Zurich University
of Applied Sciences

School of
Engineering

IAMP Institute of Applied
Mathematics and Physics

4th European STAMP Workshop 2016

STPA Tutorial - Part 1

Introduction

Objectives and Content Overview

Objectives and Organization

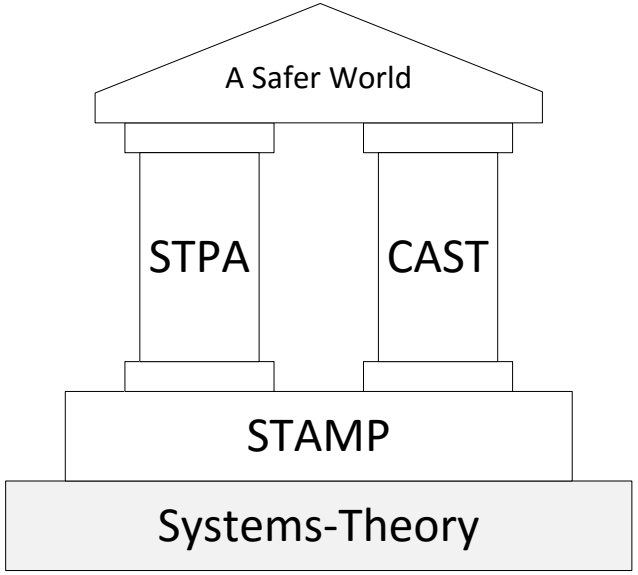
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

- The goal of this tutorial is to give you an **overview** of STPA.
  - Targeted audience: people new to STPA.
  - This is not going to be an in-depth tutorial!
  - STPA is a rather new method and is actively discussed in research.
  - We will present our view, based on our experience using STPA.
  - Slides are quite “verbose” → might help for later review.
- The tutorial will be based on a real-world example system.
  - The example has been constructed for the purpose of this tutorial.
    - It will be presented in a very simplified way!
    - It is not based on a real system design.
  - The goal is to learn about STPA, not to perform a complete and thorough analysis of a real system.
- Large number of workshop participants...
  - We will not be able to discuss all outcomes in plenum.
  - Focus will be on peer discussions, within the groups you are seated.

What is STPA?

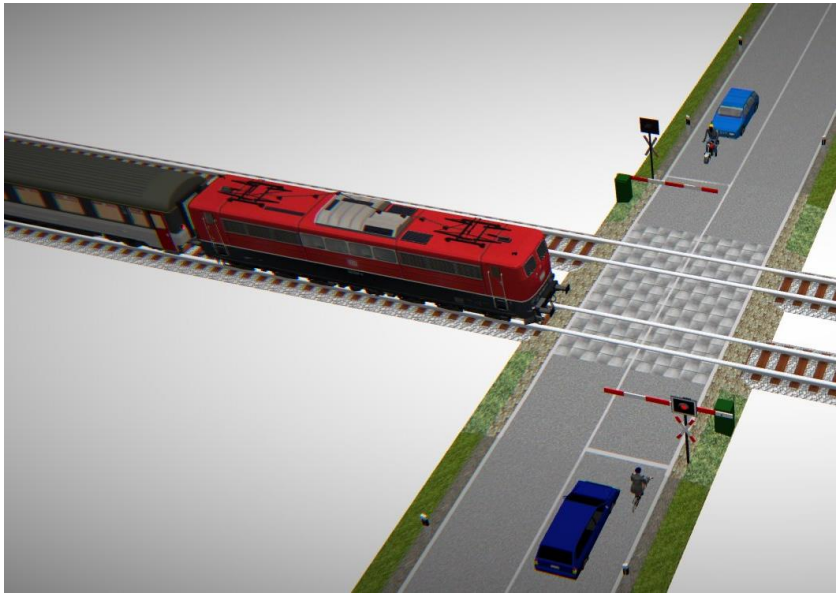
- **STPA** is a hazard analysis method.
  - Developed at MIT by Prof. Nancy Leveson and her team.
    - Read her book *Engineering a Safer World*, which you can download for free at https://mitpress.mit.edu/books/engineering-safer-world
  - Postulate: Safety is a control problem, the goal of control being to enforce safety constraints.
  - Built on top of **STAMP**, a new accident causality model based on systems theory.
  - Complemented by **CAST**, a STAMP based approach for accident analysis.

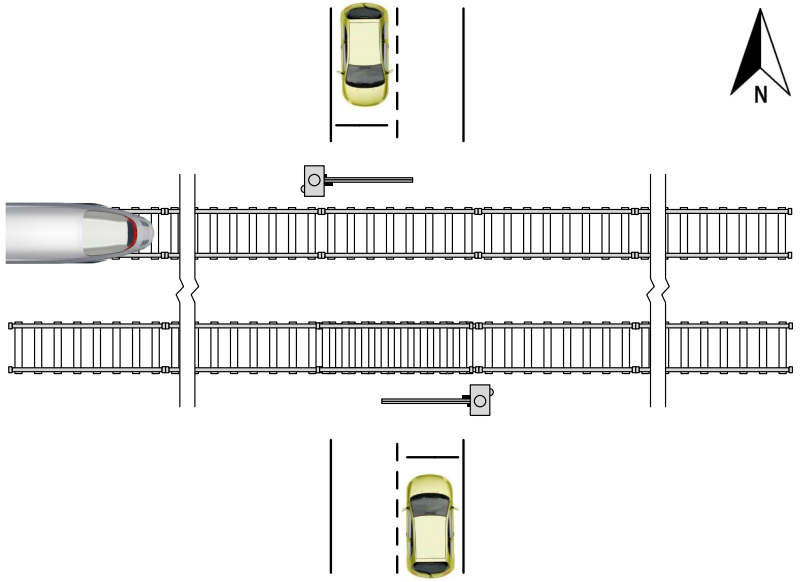
STAMP	Systems-Theoretic Accident Model and Processes
STPA	Systems-Theoretic Process Analysis
CAST	Causal Analysis based on STAMP



Tutorial Example

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

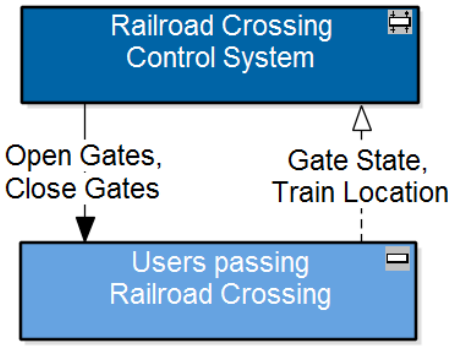


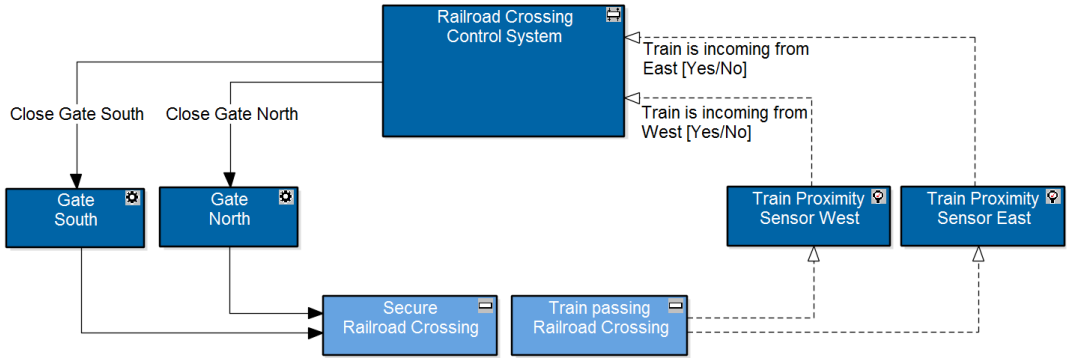


- Railroad Crossing
  - In principle a very clear and simple system...?
  - 2’067 accidents in the US in 2015, 237 people died.
    - Unfortunately rather stable over the last 5 years.
- Good example for sociotechnical system.

STPA in a Nutshell

- STPA has especially been designed to cope with sociotechnical systems.
- STPA is a model based hazard analysis method.
  - It is supported by two diagram types
    - Hierarchical Control Structures and Control Loops

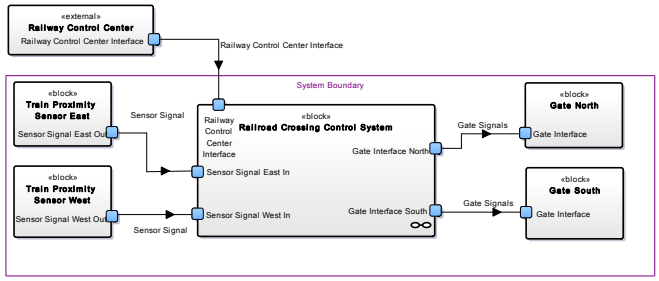


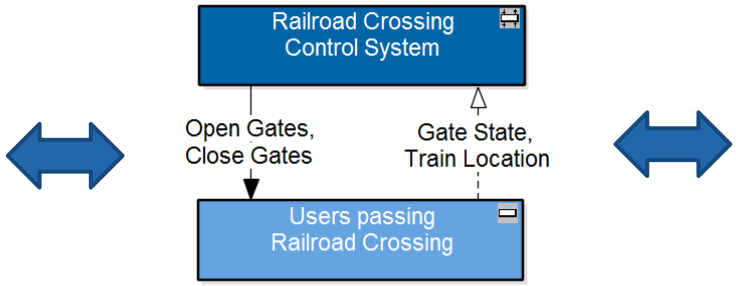


- STPA is performed in two steps... Step 1 and Step 2...

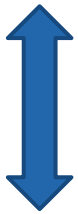
STPA in a Nutshell - Step 1

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





Unsafe Control Actions

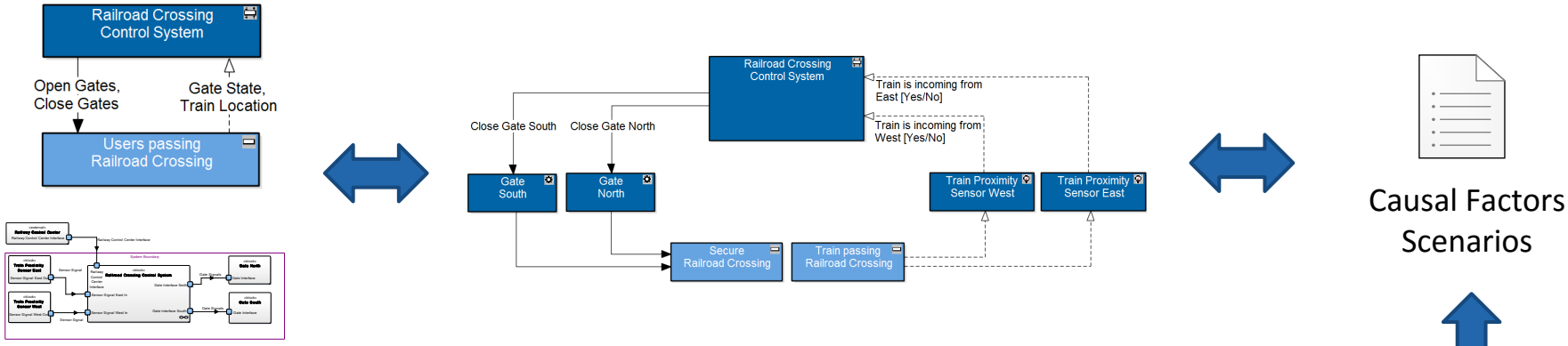


Safety Constraints

- Understand the design and represent the control flow through the system in terms of a Hierarchical Control Structure.
- Systematically identify Unsafe Control Actions.
- Check/Specify Safety Constraints.

STPA in a Nutshell - Step 2

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



- Look into the details of each UCA by modeling the full Control Loop for the related Control Action.
- Systematically check for Causal Factors and Scenarios for the UCA.
- Check/Specify/Refine Safety Constraints.

Intended Tutorial Schedule - In Three Parts

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

- STPA in a Nutshell
  - Set the scope for the Tutorial Example
  - See how STPA differs from established methods
  - Give an overview of the whole STPA Process
- Group Activity - STPA Step 1
  - Modeling the system in terms of a Hierarchical Control Structure
  - Identifying potential Unsafe Control Actions (UCA)
- Group Activity - STPA Step 2
  - Modeling the system in terms of UCA specific Control-Loops
  - Identifying scenarios and causal factors for an UCA
- We try to make a coffee break each 45 minutes, with a longer one in the middle.

The Philosophical Question: Why STPA?

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

- Why do we need yet another hazard analysis method?
  - We know about FMEA, FTA, HAZOP...
  - Those work and we can apply them in all cases...
  - So why do we need something additional?
- We will *not* discuss the reasons for STPA in this tutorial.
  - In *Engineering a Safer World* Nancy does make the case for STPA in a very convincing way!
- Instead
  - We will focus on what makes STPA different from and how it relates to the other methods to illustrate its usefulness.
  - We want to let you get active and experience STPA hands-on.

Organization of Group Activities

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

- One group per table.
  - Flipchart paper and pin board.
  - Step 1 and Step 2 table templates.
- We will collect, photograph and scan all results and put them online (somehow) for your access.
- Before we start (in 5 minutes)...

Let's do a short introduction round at each table!

