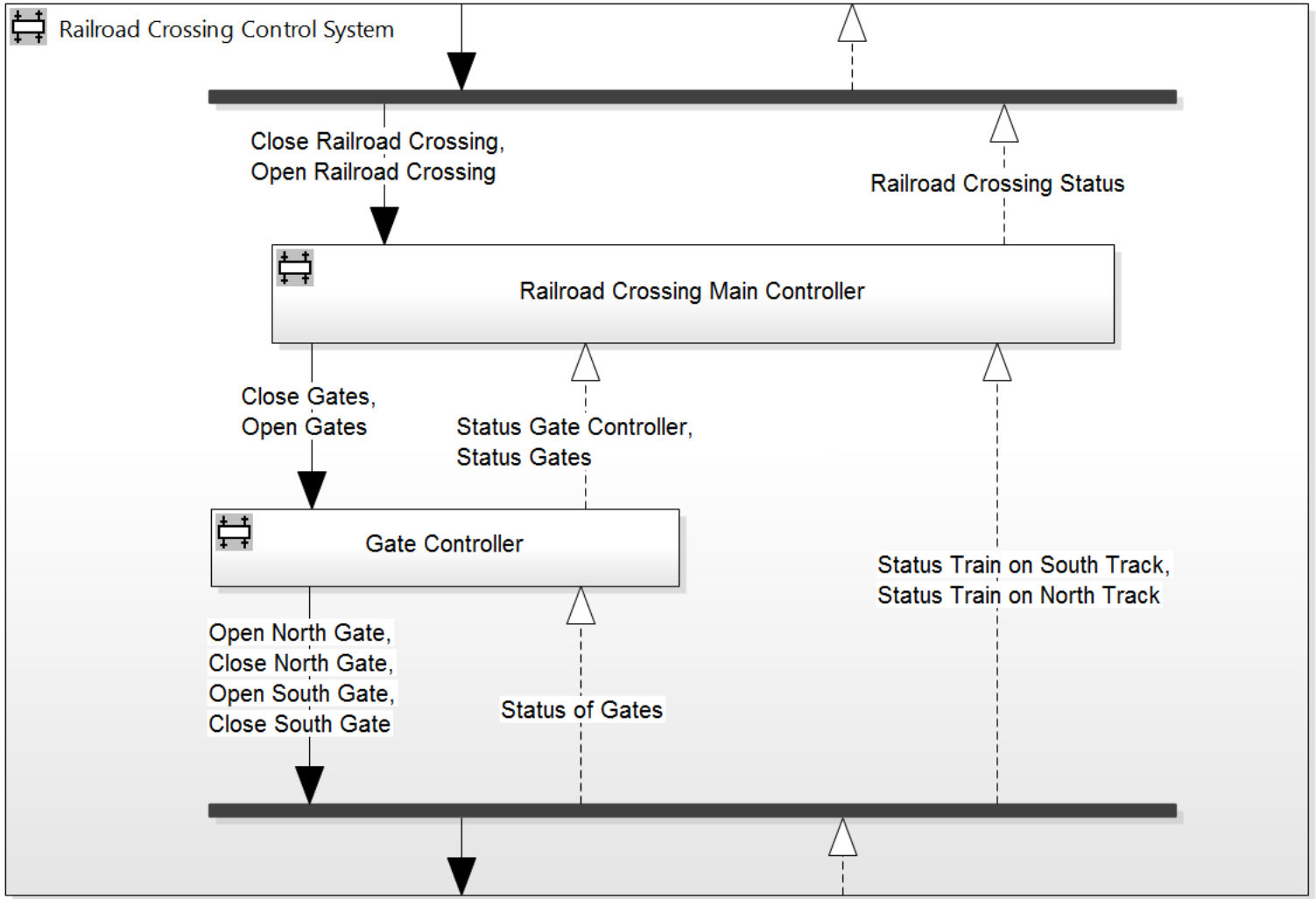
We propose to use a Hierarchical Control Structure for system concept development instead



