Zurich University
of Applied Sciences

zh
aw

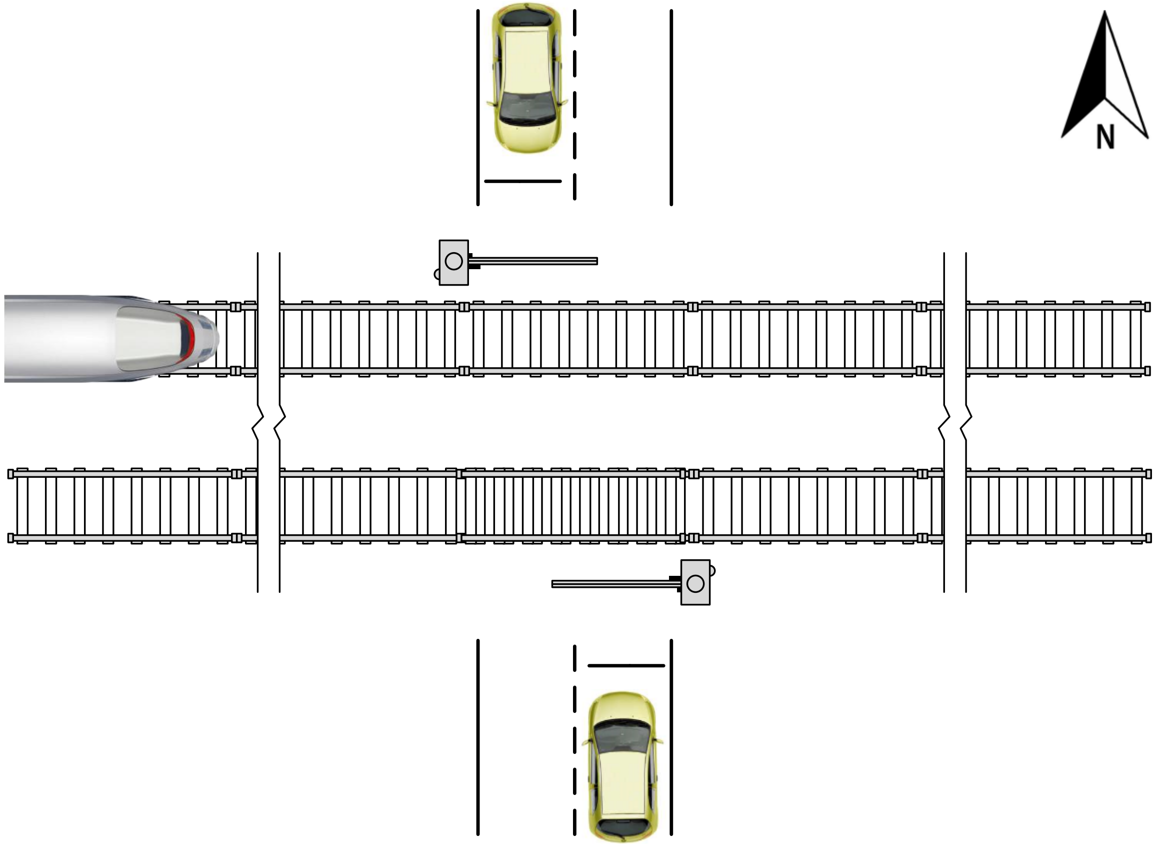
School of
Engineering

IAMP Institute of Applied
Mathematics and Physics

4th European STAMP Workshop 2016

STPA Tutorial - Part 3

Tutorial Example - Railroad Crossing



- 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 - Current State

- Previous group Activity gave some insight in
  - Construction of HCS
  - Identification of UCA
  - Specification of Safety Constraints/Requirements.

- Next is STPA Step 2
  - Identification of causal factors and scenarios that can lead to an UCA.
  - Refinement/Extension of Safety Constraints/Requirements.

