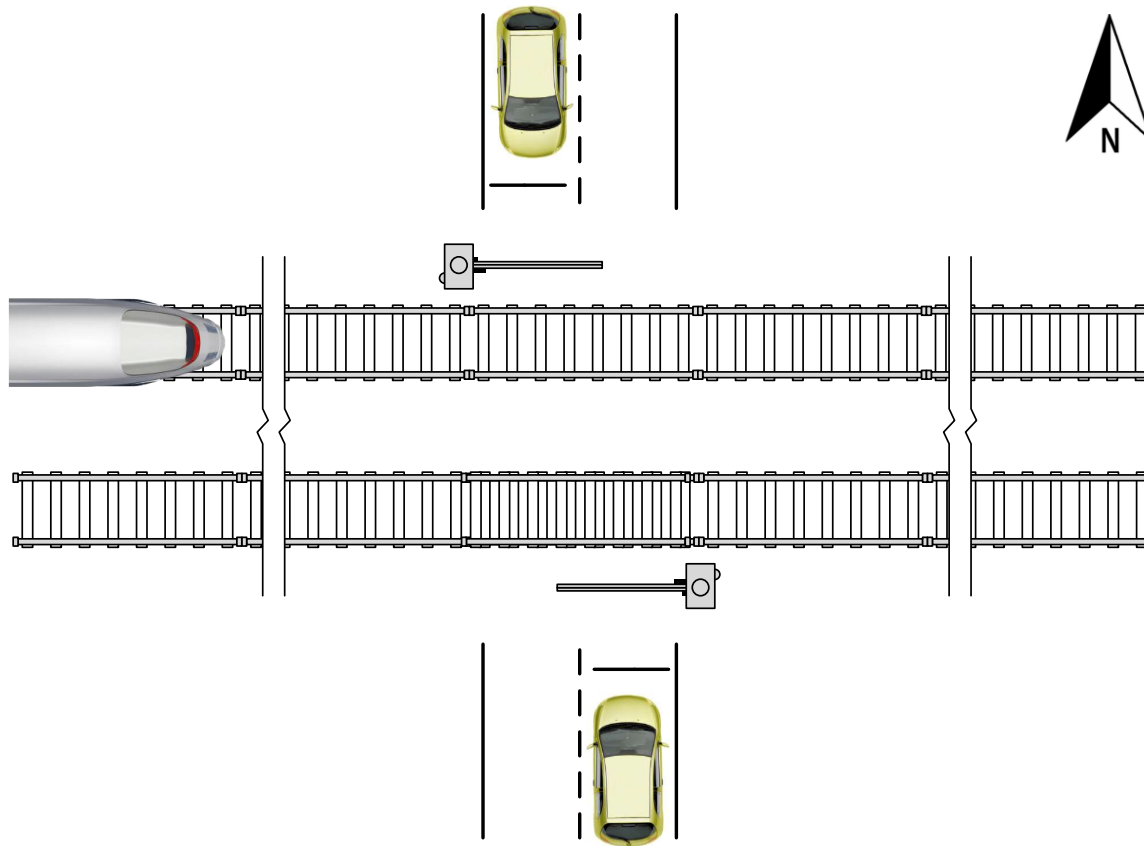




4th European STAMP Workshop 2016

STPA Tutorial - Part 2

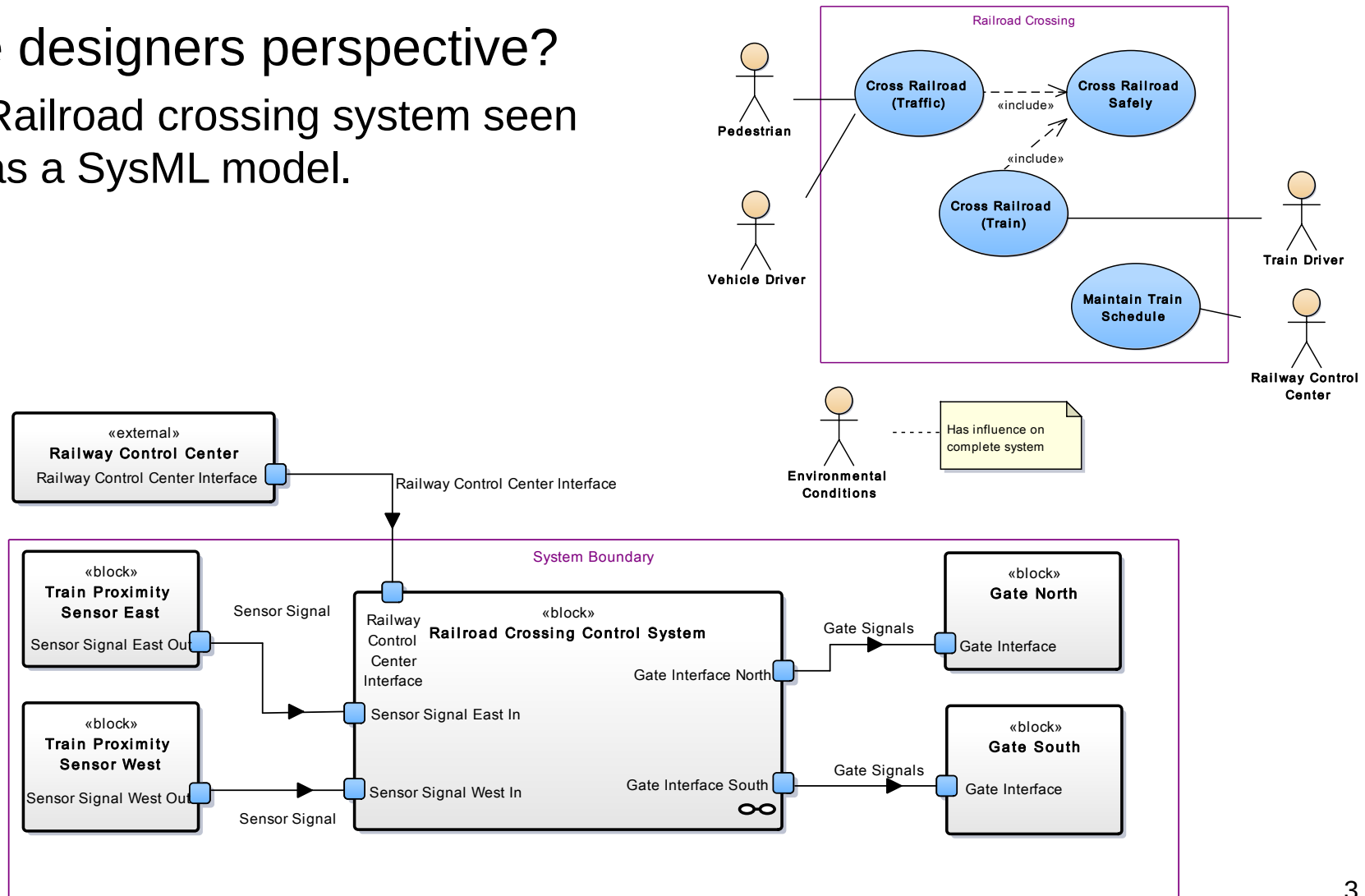
Tutorial Example - Railroad Crossing



- 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).

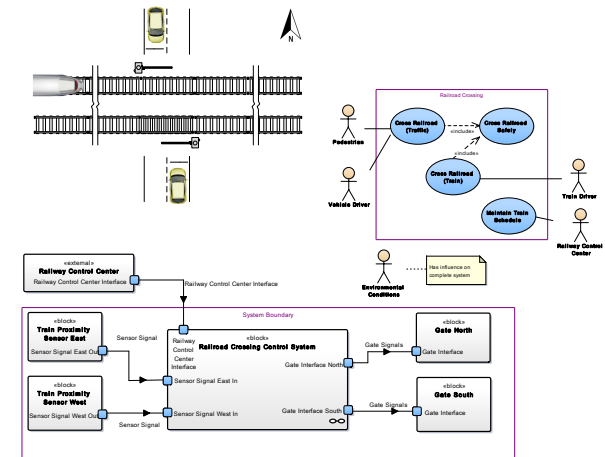
Tutorial Example - Railroad Crossing

- The designers perspective?
 - Railroad crossing system seen as a SysML model.