STPA Hierarchical Control Structure: Support for Multiple Levels of Detail

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





Top Level HCS : Railroad Crossing

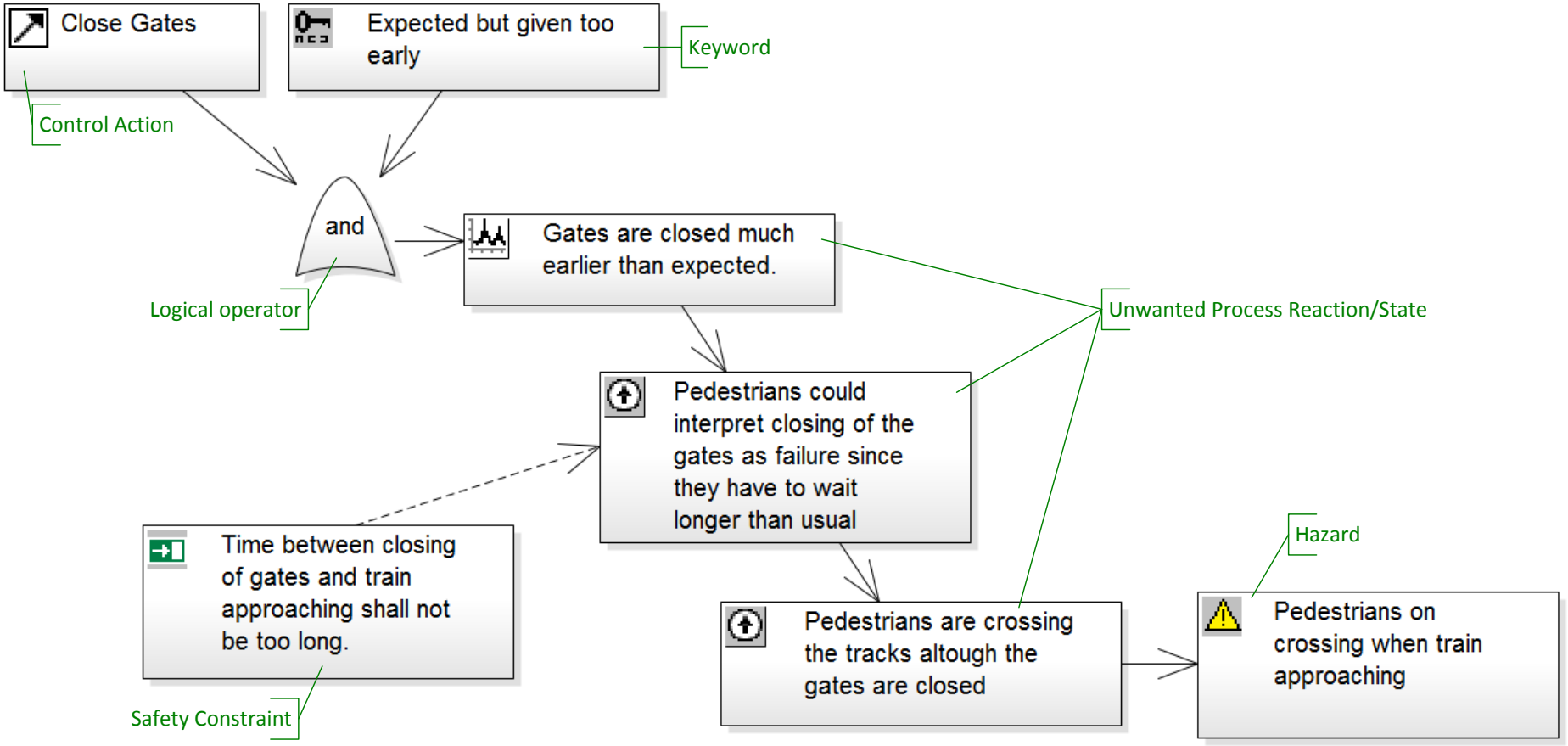
Block Diagram vs. Hierarchical Control Structure (HCS)