Picture by Christian Hilbes

Picture by Christian Hilbes

Group Activity - STPA Step 2

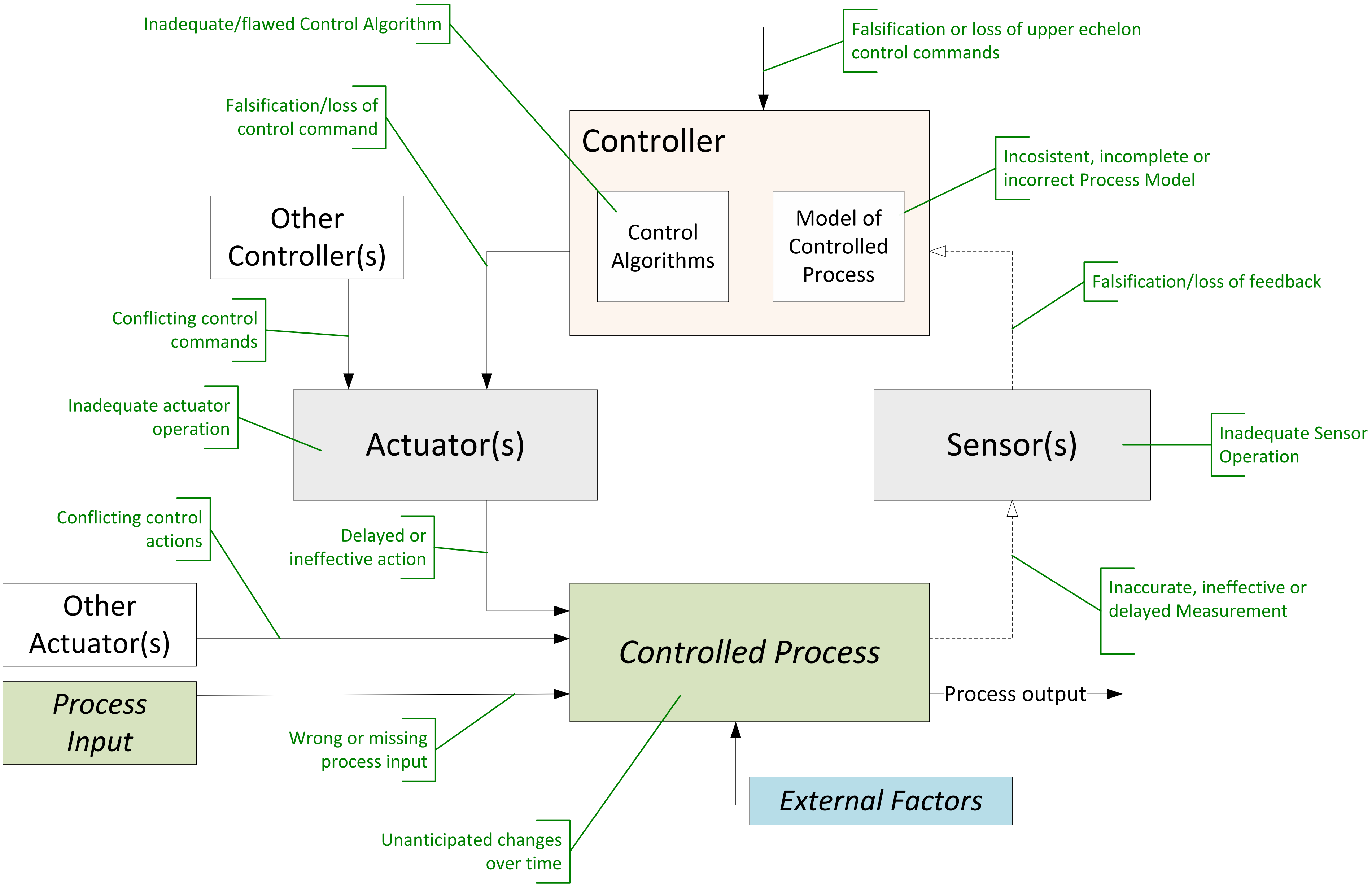
- Select an UCA from the list you compiled in the previous activity and that directly acts on the process.
- Construct the Control Loop for that UCA by proceeding as follows:
  - Identify the controller issuing the associated CA.
  - Isolate the parts of the control algorithm that are specific to that CA (best is to describe in natural language or some kind of pseudo-code)
  - Identify process model variables needed as input by the control algorithm part.
  - Identify the "Sensors" (and related processes) that provide the required information to the controller. Add them to the loop.
  - Identify the "Actuators" that "realize" the CA and complete the loop.

  - Use the Flipcharts to capture your Control Loop(s).

Group Activity - STPA Step 2

- Once the Control Loop is ready, start with the causal analysis.
- Proceed as follows:
  - Start with the Controller.
    - A good starting point is to look at the control algorithm.
    - Are there flaws in the control algorithm? Issues with the process model?
    - Ask yourself what could “convince” the controller to issue the UCA.
  - Traverse the Control Loop in the correct sense to follow the line of thoughts of that last question.
  - Figure out what could lead to the same effect at the process level, even if the controller does not issue the UCA itself.
  - Last, take a step back and look at the whole thing. Any complex scenarios?