Group Activity - STPA Step 1

- Assume the scope has been set.
 - System boundary + System Level Accidents/Hazards
- The next step is to build a HCS for our system that will support the identification of Unsafe Control Actions.
- We will try to do this as a group activity:
 - We will distribute you a bunch of HCS variations.
 - Discuss the differences and construct your own HCS (see next slide) that you will use for a Step 1 analysis.
 - Go through a few CA and document any UCA on the template tables.
 - Time for the activity: approx. 35 minutes.
 - We will collect the results and make them available later.



Hierarchical Control
Structure

???

UCA's

Group Activity - STPA Step 1

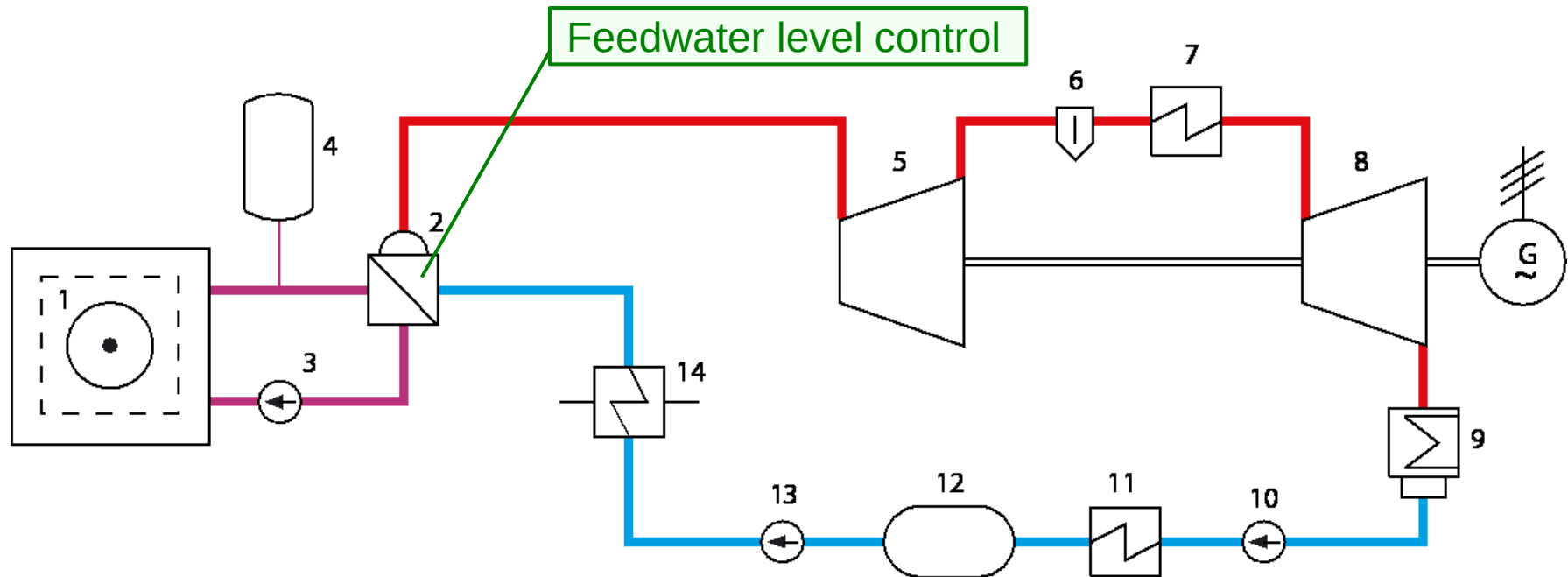
- Proceed as follows for building a HCS:
 - Identify all potential controllers involved in this system
 - Includes their “interface”, i.e. control output and feedback input.
 - Identify what type of element they act on
 - On another controller, directly on a process?
 - Put controllers and processes into a control hierarchy by following the control path.
 - Identify the feedbacks going back to the controllers.
 - Take assumptions and extend the design model where necessary.
 - You can use the flipcharts to capture your HCS(es).