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

- Block diagram
  - Focus on components emphasizes component failures
  - Was not designed as a basis for systematic safety analysis
- Hierarchical Control Structure:
  - Is designed as basis for safety analysis with STPA Step 1
  - Step 1 questions correspond to questions developer would naturally ask
- Critical challenge: do not force developer to change scope/mindset. Therefore…
  - Capture HCS, perform Step 1 in the same UML case tool
  - Invent new UML diagram types for HCS, Step 1

STPA Step 1

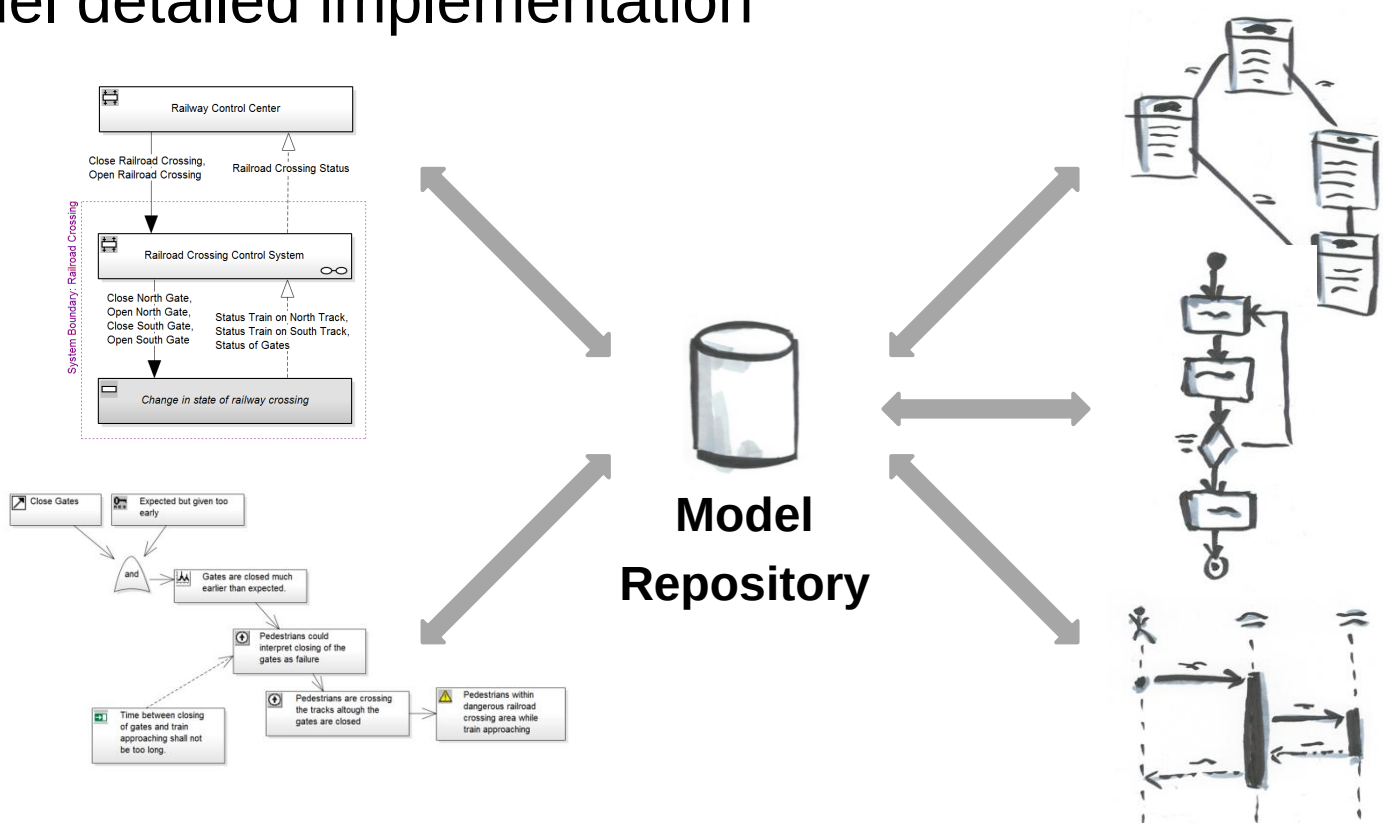
Proposal for STPA Step 1 diagram:



System Development and Traceability

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

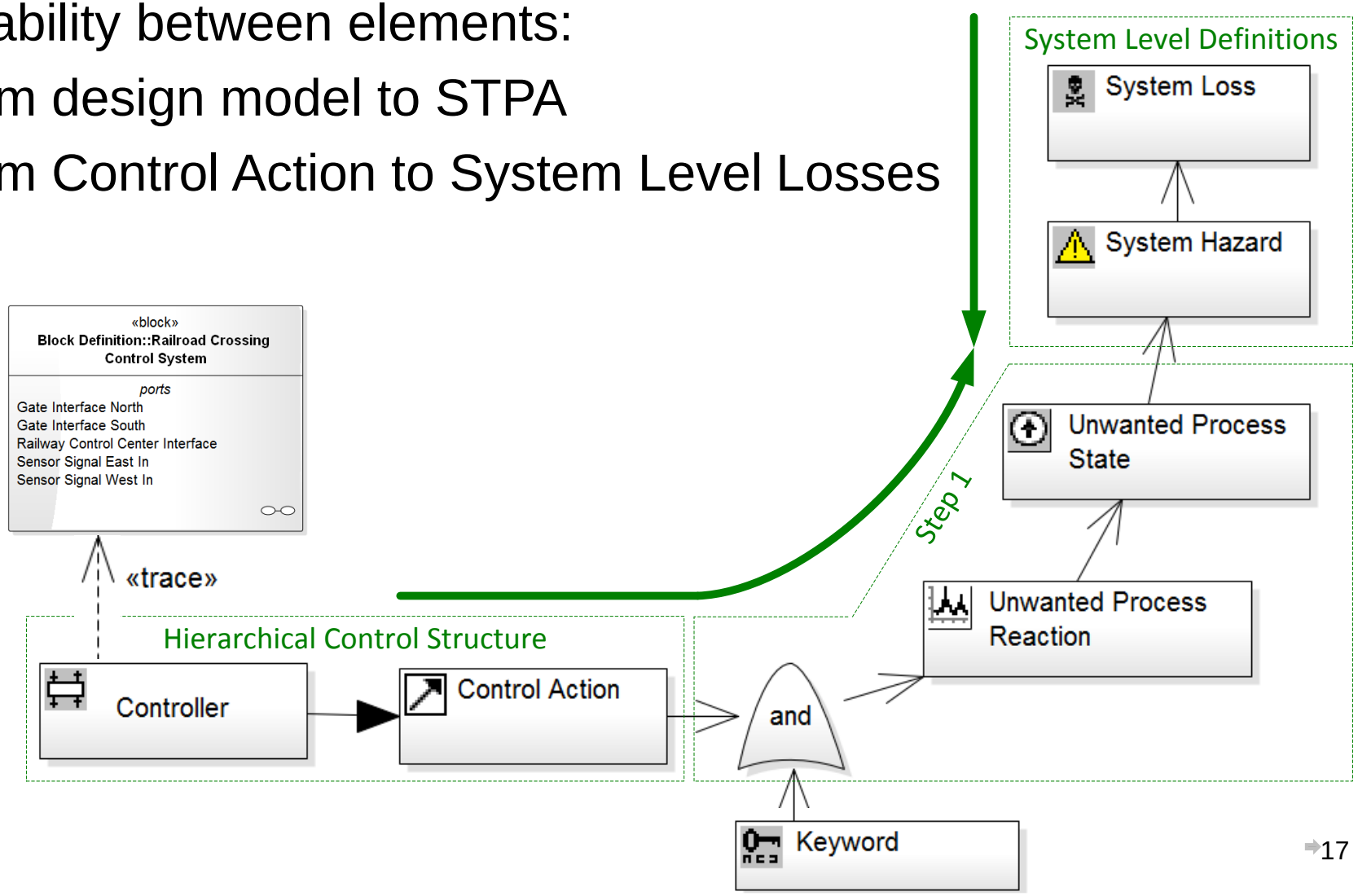
- New diagram types to model functional architecture and safety analysis
- Standard UML diagrams to progress system development and model detailed implementation