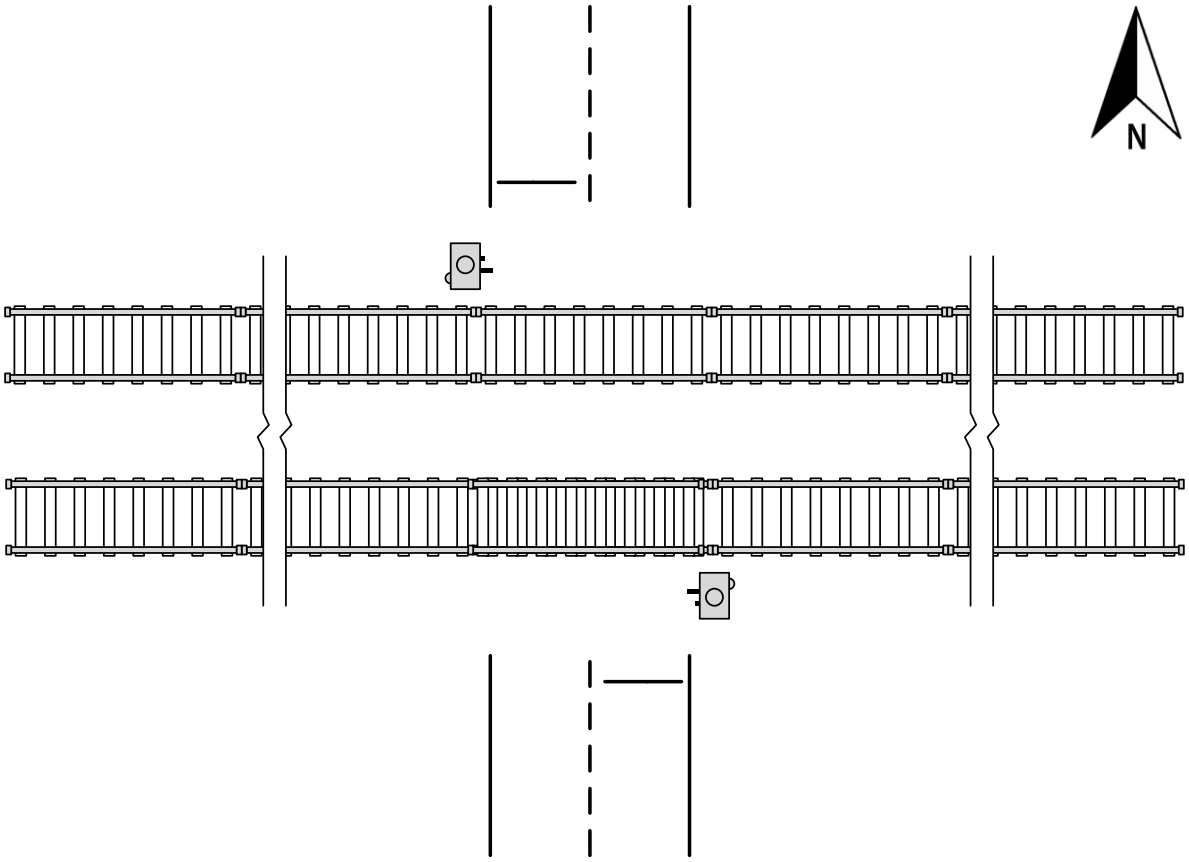
A full introduction round might take too much time, but we will have coffee breaks and will meet each other at the conference.

The Tutorial Example

Setting the Scope

Tutorial Example - Railroad Crossing

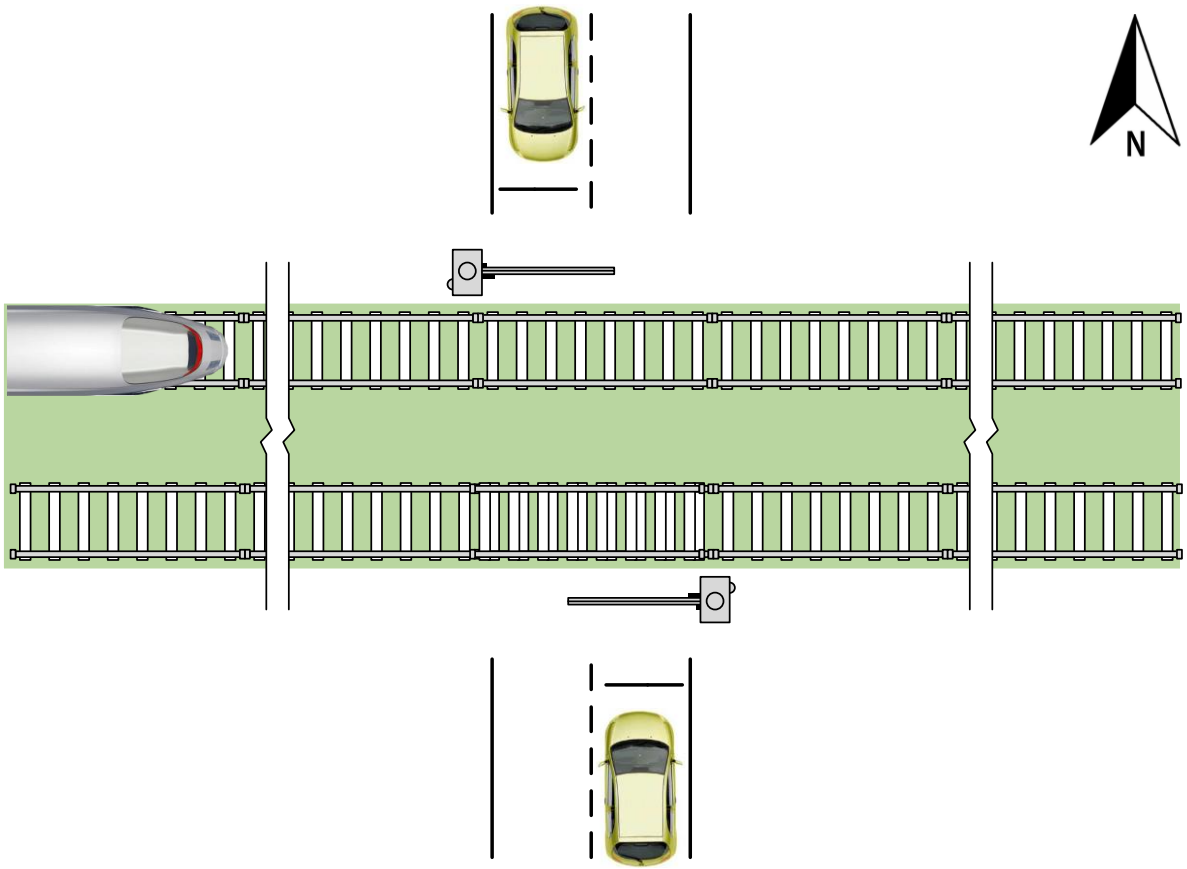
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics



- Gates on north and south side.
- Trains arrive from west or east side.

Tutorial Example - Railroad Crossing

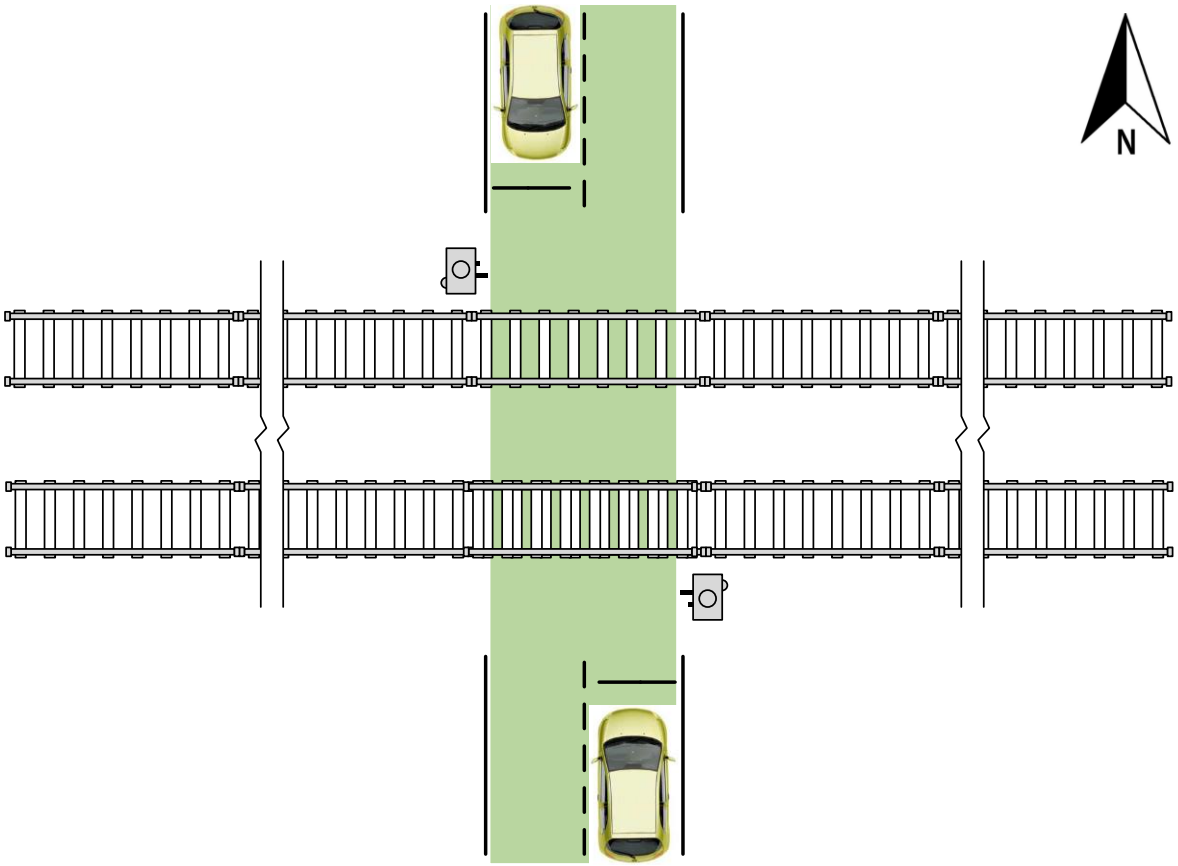
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics



- Gates on north and south side.
- Trains arrive from west or east side.
- Railroad Crossing Control System detects incoming train and secures the crossing for the train to pass.

Tutorial Example - Railroad Crossing

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



- Gates on north and south side.
- Trains arrive from west or east side.
- Railroad Crossing Control System detects incoming train and secures the crossing for the train to pass.
- Once the train has passed, cars and people are allowed to cross again (safely).

Tutorial Example - Setting the Scope

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

- The users perspective:
  - Who are the users of the system “Railroad Crossing”?
    - Drivers in automotive vehicle: cars, bikes, trucks, buses...
    - Cyclists, pedestrians.
    - Train Driver.
  - What do the users expect from the system?
    - System should support (guarantee?) them to safely pass the crossing.
  - How do the users perceive this system?
    - We know the car drivers, cyclists and pedestrians perspective from our own experience.
    - Train driver perspective → movie

Tutorial Example - Setting the Scope

- Other stakeholders? What is their perspective of the system?
  - Owner and/or Operator
    - Large maintenance effort; timetable risk; costly infrastructure because of safety regulations; ...
  - Authorities

Federal Railroad Administration
Office of Safety Analysis

Type & Highway User		Totals			At Public Crossing						At Private Crossing					
					Motor Vehicle			Other			Motor Vehicle			Other		
		Accs	Kld	Inj	Accs	Kld	Inj	Accs	Kld	Inj	Accs	Kld	Inj	Accs	Kld	Inj
Train struck highway user	Car	701	71	341	627	62	317	-	-	-	74	9	24	-	-	-
	Trucks	320	39	150	253	29	122	-	-	-	67	10	28	-	-	-
	Trk& Trail	290	4	207	203	2	180	-	-	-	87	2	27	-	-	-
	Van	53	9	14	44	7	13	-	-	-	9	2	1	-	-	-
	Buses	4	2	18	4	2	18	-	-	-	-	-	-	-	-	-
	Oth Mtr V.	112	12	52	95	10	47	-	-	-	17	2	5	-	-	-
	Pedestrian	144	66	50	-	-	-	142	64	50	-	-	-	2	2	-
	Other	53	16	16	-	-	-	44	15	14	-	-	-	9	1	2
	---- Total	1,677	219	848	1,226	112	697	186	79	64	254	25	85	11	3	2
Train struck BY highway user	Car	218	6	91	214	6	90	-	-	-	4	-	1	-	-	-
	Trucks	89	6	25	80	6	22	-	-	-	9	-	3	-	-	-
	Trk& Trail	32	-	12	23	-	11	-	-	-	9	-	1	-	-	-
	Van	17	3	21	17	3	21	-	-	-	-	-	-	-	-	-
	Oth Mtr V.	18	-	7	17	-	7	-	-	-	1	-	-	-	-	-
	Pedestrian	6	2	3	-	-	-	6	2	3	-	-	-	-	-	-
	Other	10	1	5	-	-	-	10	1	5	-	-	-	-	-	-
	---- Total	390	18	164	351	15	151	16	3	8	23	-	5	-	-	-
---- Total		2,067	237	1,012	1,577	127	848	202	82	72	277	25	90	11	3	2

http://safetydata.fra.dot.gov/OfficeofSafety/publicsite/Query/HwyRailAccidentSummaryByRR.aspx
2015 Data

Tutorial Example - Setting the Scope

- Other stakeholders? What is their perspective of the system?
  - Owner and/or Operator
    - Large maintenance effort; timetable risk; costly infrastructure because of safety regulations; ...
  - Authorities

