Zurich University
of Applied Sciences

School of
Engineering
IAMP Institute of Applied
Mathematics and Physics

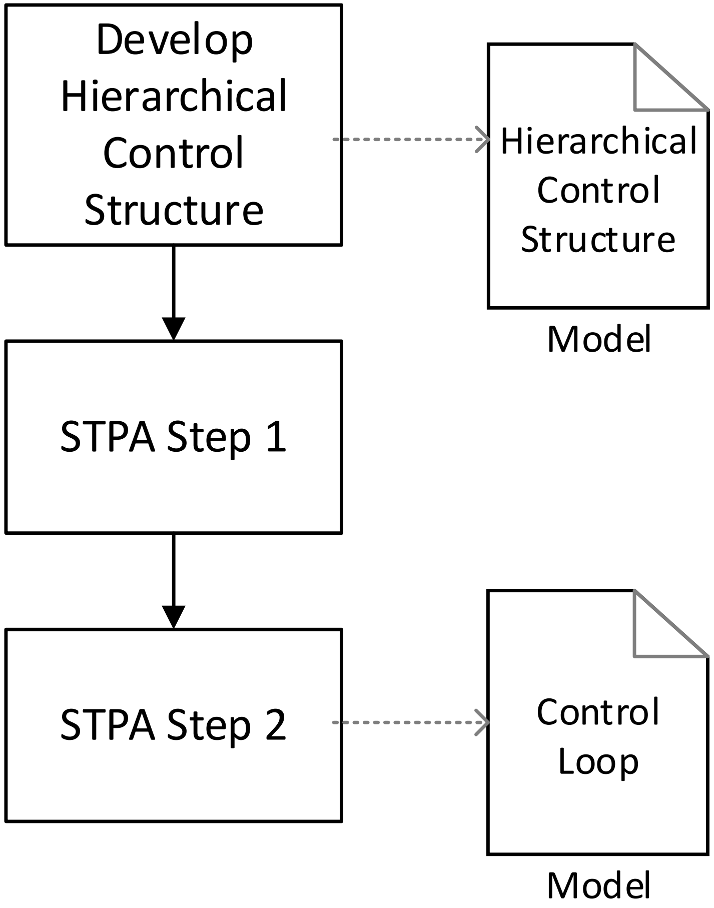
Modelling Multiple Levels of Abstraction in Hierarchical Control Structures