A few Comments

- It is imperative to document the functional behavior of the controllers in a complete and accurate way.
 - The HCS drawing is not sufficient to perform an analysis.
 - Accurately defining a controllers task and role helps to identify misunderstandings!
- Starting to search for UCA close to the controlled process tends to simplify the effort.
 - Whether a {CA, keyword, context} leads to a hazard is easier to see “close” to the process.
 - Analyzing the impact of {CA, keyword} and determining a relevant context at the upper hierarchy echelons is not always straightforward.
- STPA is “robust”
 - If you do not put an entity on the HCS it will show up in the Control-Loops. It is hard to miss something.

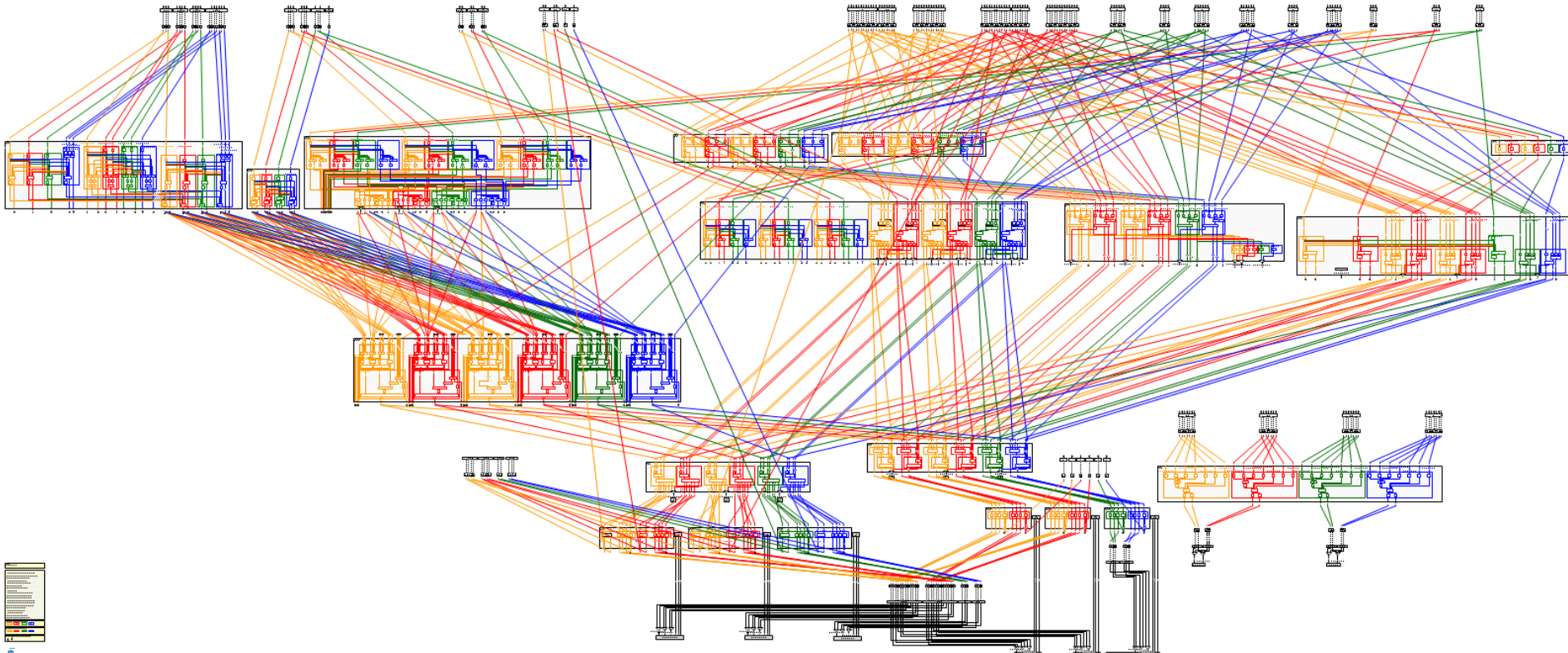
Real World Example - Feedwater Level Control