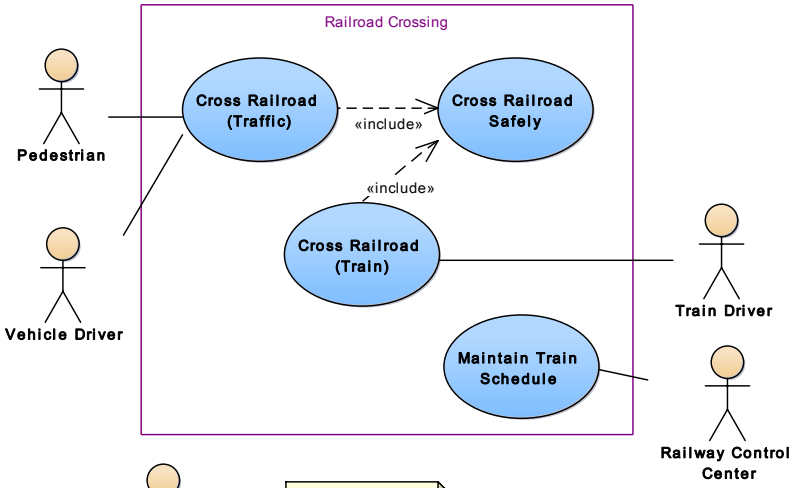
Federal Railroad Administration
Office of Safety Analysis

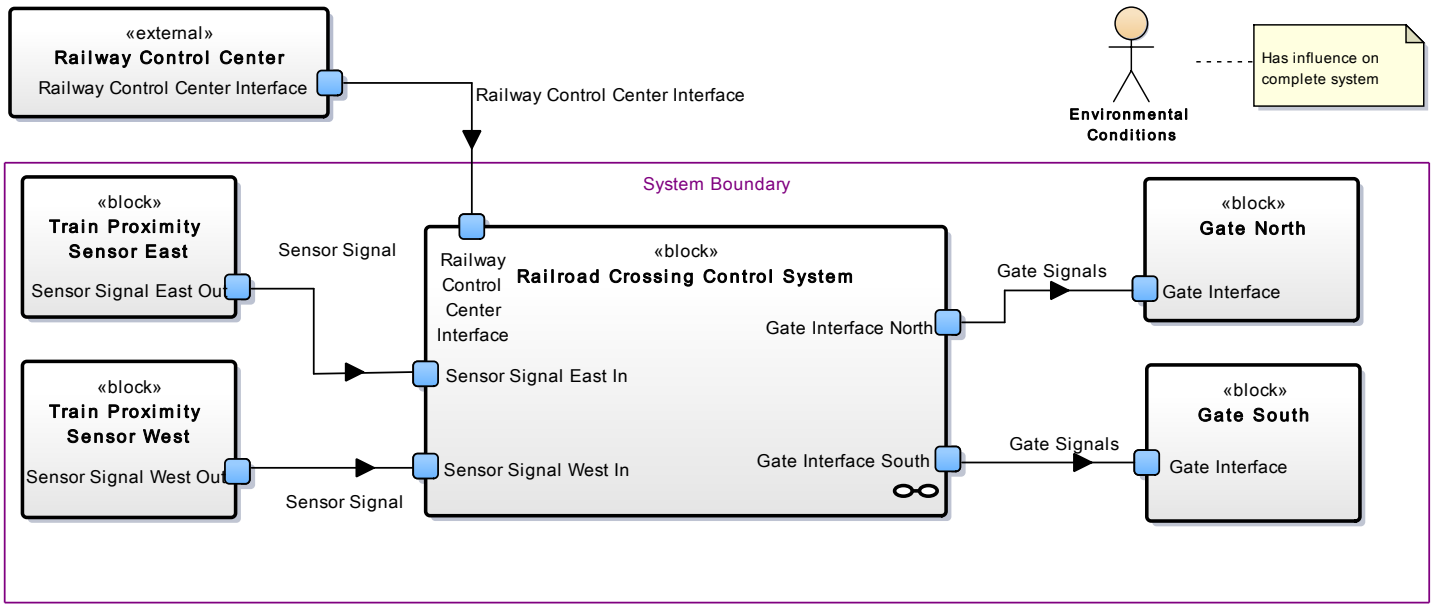
Warning		Totals			At Public Crossing						At Private Crossing					
					Motor Vehicle			Other			Motor Vehicle			Other		
		Accs	Kld	Inj	Accs	Kld	Inj	Accs	Kld	Inj	Accs	Kld	Inj	Accs	Kld	Inj
Train struck highway user	Gates	824	139	442	652	64	392	155	72	47	15	1	3	2	2	-
	Flashing lights	158	11	65	147	9	59	7	2	4	3	-	2	1	-	-
	HWTS,WW,Bells	11	1	2	9	-	1	1	1	-	1	-	1	-	-	-
	Watchman	19	-	5	11	-	1	-	-	-	8	-	4	-	-	-
	Stop signs	289	43	148	142	21	95	5	-	4	136	22	48	6	-	1
	Cross bucks	311	21	173	258	18	149	16	3	8	36	-	16	1	-	-
	Other	4	-	2	-	-	-	-	-	-	4	-	2	-	-	-
	None	61	4	11	7	-	-	2	1	1	51	2	9	1	1	1
	---- Total	1,677	219	848	1,226	112	697	186	79	64	254	25	85	11	3	2
Train struck BY highway user	Gates	172	13	74	159	10	69	13	3	5	-	-	-	-	-	-
	Flashing lights	85	2	43	80	2	39	3	-	3	2	-	1	-	-	-
	HWTS,WW,Bells	4	-	1	3	-	1	-	-	-	1	-	-	-	-	-
	Watchman	8	-	4	7	-	4	-	-	-	1	-	-	-	-	-
	Stop signs	27	-	8	20	-	7	-	-	-	7	-	1	-	-	-
	Cross bucks	86	3	34	82	3	31	-	-	-	4	-	3	-	-	-
	Other	1	-	-	-	-	-	-	-	-	1	-	-	-	-	-
	None	7	-	-	-	-	-	-	-	-	7	-	-	-	-	-
	---- Total	390	18	164	351	15	151	16	3	8	23	-	5	-	-	-
---- Total		2,067	237	1,012	1,577	127	848	202	82	72	277	25	90	11	3	2

http://safetydata.fra.dot.gov/OfficeofSafety/publicsite/Query/HwyRailAccidentSummaryByRR.aspx
2015 Data

Tutorial Example - Setting the Scope

- Yet another Stakeholder: the Designer!
  - Her/his perspective seeing the railroad crossing system as a SysML model.





Tutorial Example - Setting the Scope

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

- What can go wrong?
  - System level accidents or losses?
  - System level hazards?

- A (slightly sarcastic) side-note on definitions
  - There are as many unique, precise and unambiguous definitions for terms like hazard, risk, etc... as there are experts on this topic!

- For the sake of this tutorial, let's define the hazard and accident/loss terms, as suggested by this movie.

The Hazard Analysis Phase

The Choice of Method and STPA as an Option

Tutorial Example - Perform Hazard Analysis!

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

- What method shall we use?
  - As risk analysts, we master a broad selection of hazard analysis techniques: FTA, FMEA, HAZOP, ...
- Criteria for method selection?
  - From Merriam-Webster - *Method: a systematic procedure, technique, or mode of inquiry employed by [...]*
  - As long as you are systematic, there is not really a right/wrong in the selection of the tool, there's rather a more/less useful!


Picture by Christian Hilbes

Tutorial Example - Perform Hazard Analysis!

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

- What method shall we use?
  - As risk analysts, we master a broad selection of hazard analysis techniques: FTA, FMEA, HAZOP, ...
- Criteria for method selection?
  - From Merriam-Webster - Method: a systematic procedure, technique, or mode of inquiry employed by [...]
  - As long as you are systematic, there is not really a right/wrong in the selection of the tool, there's rather a more/less useful!
- Useful? Purpose of a hazard analysis?
  - Cited freely from the FAA System Safety Handbook: *Hazard analyses are performed to identify and define hazardous conditions for the purpose of their elimination or control.*
  - Meaning of *useful* in this context: Supporting the analyst in a systematic way to most efficiently *see* and *document hazards* and their *causal factors*, and to propose ways to *improve safety*.

Hazard Analysis and Lifecycle Phase

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

- How useful a method is depends on the type of system you have to analyze and its lifecycle phase.
- Depending on a systems lifecycle phase
  - The inputs to the hazard analysis can be very different.
  - The analysis outcome can have a very different impact.
  - During the Design Phase → Safety-Guided-Design
    - Inputs: No detailed component information available yet.
    - Impact Potential: Potential to change the system design to make the system safer.
  - Once the system is in operation → Safety Assessment
    - Inputs: All details known.
    - Impact Potential: Can put restrictions on the systems use or “fix” the problem by e.g. adding system external measures.

Hazard Analysis and System Type

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

- Depending on the type of system
  - We (think we) know what is understood by IT-Systems, Embedded-Systems,...!
    - We know for sure, how hard it is to analyze complex distributed systems or even the simplest software based systems!
  - But what is a *Sociotechnical System*?
    - Not easy to define: System where humans and technology interact in a way defined by laws, regulations and culture...
    - Easier to see the point by looking at an example → Movie

Hazard Analysis and System Type

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

- A thorough discussion of sociotechnical systems can be found in Nancy's book *Engineering a Safer World.*
- A few quotes from *Engineering a Safer World*:
  - *Each local decision [in a sociotechnical system] may be correct in the limited context in which it was made but lead to an accident when the independent decisions and organizational behaviors interact in a dysfunctional way.*
  - *Safety, on the other hand [compared to reliability] is an emergent property of systems: Safety can be determined only in the context of the whole.*

- ... that doesn't make the task any easier for the risk analyst :/

Usefulness of STPA - How is it different?

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

- The STPA process
  - has been specifically designed to cope with complex sociotechnical systems.
  - guides the analyst through the hazard analysis effort in a very structured and systematic way.
- STPA is a model based hazard analysis technique
  - FMEA, FTA, ... are typically based on design models of a system.
  - STPA is based on a very specific representation of the system specially designed for the purpose of a hazard analysis.
    - This representation has to be built from the design model.
    - In the *Safety-Guided-Design* paradigm it can be used as a design tool.
  - The risk analysts assumptions are made very explicit, hence reviewable!

Enlightenment depends on the point of view

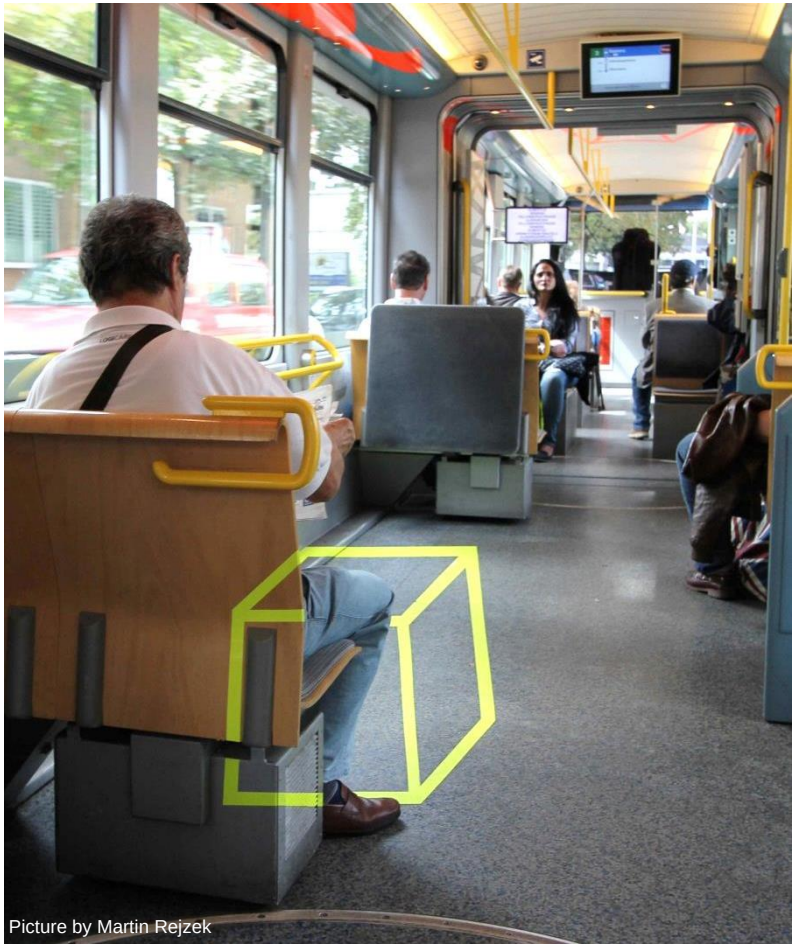
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Picture by Martin Rejzek


Picture by Martin Rejzek

Enlightenment depends on the point of view

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


Picture by Martin Rejzek


Picture by Martin Rejzek

STPA Analysis Steps and System Views

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

- STPA is performed in two steps, called... Step 1 and Step 2.
- Step 1
  - Goal: Identify potential for inadequate control of the system that could lead to hazards (Unsafe Control Actions, UCA) and check/specify safety constraints.
  - Required Input: Hierarchical Control Structure (HCS) + Design Documentation of the system
- Step 2
  - Goal: Determine how each of the UCA identified in Step 1 could occur and check/specify/refine safety constraints.
  - Required Input: UCA specific Control Loops + Design Documentation of the system
- Reminder (FAA System Safety Handbook):
  - *Hazard analyses are performed to identify and define hazardous conditions for the purpose of their elimination or control.*