  - Document your analysis using the template sheets.

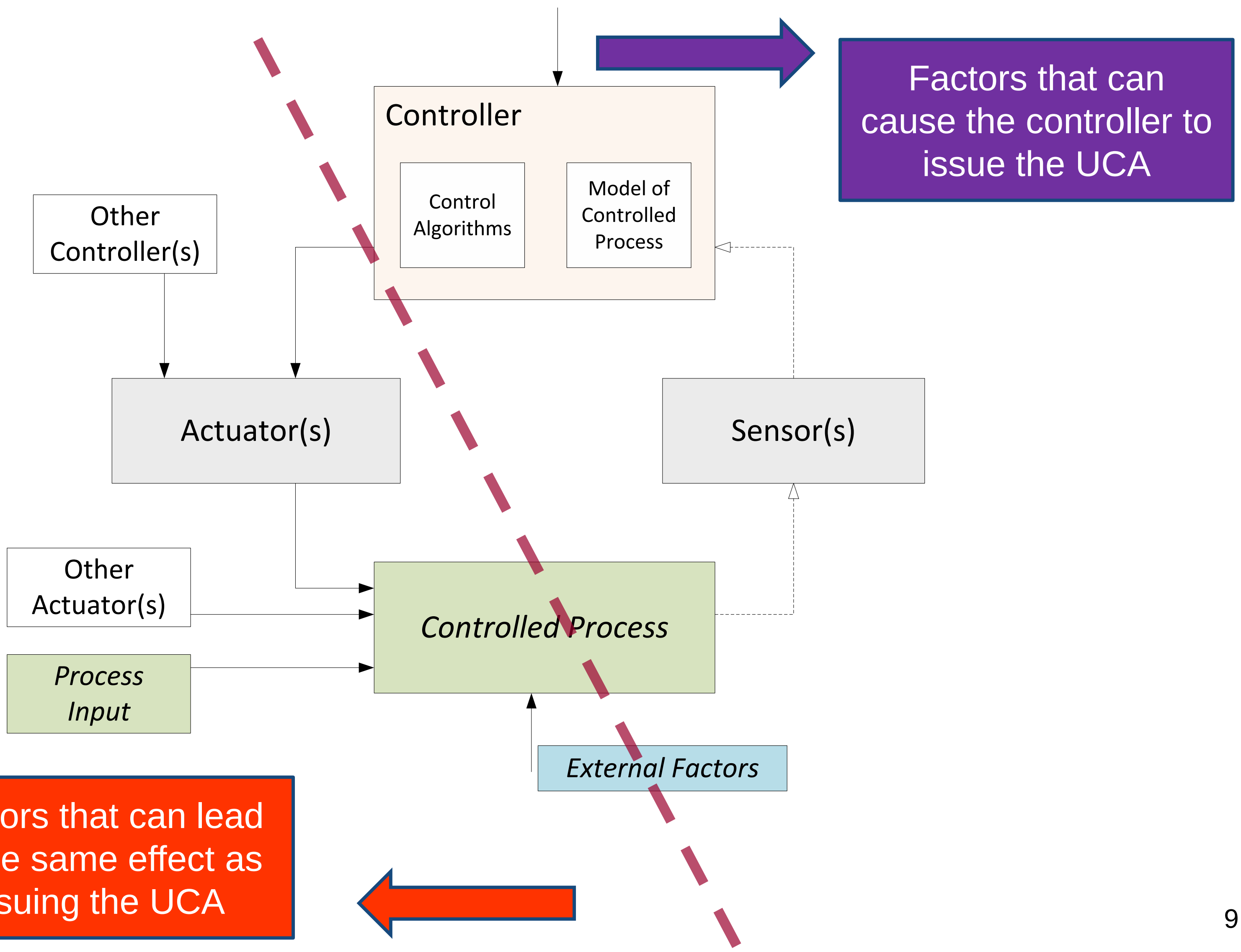

Inadequate/flawed Control Algorithm
Falsification or loss of upper echelon control commands
Falsification/loss of control command
Controller
Incosistent, incomplete or incorrect Process Model
Other Controller(s)
Control Algorithms
Model of Controlled Process
Falsification/loss of feedback
Conflicting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

Group Activity - STPA Step 2

- Discuss the following questions:
  - Where could existing FTA or FMEA analyses be of use in this step?
  - What about Control-Loop reuse (for other UCA).
  - How large do you judge the effort to conduct an STPA in comparison to other methods like FMEA and FTA.
  - Is it necessary to fully complete Step 1 before starting with Step 2?