Martin Rejzek, Svana Helen Björnsdóttir, Sven Stefan Krauss

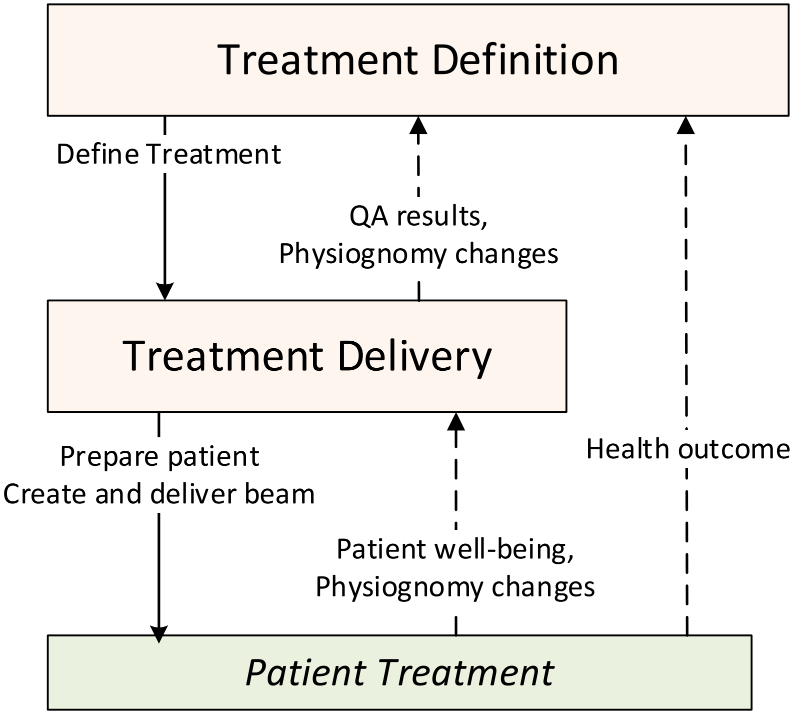
Outline

- The role of models in STPA
- Different views
- Key features
- Use cases
  - Problem statement
  - Examples
  - Rulesets
- Conclusion and outlook

The Role of Models in STPA


Develop Hierarchical Control Structure
Hierarchical Control Structure
Model
STPA Step 1
STPA Step 2
Control Loop
Model

Examples of Abstract HCS Diagrams



Treatment Definition

Define Treatment

QA results,
Physiognomy changes

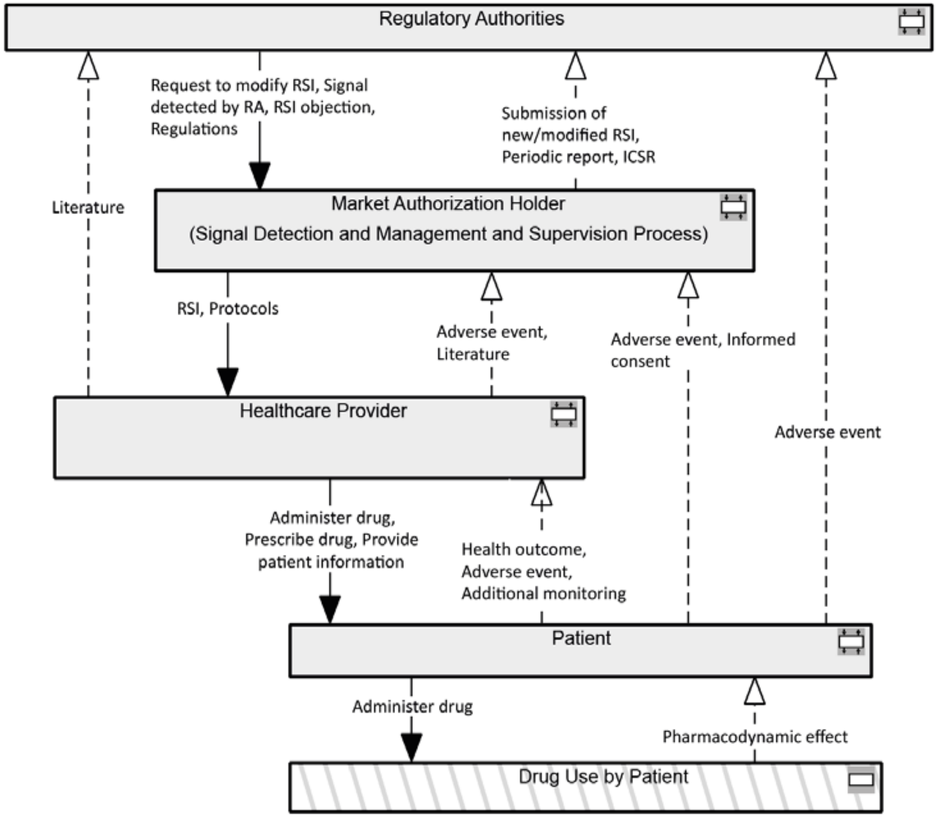
Treatment Delivery

Prepare patient
Create and deliver beam

Patient well-being,
Physiognomy changes

Health outcome

Patient Treatment



Regulatory Authorities

Request to modify RSI, Signal detected by RA, RSI objection, Regulations

Submission of new/modified RSI, Periodic report, ICSR

Literature

Market Authorization Holder
(Signal Detection and Management and Supervision Process)