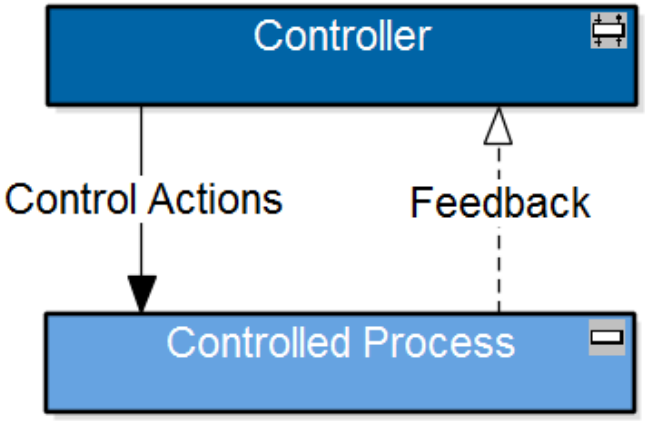
STPA in a Nutshell

STPA Step 1

STPA Step 1 - Hierarchical Control Structure

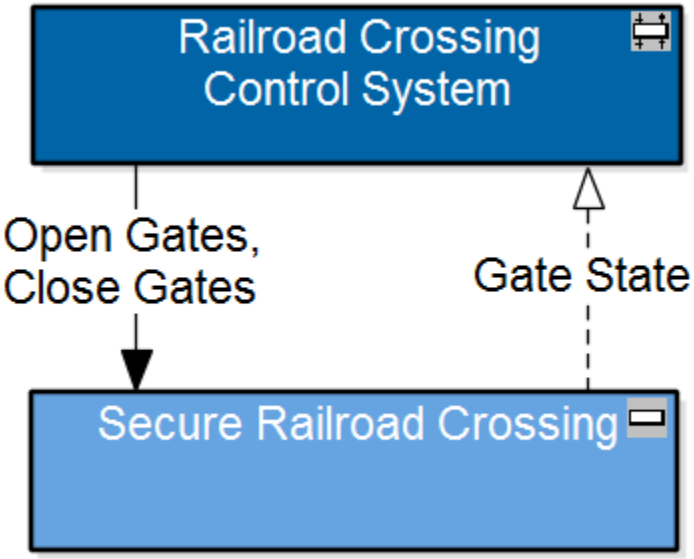
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

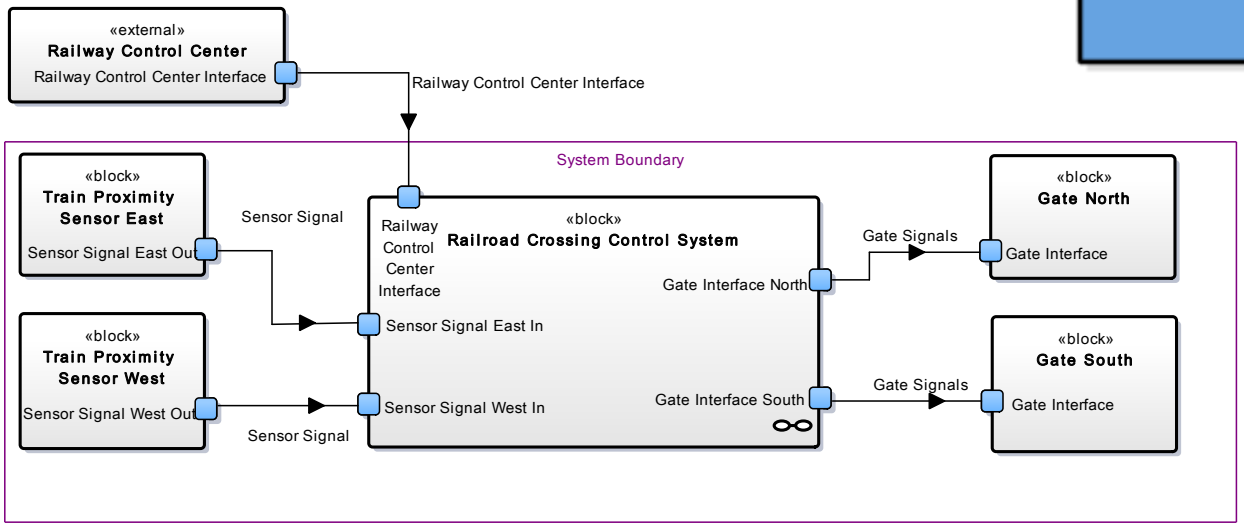
- System seen as a HCS
  - Controller
    - Entity that controls the process as to satisfy our expectations.
  - Controlled Process (Difficult to define)
    - “That” what happens under control of the system.
    - “Service” we expect from the system.
  - Control Actions
    - Ways the controller can influence the process.
  - Feedback
    - Information the controller gets from the process.



STPA Step 1 - Hierarchical Control Structure

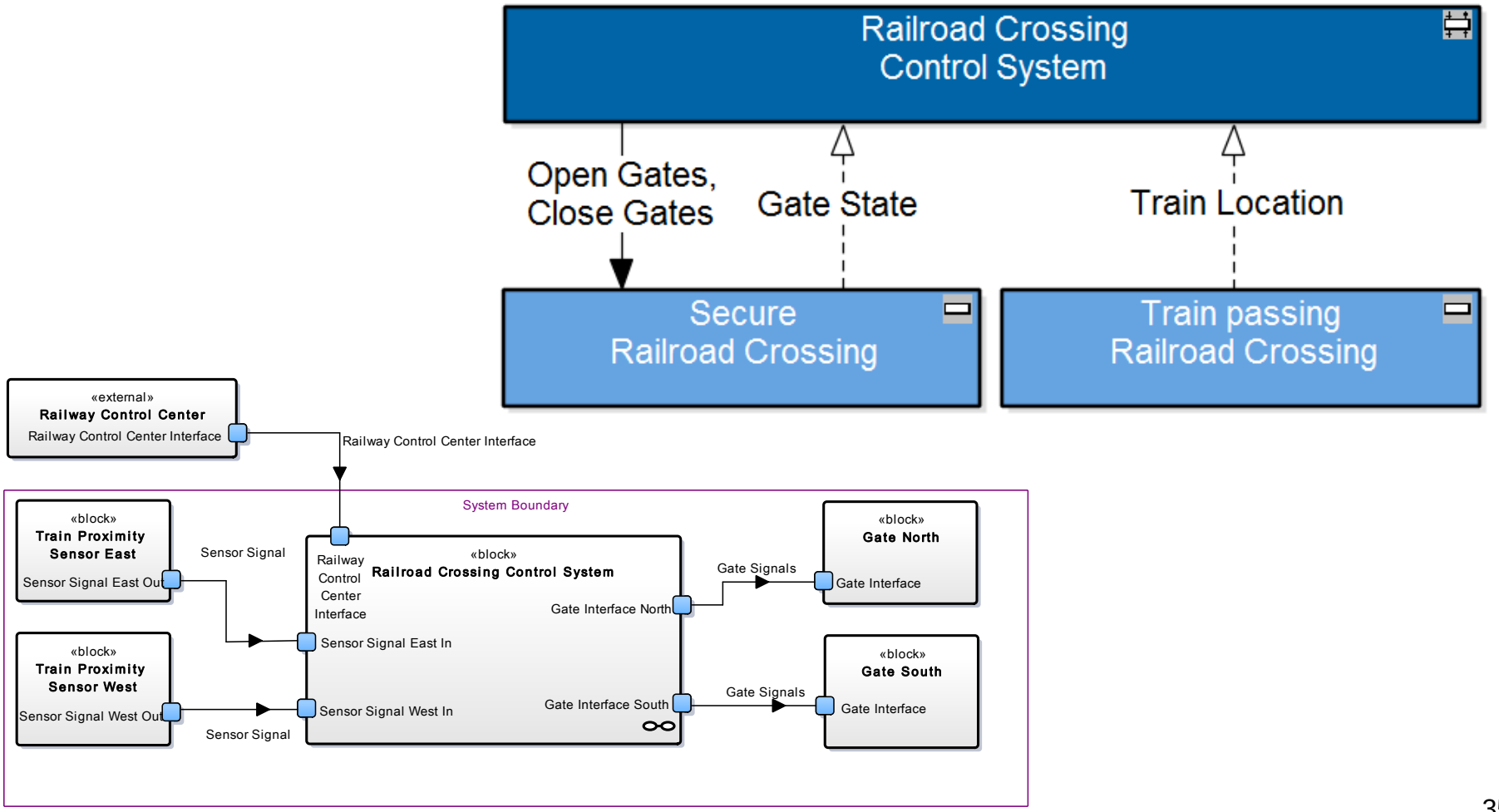
- Simple (?) Example





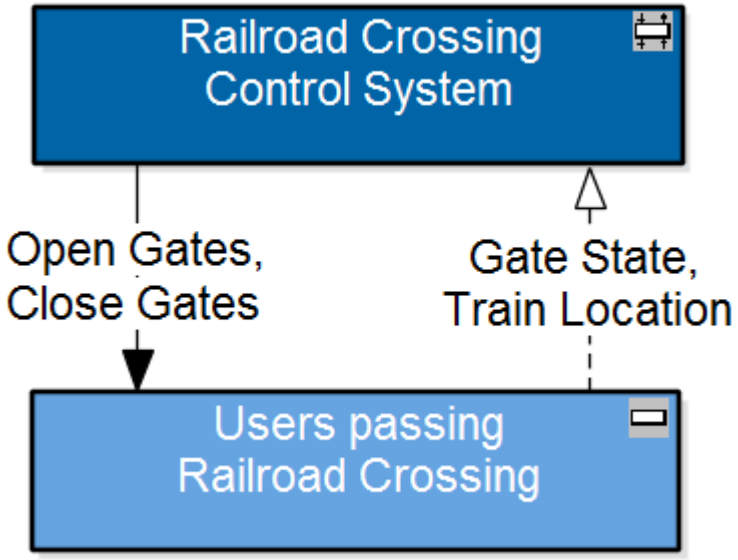
STPA Step 1 - Hierarchical Control Structure

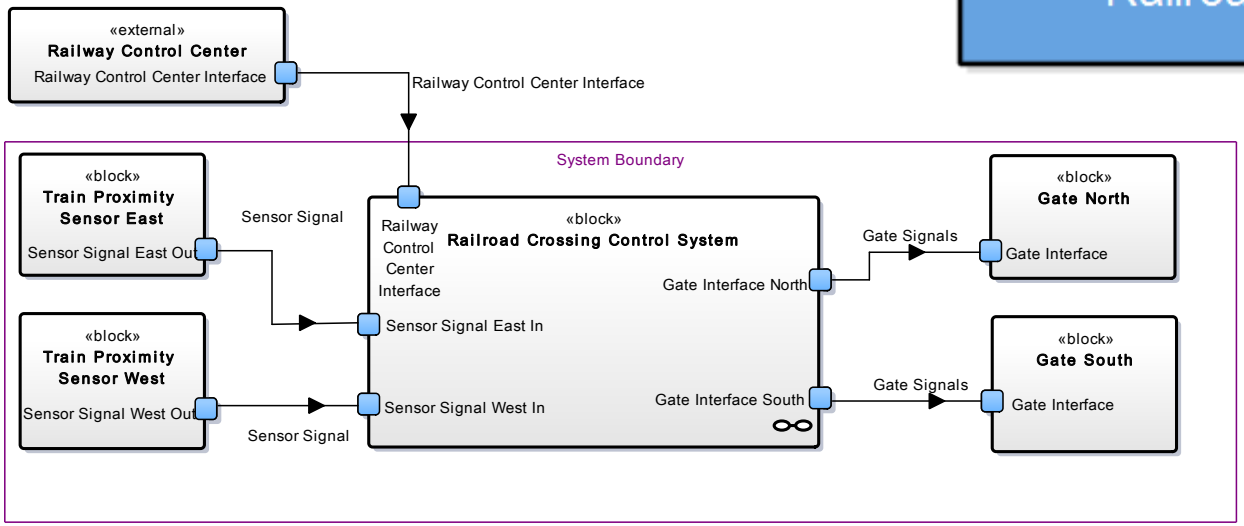
- Simple (?) Example



STPA Step 1 - Hierarchical Control Structure

- Simple (?) Example





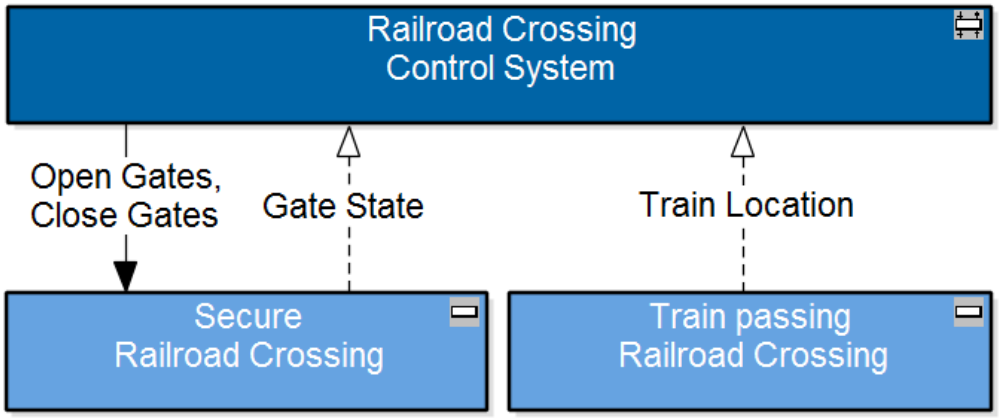
STPA Step 1 - Hierarchical Control Structure

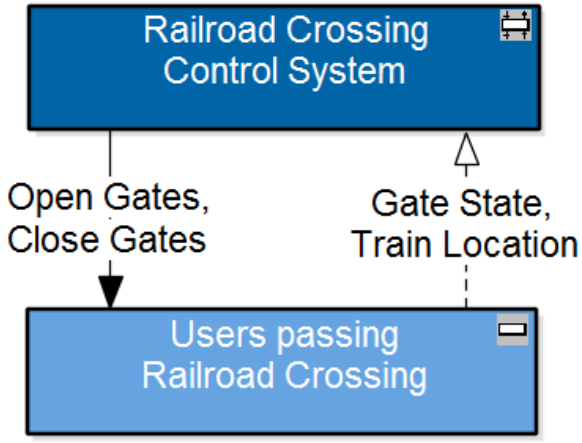
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

- This not so simple example illustrates some of the challenges
  - There is no unique “correct” HCS for a system
    - It’s a question of completeness and accuracy and of being more/less useful rather than right or wrong.