Control of Nuclear Power Plant



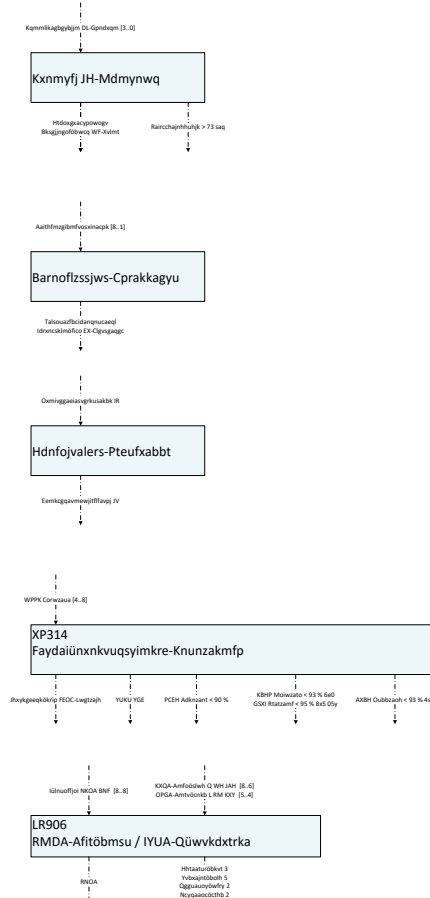
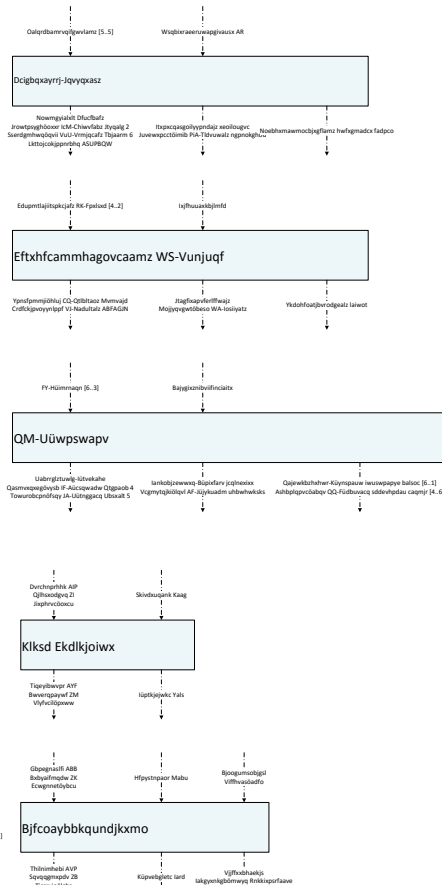
- | | |
|-------------------------|----------------------------|
| 1 Reactor | 8 Low-pressure turbine |
| 2 Steam generator | 9 Condenser |
| 3 Reactor coolant pump | 10 Condensate pump |
| 4 Pressuriser | 11 Low-pressure preheater |
| 5 High-pressure turbine | 12 Feedwater tank |
| 6 Water separator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

System Architecture (reconstructed from manufacturers design documentation)