RSI, Protocols

Adverse event, Literature

Adverse event, Informed consent

Healthcare Provider

Adverse event

Administer drug, Prescribe drug, Provide patient information

Health outcome, Adverse event, Additional monitoring

Patient

Administer drug

Pharmacodynamic effect

Drug Use by Patient

Blandine A.
STPA Applied to the Risk Review of Complex Systems: An Example from the Medical Device Industry
MIT Ph.D Dissertation, 2012 (adaptation shown)

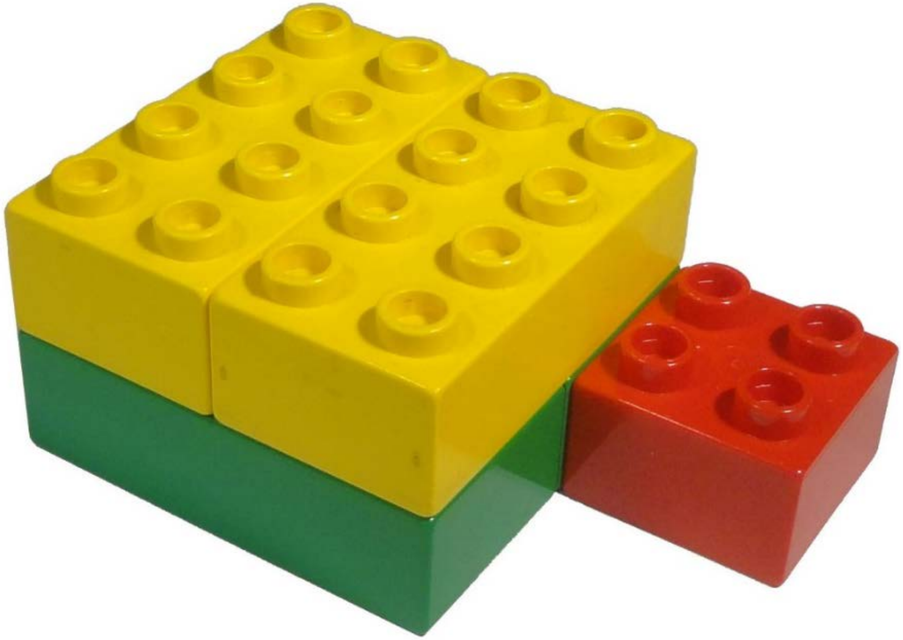
Adesina A., Hussain Q., Pandit S., Rejzek M., Hochberg A.
Assessing the Value of System Theoretic Process Analysis in a Pharmacovigilance Process: An Example Using Signal Management
In Pharmaceutical Medicine, Springer; July 2017

Benefits and Problem Statement

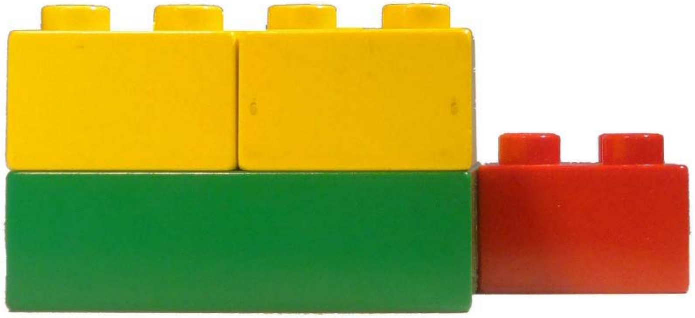
- Starting with abstract representations can be beneficial
  - Helps to define the analysis scope
  - May serve as common starting point for different systems/applications
  - Supports uncovering unclear aspects quickly
- While iteratively progressing with the analysis, abstract representations are typically «discarded»

→ Proposal: Differentiate between Model and View;
Support multiple views.