STPA Step 1 - Hierarchical Control Structure

- Which one is more useful???





- Hard to tell at this stage...

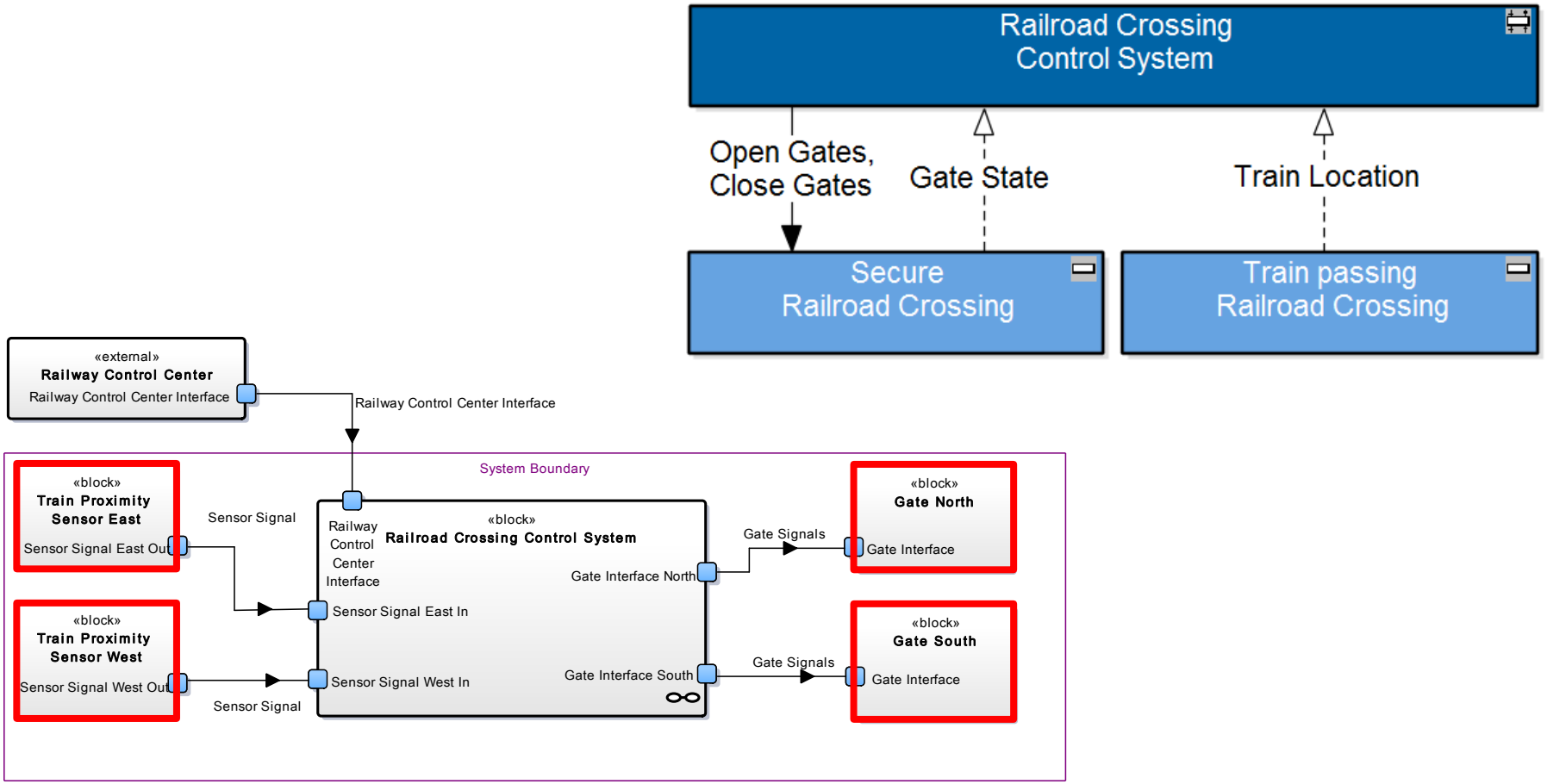
STPA Step 1 - Hierarchical Control Structure

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

- This not so simple example illustrates some of the challenges
  - There is no unique “correct” HCS for a system
    - It’s a question of completeness and accuracy and of being more/less useful rather than right or wrong.
  - Some pieces seem to be missing...

STPA Step 1 - Hierarchical Control Structure

- What about actuators and sensors?



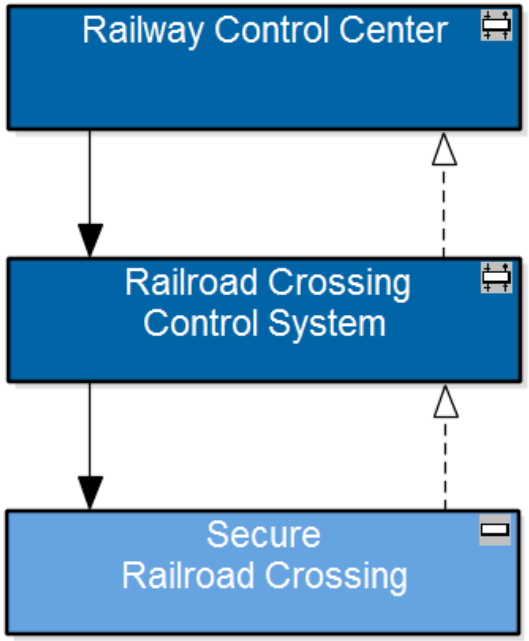
STPA Step 1 - Hierarchical Control Structure

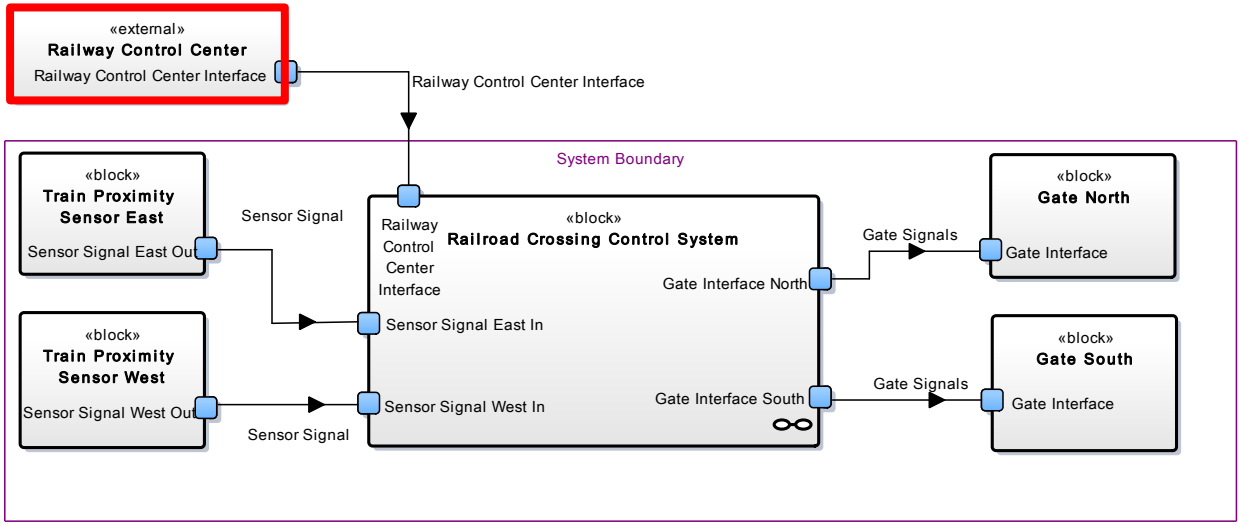
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

- This not so simple example illustrates some of the challenges
  - There is no unique “correct” HCS for a system
    - It’s a question of completeness and accuracy and of being more/less useful rather than right or wrong.
  - Some pieces seem to miss...
    - It is in general not very useful to have actuators and sensors on the HCS.
    - They are much better dealt with in Step 2.
    - Identifying what parts of a system really are “Controllers” in the sense of STPA is not always trivial.
- From our experience, we believe STPA to be a rather robust method.
  - It does not matter that much how your model “looks” like...
  - As long as you are complete and accurate, you will be lead to the critical questions at some point of another.

STPA Step 1 - Hierarchical Control Structure

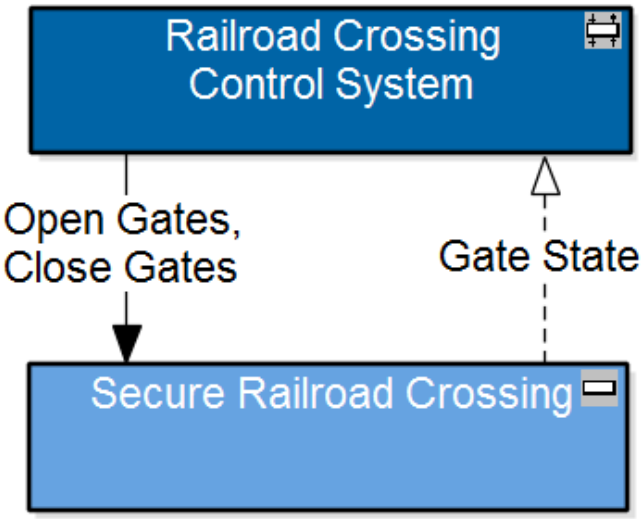
- Why *Hierarchical ?*
  - Typically, not one single controller, but a whole control hierarchy is in charge of the process.
  - The top one influences the process by means of it's subordinates.
  - It might have direct or only indirect feedback.





Step 1 - Identify Unsafe Control Actions

- Goal of Step 1: Identify potential for inadequate control of the system that could lead to hazards!
- Procedure illustrated by example
  - Select control action: Close Gates
  - Potential for inadequate control that could lead to hazard?
  - The intuitive way:
    - If gates are not closed when a train approaches, we might be in trouble.
    - If gates are closed too late when a train approaches, we might be in trouble.
    - ...
  - STPA formalizes and systematizes this by using a set of keywords.



Step 1 - Identify Unsafe Control Actions

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

- One possible way for the formulation of an UCA is:

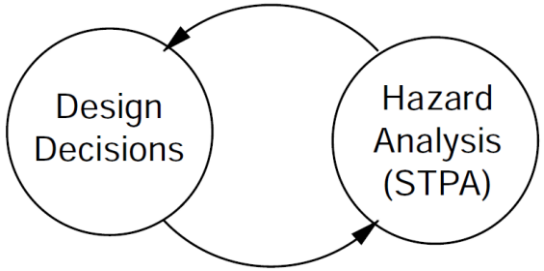
  If {*control action}* is {*keyword}* in {*context}* then {*hazard}.*

- One possible set of keywords is the following:

Keyword	UCA for CA Close Gates
... not provided when expected/required	If Close Gates is not provided when a train is approaching then we might have people or vehicles on the tracks that the train could collide with.
... provided when not expected/required	If Close Gates is provided when no train is approaching then we might cause a traffic jam and people getting very impatient.
... provided too early	...
... provided too late	If Close Gates is provided too late when a train is approaching then... *same as in first case.*
... stopped too soon	...
... applied too long	...

Step 1 - Impact of Findings

- If you are still in the design phase
  - Translate the identified hazardous behaviors into safety constraints or requirements and add those to the system requirements!
  - Example:
    - The system must ensure that the gates are closed early enough to avoid having people or vehicles on the track when the train crosses.



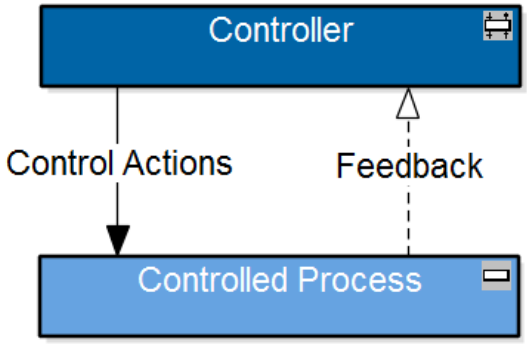
- If the system is already in operation
  - Check if the identified hazardous behaviors are covered by the system design, i.e. existing safety constraints... and by its implementation!