System Development and Traceability

Traceability between elements:

- From design model to STPA
- From Control Action to System Level Losses

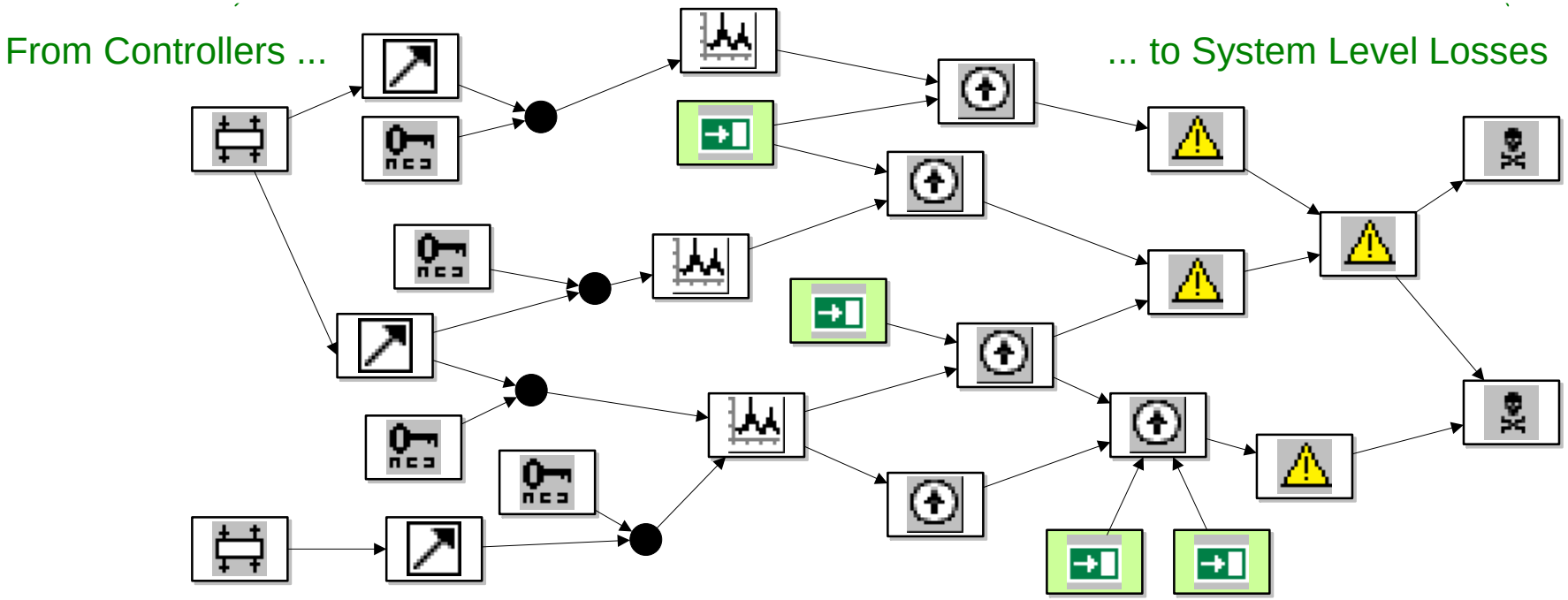


Graph Visualization

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

Visualizing elements and relationships as graph allows:

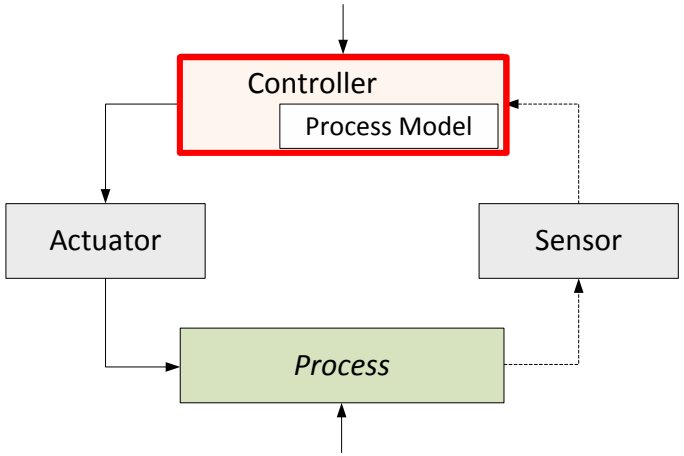
- Seeing the “big picture”
- Analyzing the relevance of controllers
- Doing a safety constraint impact analysis