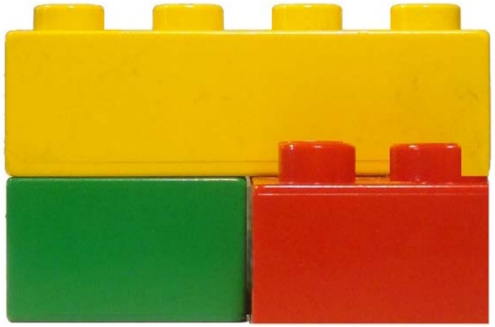
Model versus View



View from Left



View from Right

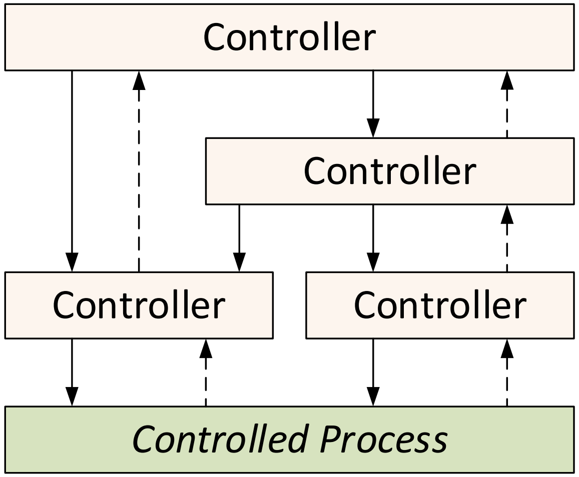


Applied to STAMP

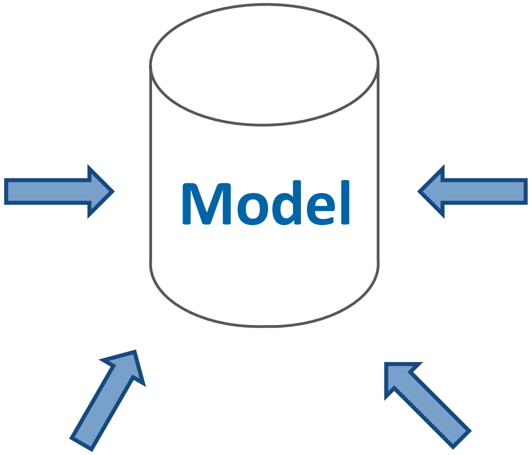
Zurich University of Applied Sciences

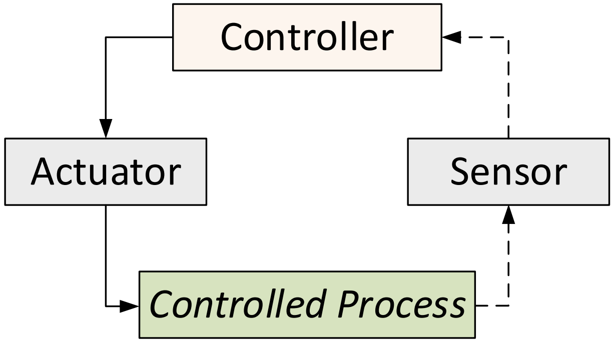
School of Engineering

IAMP Institute of Applied Mathematics and Physics

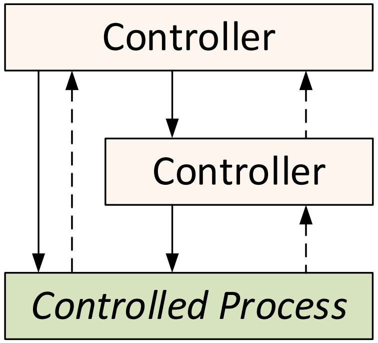


HCS Diagram





Control Loop Diagram