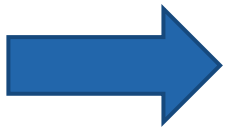
STPA in a Nutshell

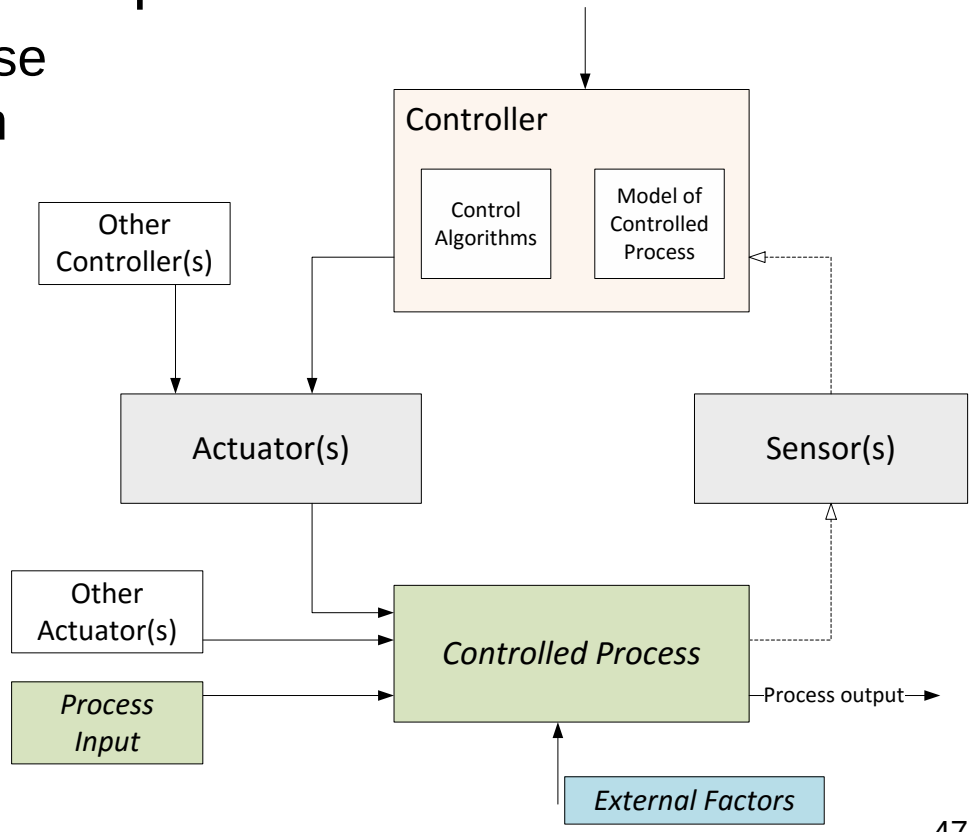
STPA Step 2

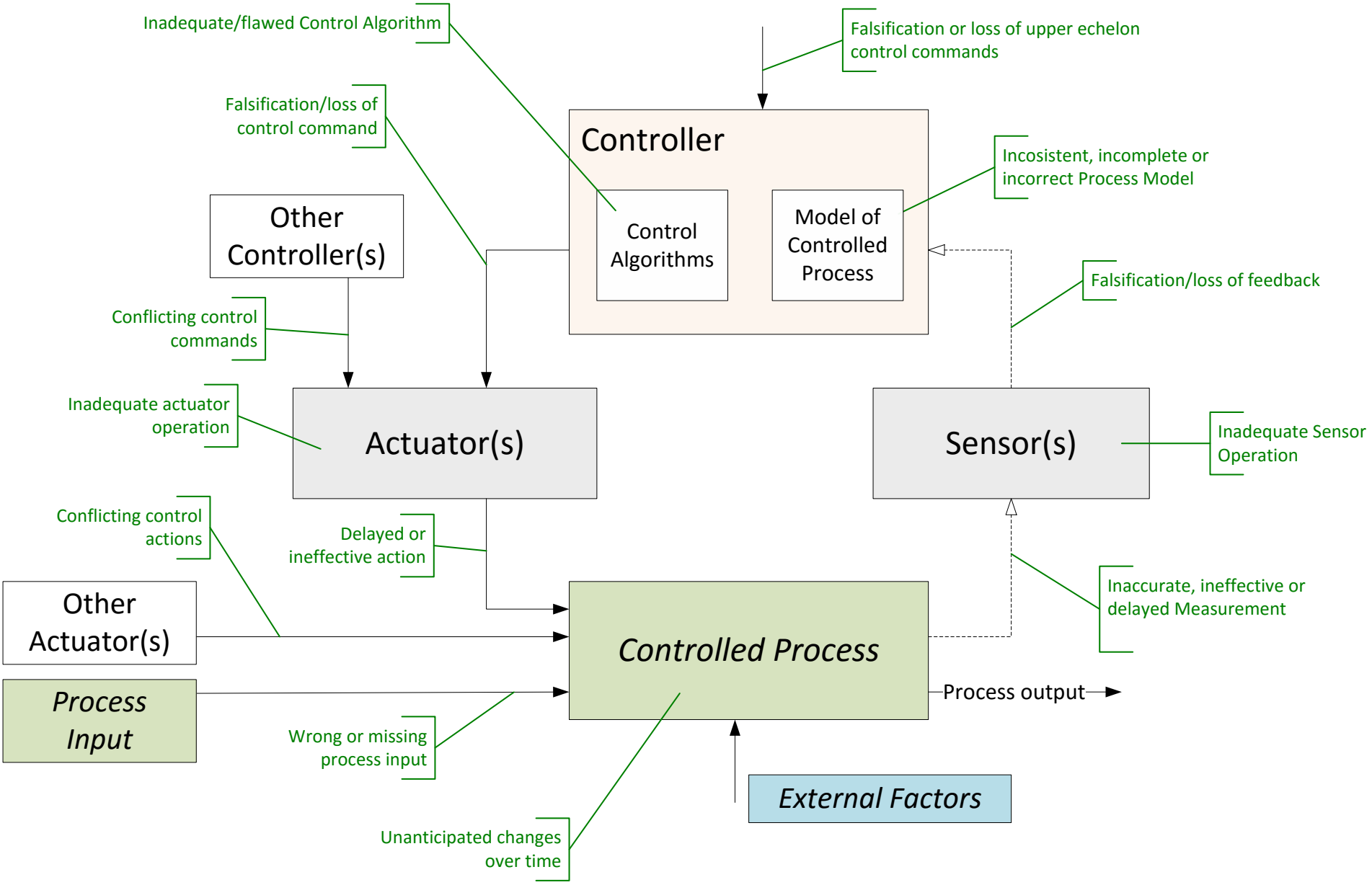
Step 2 - Control Loops

- Goal of Step 2 is to determine how each of the UCA identified in Step 1 could occur.
- Step 2 supported by Control-Loop view
  - Detailed representation of those parts of the system involved in the UCA being analyzed.
  - Causal Analysis guided by checklist.








Inadequate/flawed Control Algorithm
Falsification or loss of upper echelon control commands
Falsification/loss of control command
Controller
Incosistent, incomplete or incorrect Process Model
Other Controller(s)
Control Algorithms
Model of Controlled Process
Falsification/loss of feedback
Conflicting control commands
Inadequate actuator operation
Actuator(s)
Sensor(s)
Inadequate Sensor Operation
Conflicting control actions
Delayed or ineffective action
Inaccurate, ineffective or delayed Measurement
Other Actuator(s)
Controlled Process
Process Input
Process output
Wrong or missing process input
External Factors
Unanticipated changes over time

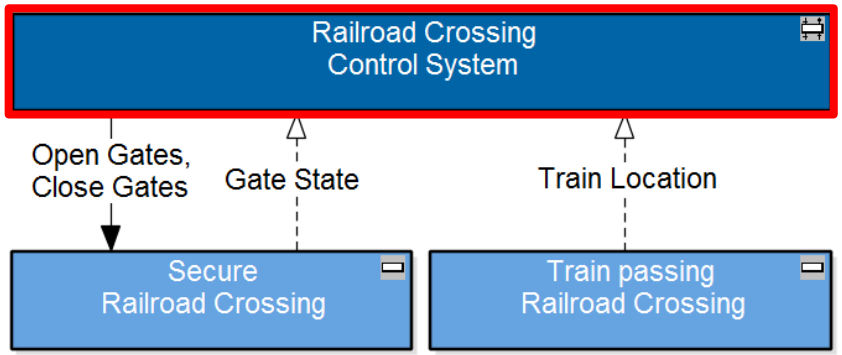
Step 2 - Example (Simplified)

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

- In Step 1 we identified the following UCA

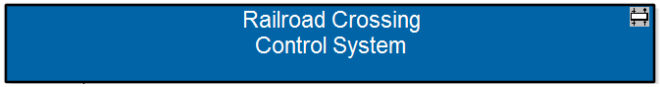
  If *Close Gates* is *not provided when a train is approaching* then we might have people or vehicles on the tracks that the train could collide with.

- The first activity in Step 2 is to build the Control-Loop for that UCA.
- Identify the controller responsible for the UCA



Step 2 - Example (Simplified)

- Isolate the control algorithm part of that controller that is specific to the Control Action.

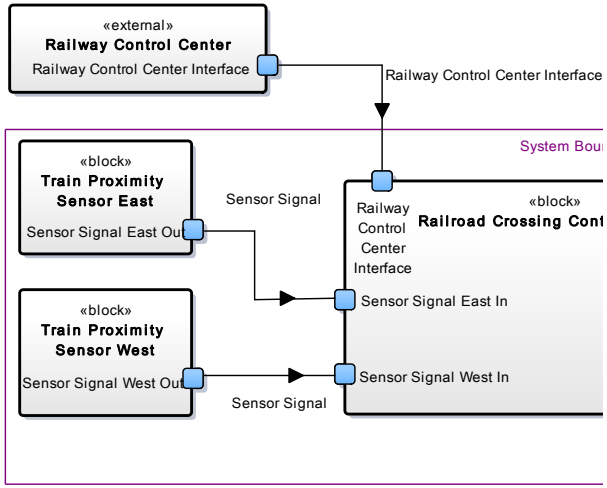


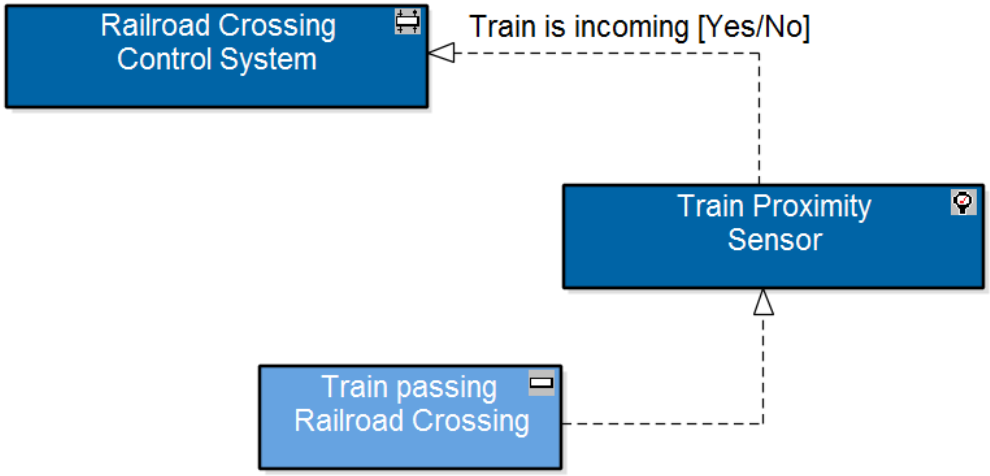
  - Describe it in plain Text or some kind of pseudo-code. For example: *If a train is incoming then close the gates.*
- Identify what process model variables are needed in this algorithm.
  - Analyze the algorithm: *If a train is incoming then close the gates.*
  - Define process model variable: Train is incoming [Yes/No]
- Identify the sensors “feeding” the required process model variables.
  - They will generally NOT be on the HCS!
  - You have to go back to the Design Documentation to identify them.

Step 2 - Example (Simplified)

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

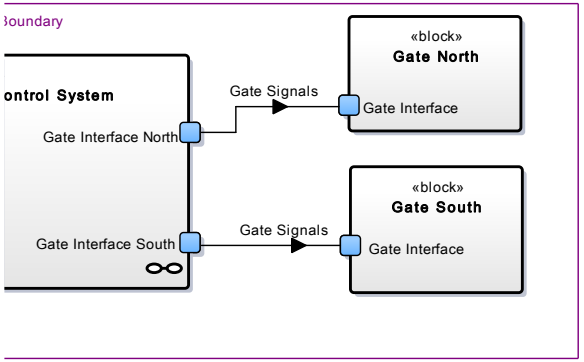
- Identify the sensors “feeding” the required process model variables.
  - The design features Train Proximity Sensors.
    - Add them to the Control-Loop.
    - Link the sensor to the process it is observing.