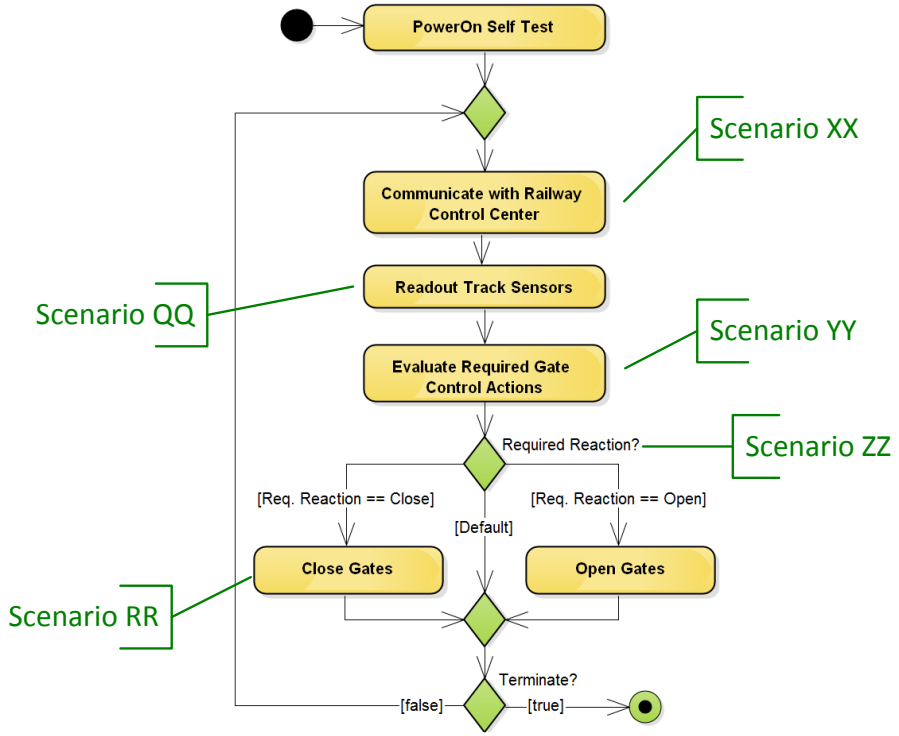


STPA Step 2 – Methods

Methods to identify accident scenarios:

- For simple actuators, sensors, data transmission: FTA, FMEA,
- For complex actuators, sensors: dedicated subsystem STPA
- For controller algorithm: Annotation of Behavioral diagrams