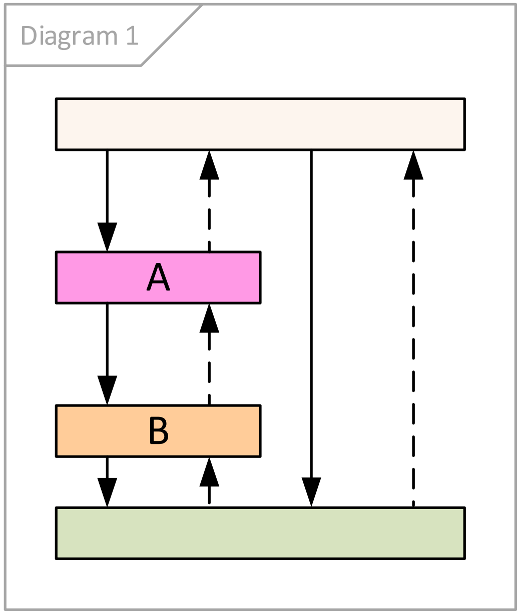
HCS Diagram

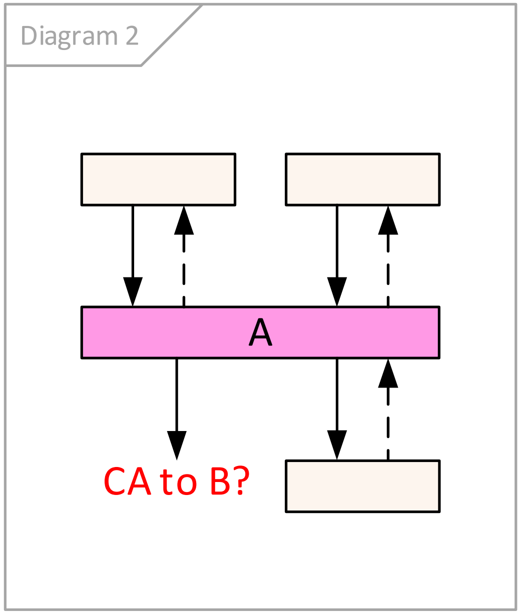
Controller	Description

Table representation

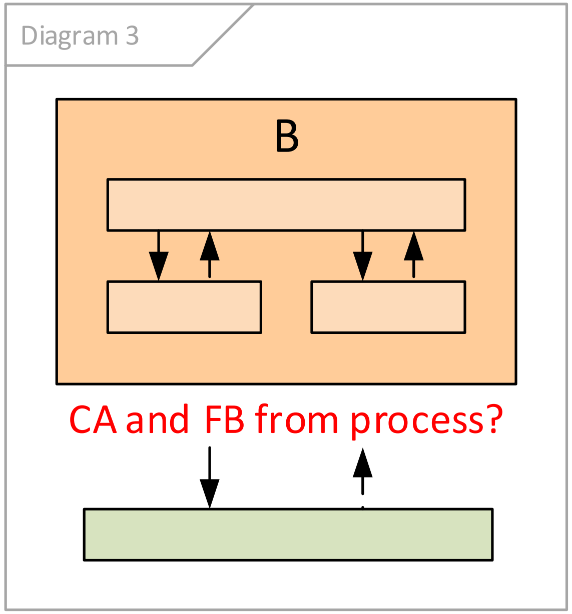
Key Features

- Key features to support proposed concept:
  - Allow to represent HCS by means of multiple diagrams (views)
  - Allow using the same element on multiple diagrams
  - Allow (certain) parent-child relationships among elements
- Sounds trivial … but it is not !