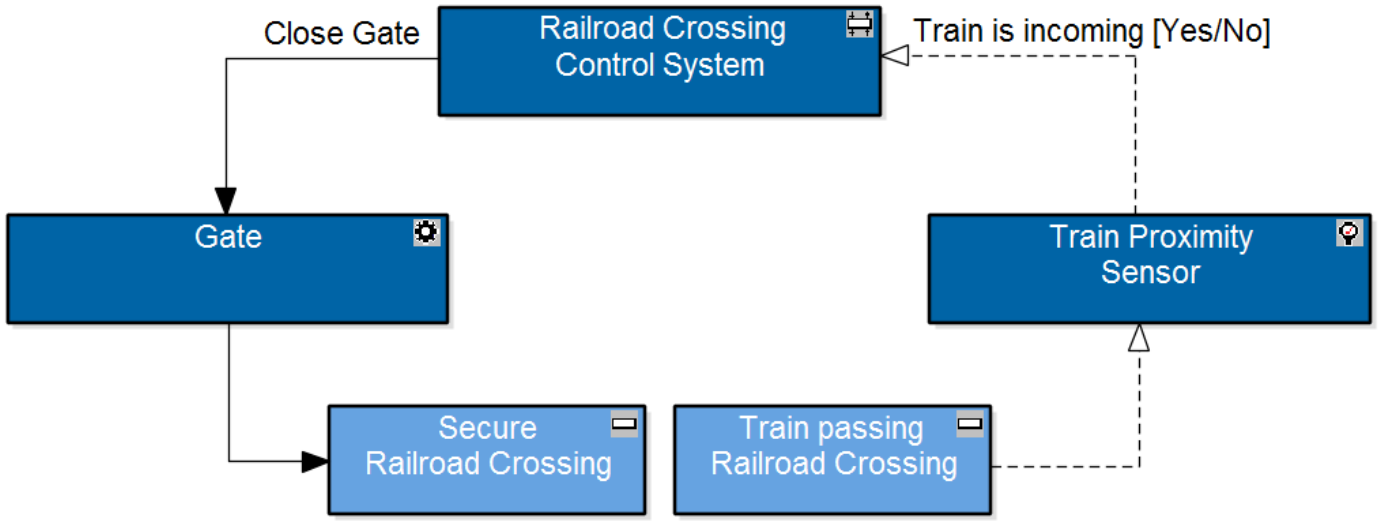




Step 2 - Example (Simplified)

- Identify the actuators that “realize” the control action.
  - The design features Gates.
    - Add them to the loop, including the process(es) they act on.

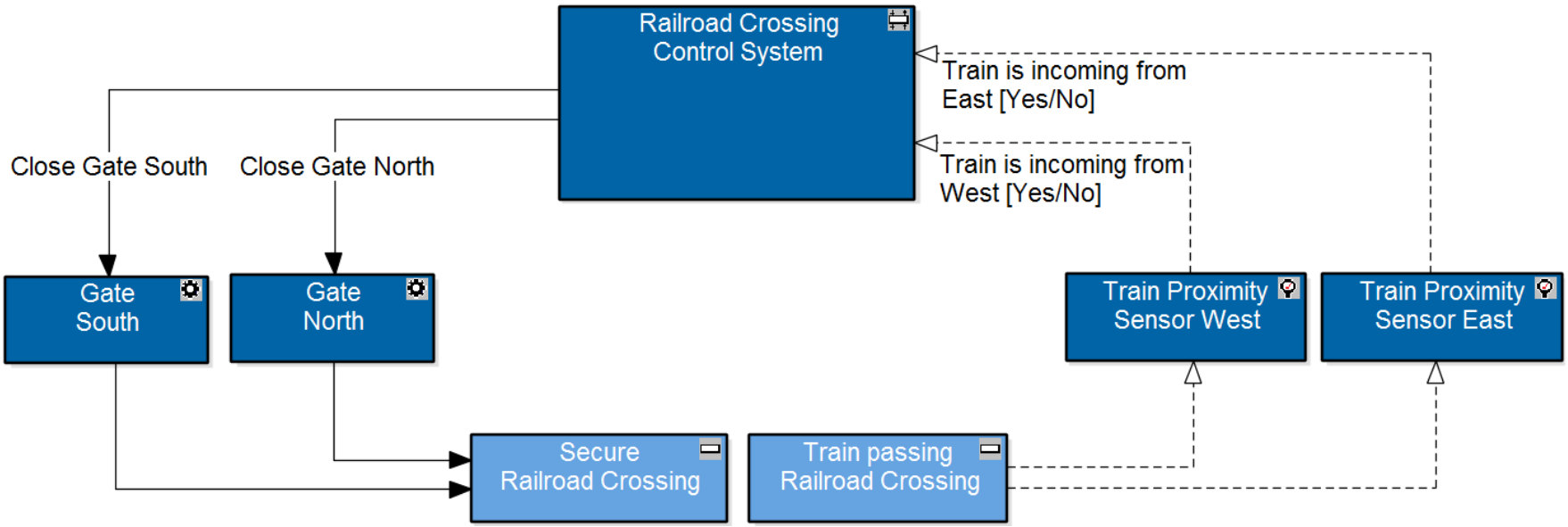




Step 2 - Example (Simplified)

- Again, there is not one unique “correct” Control-Loop.
  - The focus should again be on completeness and accuracy.

If *train is incoming from west* or *train is incoming from east* then ***close gate north*** and ***close gate south***.



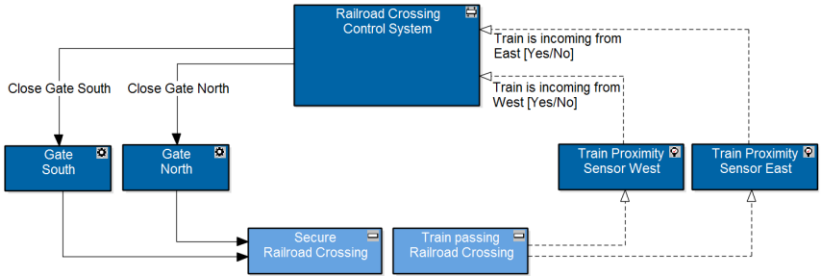
Comments on Step 2

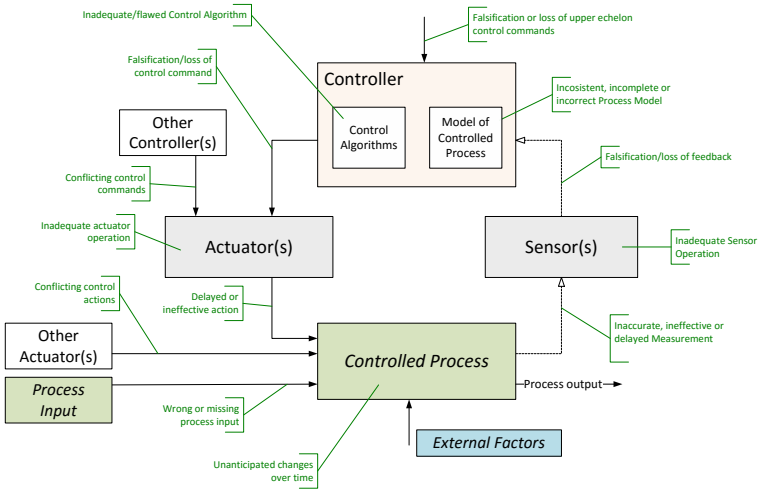
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

- The Control-Loop is generally not at such an abstract level as the HCS.
  - On the HCS we just put “Close Gates”, on the Control-Loop this reappeared as a set of commands {Close Gates North, Close Gates South}.
  - There are ways to directly link the control loop to the physical system realization, but this is out of the scope of this introduction.
- Rather than trying to enforce a rigid set of rules while doing STPA, think about your primary goal.
  - Supporting the analyst in a systematic way to most efficiently *see* and *document hazards* and their *causal factors*, and to propose ways to *improve safety*.
- But, whatever you do, do not loose traceability!

Identifying Causal Factors and Scenarios

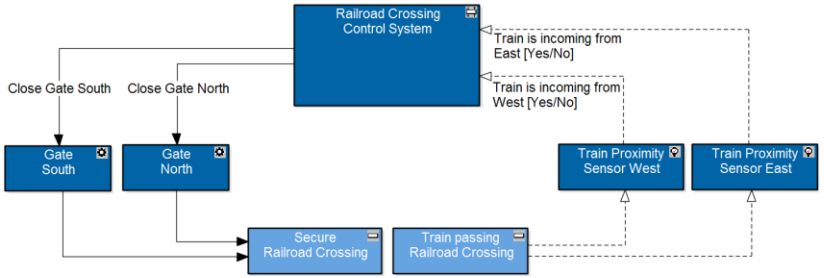
- Start with the analysis at the Controller level.
  - What could cause the controller not to close the gates when there is an incoming train?
  - Flaw in the algorithm?
  - Issue with the process model?
    - Incorrect process model?
      - Process model did not get updated?
        - Loss of signal from sensor?
        - Sensor is broken?
        - Sensor has moved on the tracks?

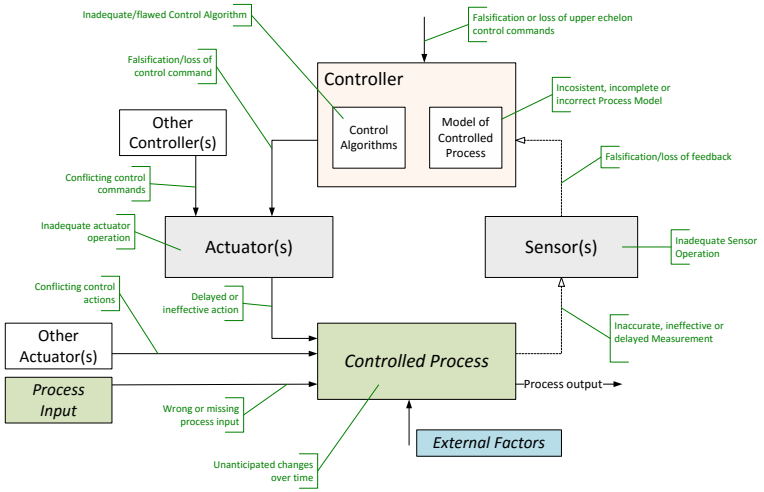




Identifying Causal Factors and Scenarios

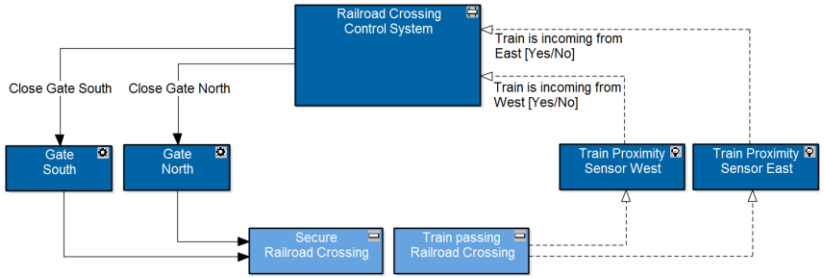
- On the other side, think about what could have the same effect as “Controller does not issue Close Gates”?
  - Command is lost on way to gates?
  - Gates are not working properly?
  - Something on the road prevents the gates from closing?



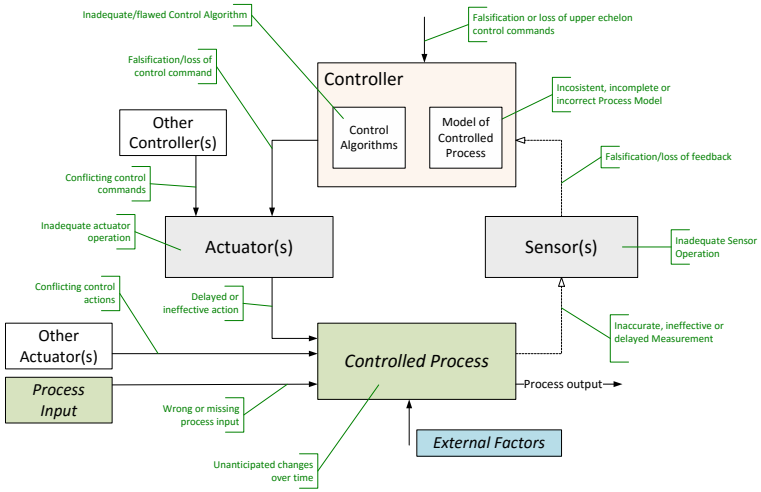


Identifying Causal Factors and Scenarios

- Last, take a step back and look at the whole.
  - What happens when only one gate is closing and the other is not?
  - Hmmm... how are the gates built anyway? Full gates or half gates?

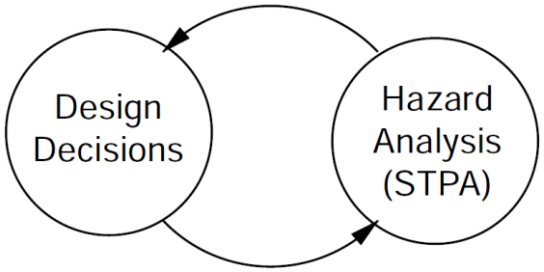


- You might get inspired to go back to the designers and ask them for more details!
  - Do not forget to update the HCS if needed...



Step 2 - Impact of Findings

- If you are still in the design phase
  - Refine/Extend the Safety Constraints/Requirements.
  - Augment the basic system design to eliminate causal factors.
  - Add control and mitigation measures to contain the effects of causal factors.



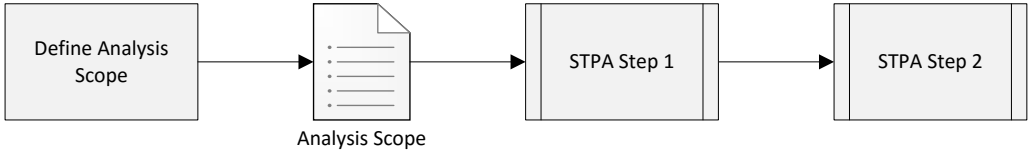
- If the system is already in operation
  - Check if the identified causal factors are appropriately managed by the system design and safety constraints... and its implementation!
  - Scenarios and causal factors identified by Step 2 might be good inputs for system tests!