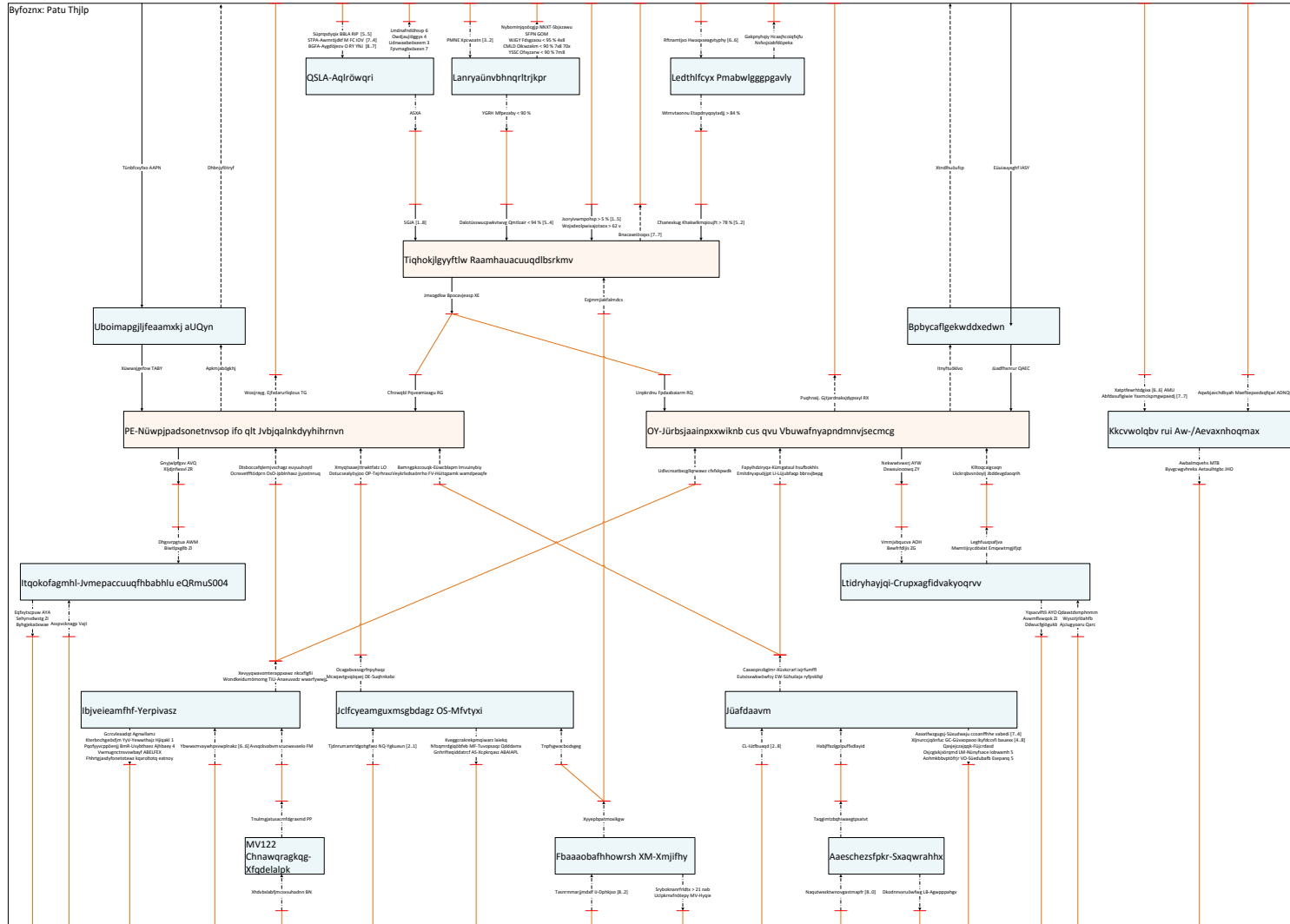


Now... where do you want to start?