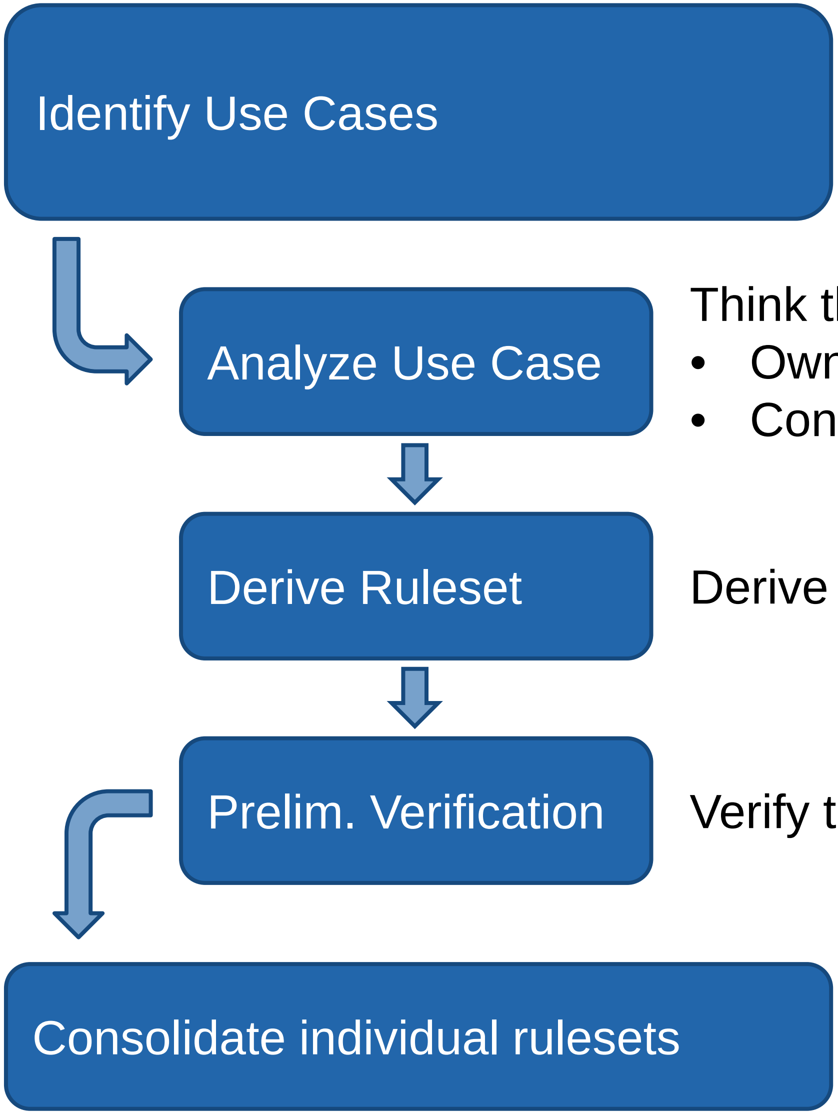


CA to B?



CA and FB from process?

Process used to analyze Concept



Identify Use Cases

- ❖ Complementing views
- ❖ Levels of abstraction
- ❖ Intelligent sensors and actuators
- ❖ Functional redundancies

Analyze Use Case

Think through use case and analyze it:

- Own examples / literature
- Constructed examples

Derive Ruleset

Derive a ruleset for this use case

Prelim. Verification

Verify the derived ruleset (a-posteriori)