Introduction to STPA

STPA Process Overview

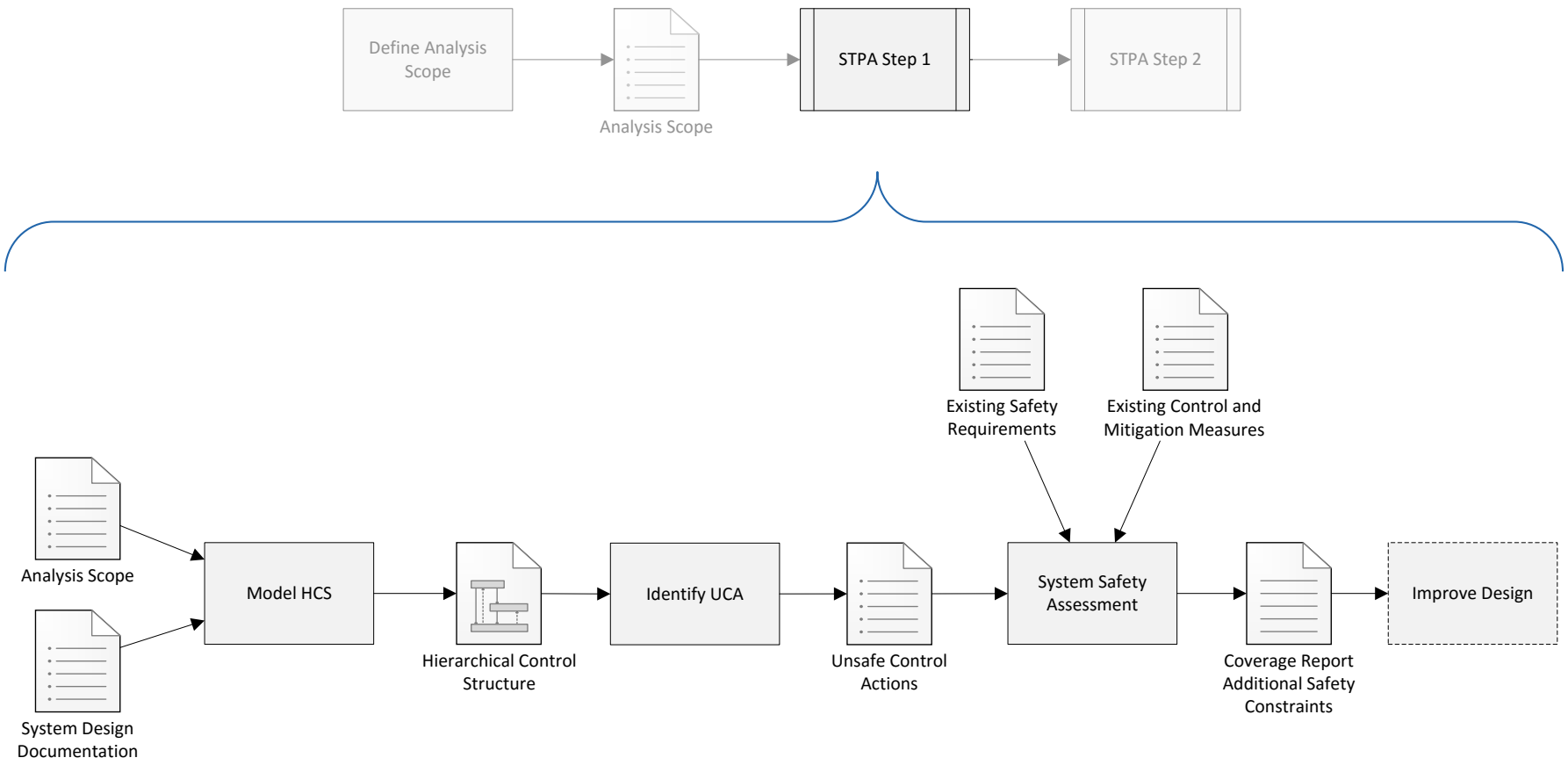
STPA - The whole Process

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



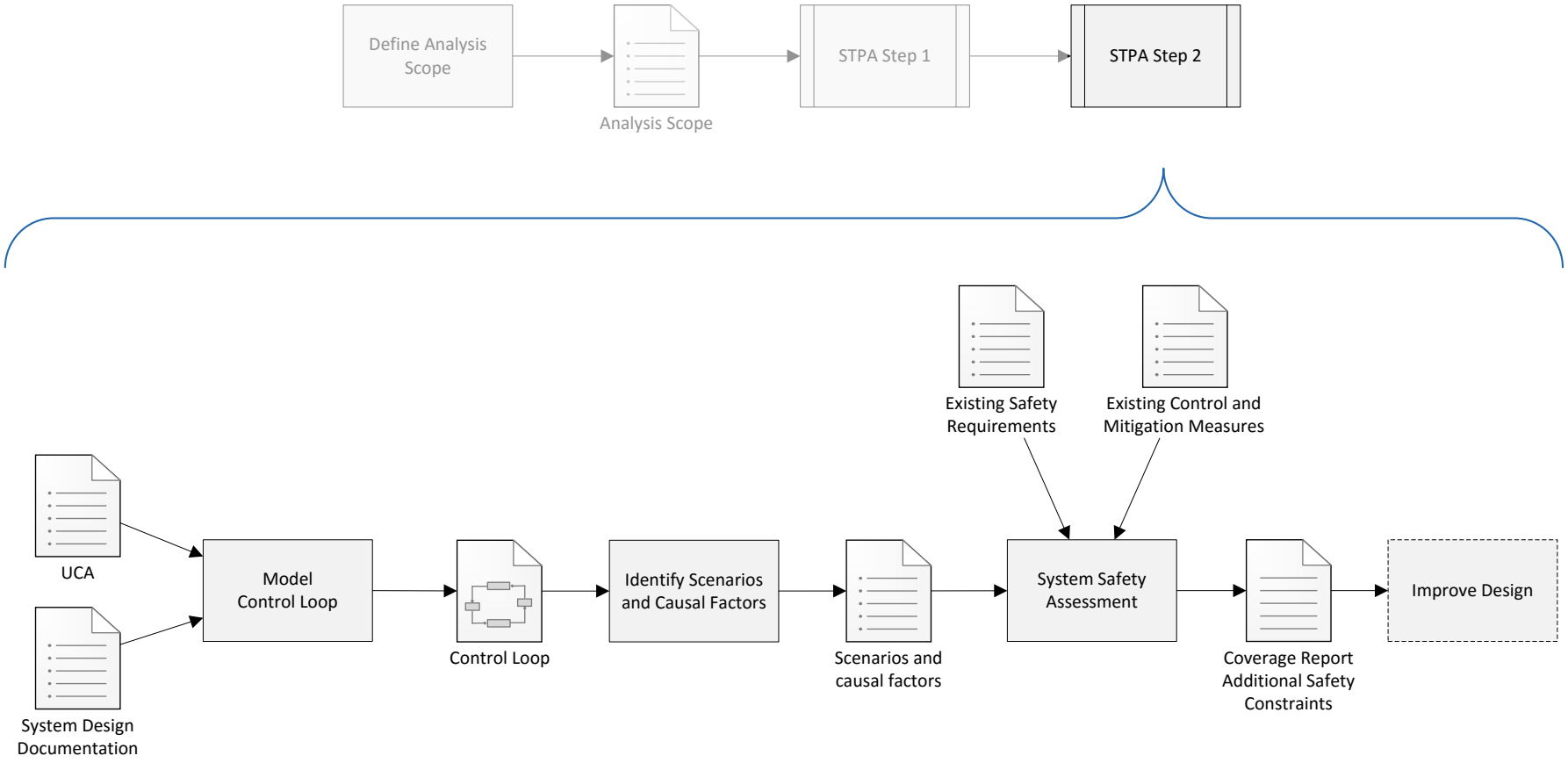
STPA - The whole Process

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



STPA - The whole Process

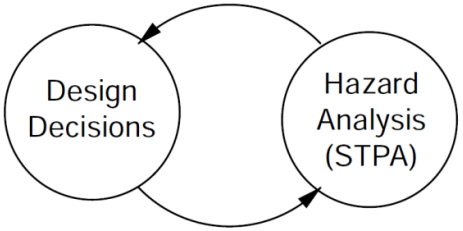
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics



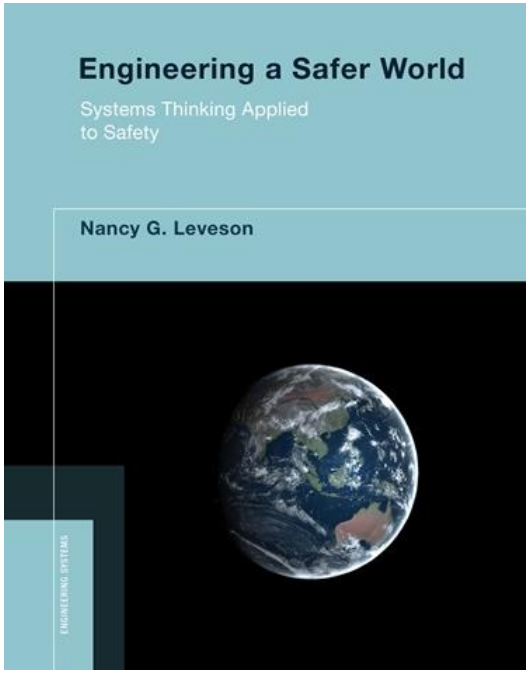
The best way to go: Safety Guided Design

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

- *Engineering a Safer World*, Chapter 9: Safety-Guided Design



Iterate over the process until all hazardous scenarios are eliminated, mitigated or controlled.



- The whole approach perfectly fits into any ISO31000 compliant risk management process (e.g. ISO12100, ISO14971).

Engineering a Safer World, free download at https://mitpress.mit.edu/books/engineering-safer-world

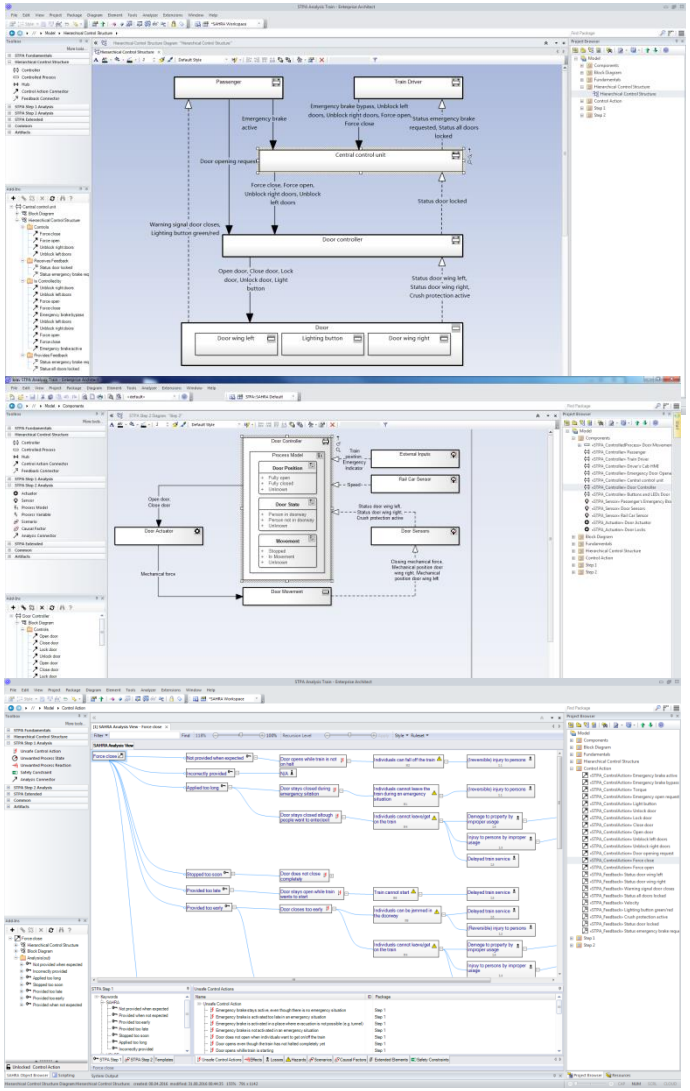
Tool Support for Safety Guided Design

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

SAHRA
STPA based hazard and risk analysis

Contact: Sven Stefan Krauss
svenstefan.krauss@zhaw.ch

http://www.sahra.ch



SAHRA Key Features

- Extension for Sparx Systems Enterprise Architect.
- Perform STPA together with requirements and design activities in same UML/SysML CASE tool.

SAHRA STPA Profile

- The STPA Profile provides the STPA diagram types, all needed elements in toolboxes, query and document export templates.

SAHRA Object Brower

- Context-sensitive object browser provides traceability information and supports efficient editing during modeling and analysis.

SAHRA Analysis Editor

- The analysis editor allows doing STPA Step 1 and Step 2 analysis in an innovative way using mind maps for analysis visualization and drag and drop support for easy editing.

Contact Persons in our Team at ZHAW

Zurich University of Applied Sciences

School of Engineering

IAMP Institute of Applied Mathematics and Physics

Sven Stefan Krauss

- Dipl. Inf. FH Computer Engineering
- Functional Safety with focus on Machinery and Process Sectors
- STPA Tool Support

svenstefan.krauss@zhaw.ch

Martin Rejzek

- Dipl. Ing. FH Electrical Engineering
- Functional Safety, Medical Products Safety
- STPA Methodology

martin.rejzek@zhaw.ch

Dr. Monika Reif

- Dipl. Ing. Mechanical Engineering, PhD Reliability Engineering
- Complex Systems Reliability and Safety Modelling
- Functional Safety with focus on Automotive and Railway Sectors

monika.reif@zhaw.ch

Dr. Karl Lermer

- Dipl. and PhD Mathematics
- Mathematical Reliability and Safety Modelling
- Formal Verification Methodology

karl.lermer@zhaw.ch

Contact:

Christian Hilbes
christian.hilbes@zhaw.ch

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