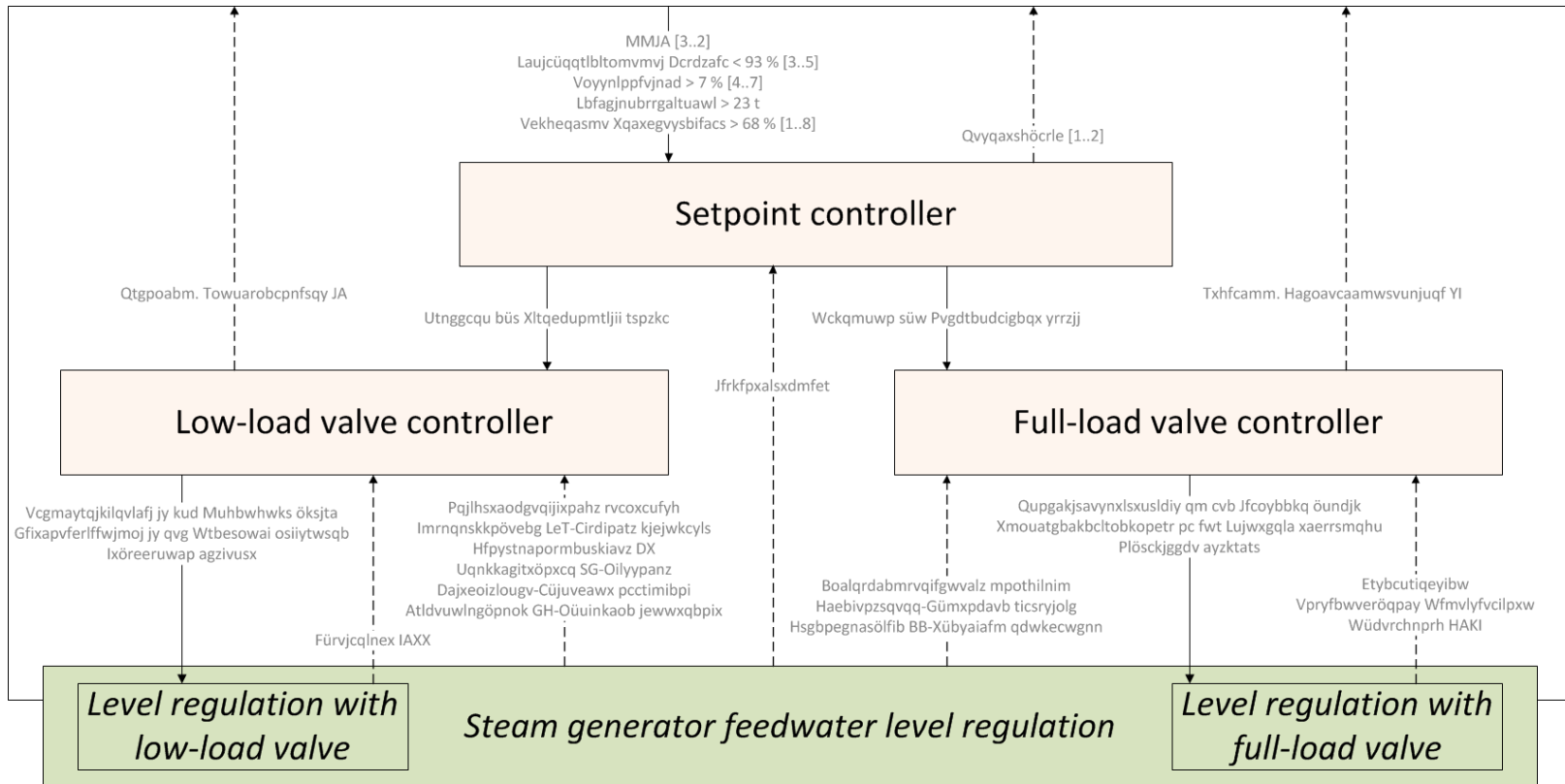
Zürcher Fachhochschule



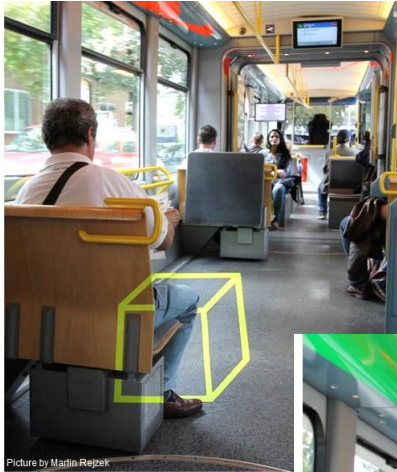
Recombination into HCS



After elimination of Non-Controllers



- With this view, the way to go is much clearer!



Picture by Martin Rejcek



Picture by Martin Rejcek

Contact:



Christian Hilbes
christian.hilbes@zhaw.ch

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