- Time for this activity: rest of the tutorial time... minus 10 minutes for last comments.

Control Loop Structure



Factors that can cause the controller to issue the UCA

Factors that can lead to the same effect as issuing the UCA

A few final Comments

- Many more things to cover... but not in that short time.
- You need some experience to fully grasp STPA.
  - We are still learning a lot!
- Where could existing FTA or FMEA analyses be of use in this step?
  - In principle wherever a readily existing analysis answers one of the questions raised in the STPA process, it can be “plugged-in”.
  - STPA as a “framework” allows to put existing low-level analyses in a common context.
- Is it necessary to fully complete Step 1 before starting with Step 2?
  - “Drill-Down” is possible at any time.
    - You can switch from Step 1 to Step 2 at any point you deem necessary.
    - Quite straightforward to follow prioritized questions from top to bottom.

A few final Comments

- STPA seems to be a very “expensive” method...
  - Seriously analyzing complex systems is not a trivial task.
  - Need to compare with the effort to do an FMEA or FTA with the same level of completeness and systematics!
  - FMEA and FTA are generic “techniques”. Their application needs to be defined in a SOP. This comes at a cost.
    - The risk of missing or misunderstanding something is much bigger, compared to the structured and guided approach of STPA.
  - The basis for an STPA is well documented in diagrammatic form.
    - Much easier to maintain the analysis after system changes.

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

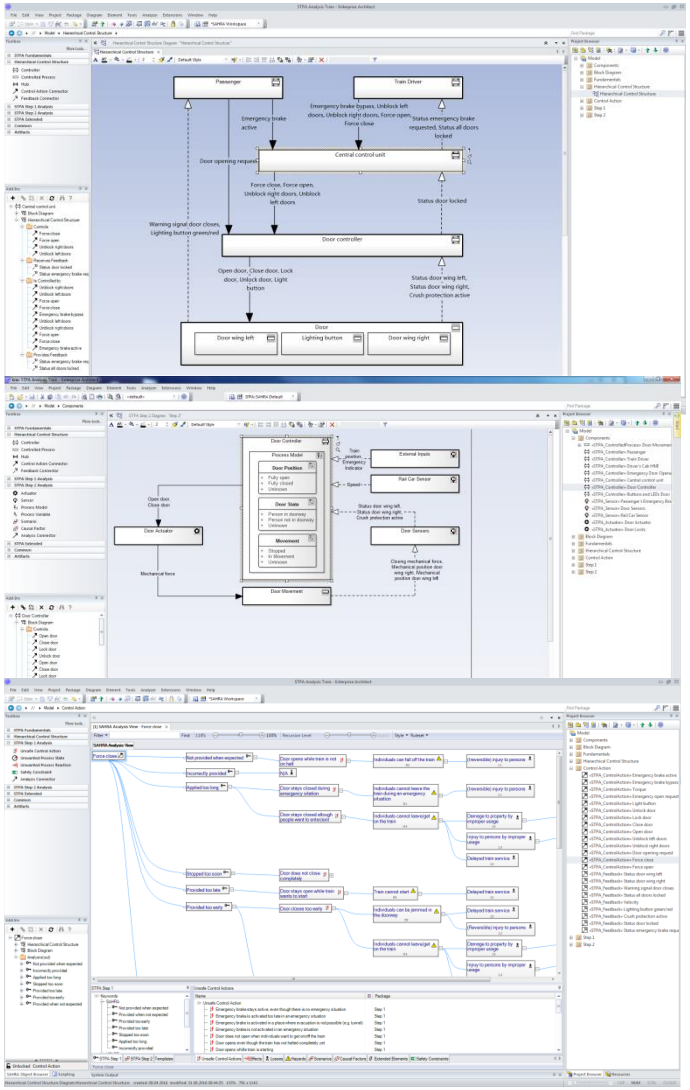
- The STPA Profile provides the STPA diagram types, all needed elements in toolboxes, query and document export templates.

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.



Sparx Systems, Sparx Systems Logo, Enterprise Architect are registered trademarks of Sparx Systems Ltd., Creswick, Australia

Picture by Christian Hilbes

Contact:

Christian Hilbes
christian.hilbes@zhaw.ch

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