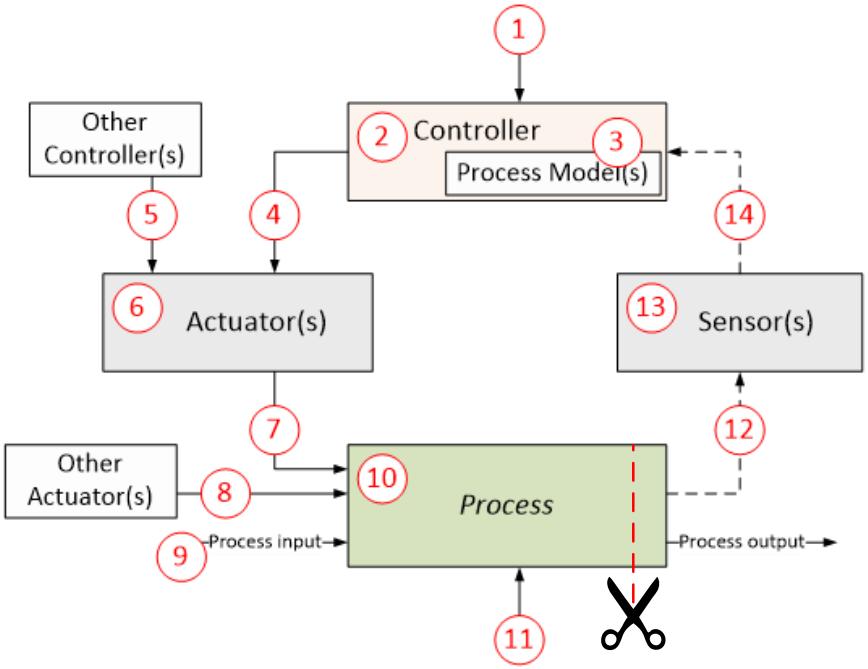


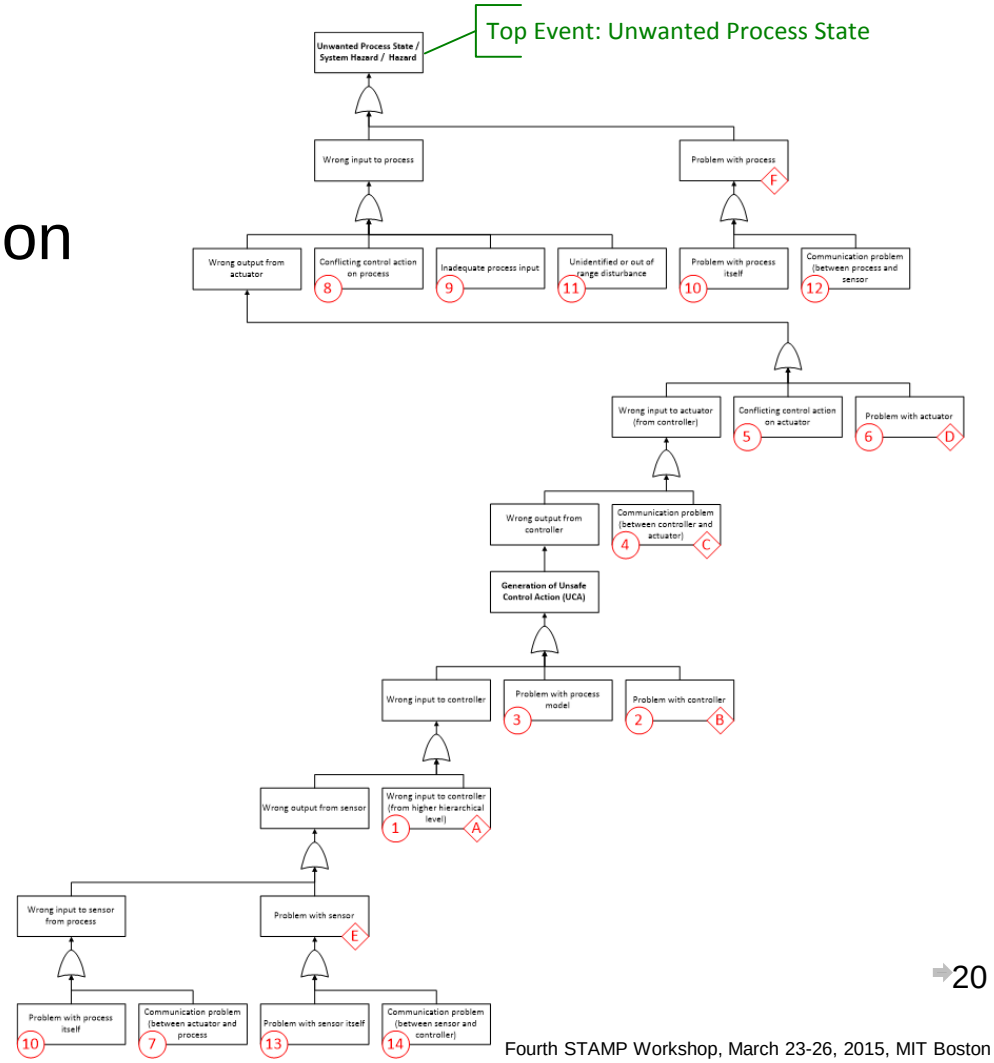
STPA Step 2 – Structured Organization

Organization of accident scenarios with generic fault tree:

- Structured documentation
- Interface to other tools

In principal: allows quantification of accident scenarios





Conclusion and Outlook (1/2)

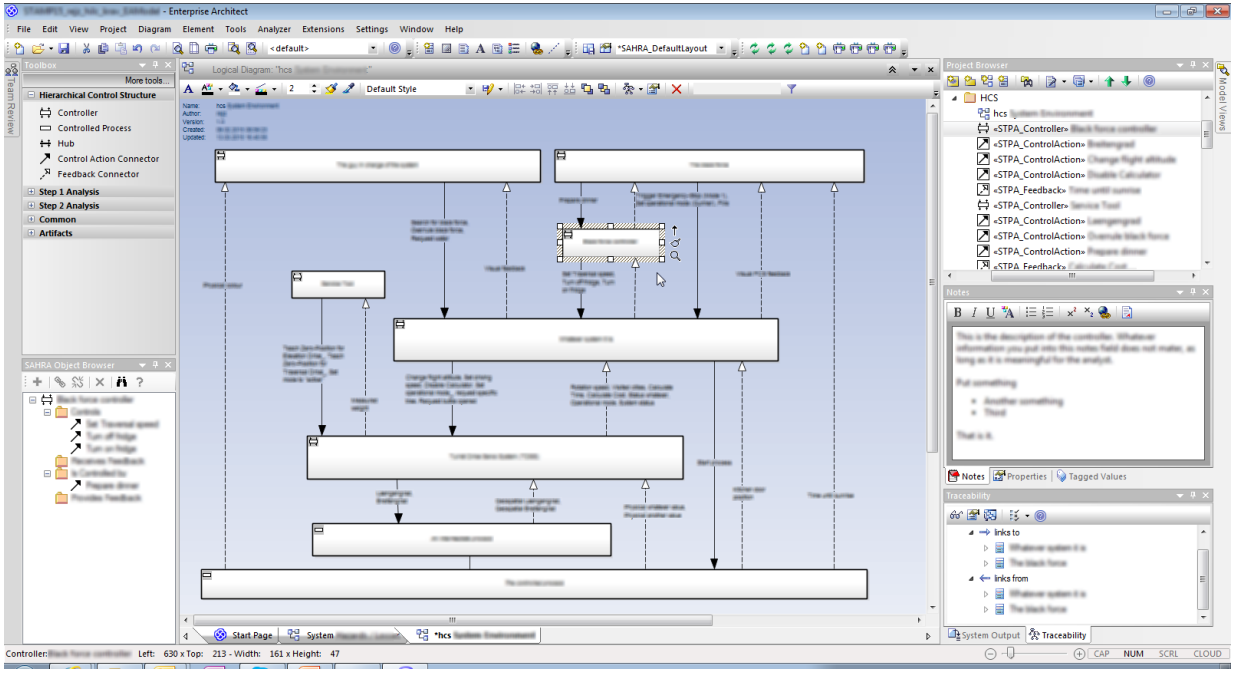
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

We developed a practical approach to safety driven design: the integration of system and safety engineering

- Extended UML with profile for STPA diagrams
  - Hierarchical Control Structure
  - STPA Step 1 diagrams
- Augment behavioral and structural diagrams with annotations to capture accident scenarios
  - STPA Step 2
- Realize and maintain traceability between system design, system implementation and hazards, accidents
- Organize accident scenarios with generic fault tree

Conclusion and Outlook (2/2)

- Project in collaboration with Curtiss Wright Drive Technology, Schaffhausen, Switzerland and funded by Swiss Commission of Technology and Information
- Tool Development:
  - Plan to present the tool at the European STAMP Workshop 2015



SAHRA
STPA based hazard and risk analysis

Contact:

Martin Rejzek
martin.rejzek@zhaw.ch

Sven Stefan Krauss
svenstefan.krauss@zhaw.ch

Christian Hilbes
christian.hilbes@zhaw.ch

http://www.iamp.zhaw.ch/sks
http://www.sahra.ch