for each use case separately

Consolidate individual rulesets

Use Case: Complementing Views

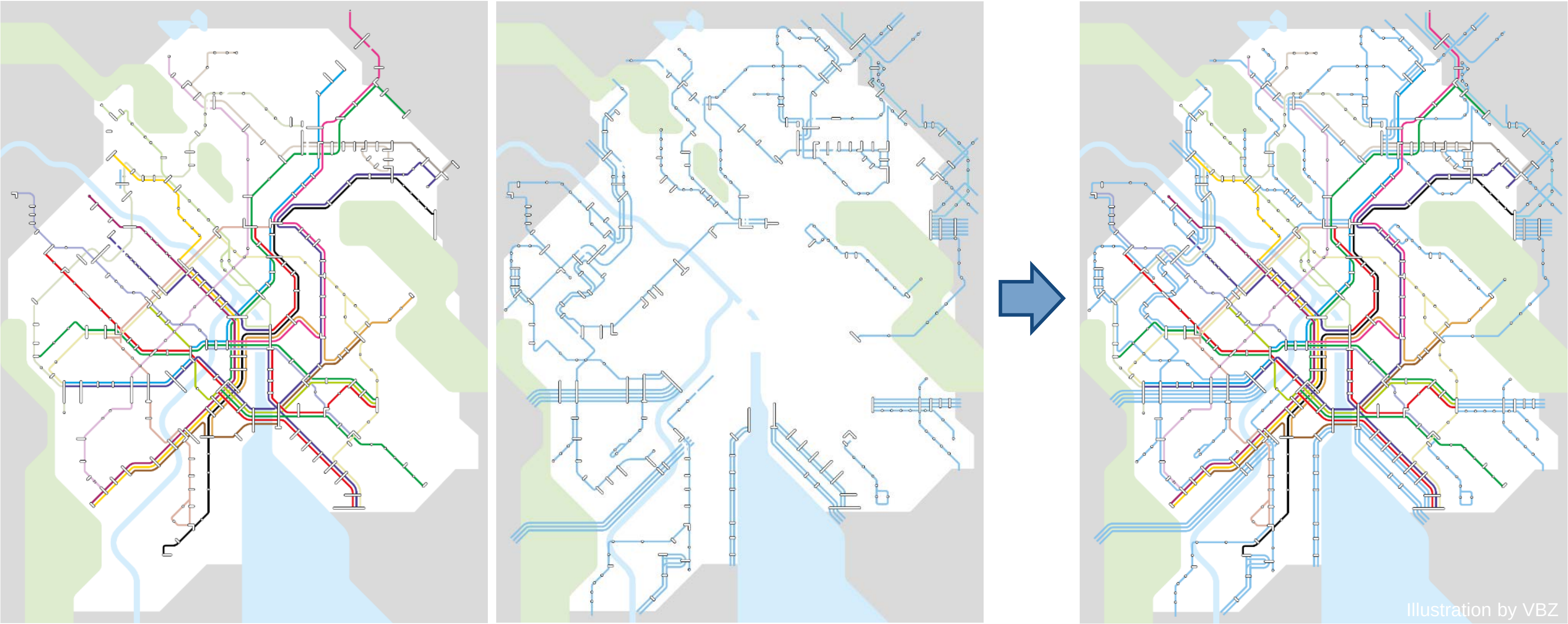


Illustration by VBZ

Maps of the public transportation system in Zürich

Problem Statement

Besides this being a pre-requisite for the other Use Cases …

An Analyst may want to analyze:

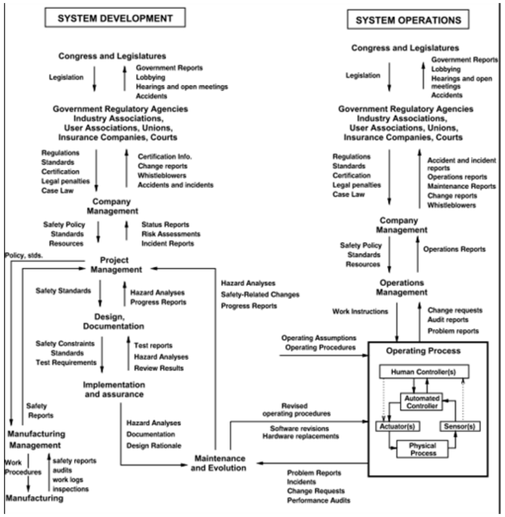
- different phases of a system
  - Design Phase
  - Operation Phase
  - Decommissioning
  - Basic Research
  - Preclinical studies
  - Clinical Development Phases I, II, III
  - Post-marketing evaluation
- different «characteristics» of a system
  - Dose control for radiation treatment
  - Position control for radiation treatment

Model and analyze phases/characteristics separately 👎

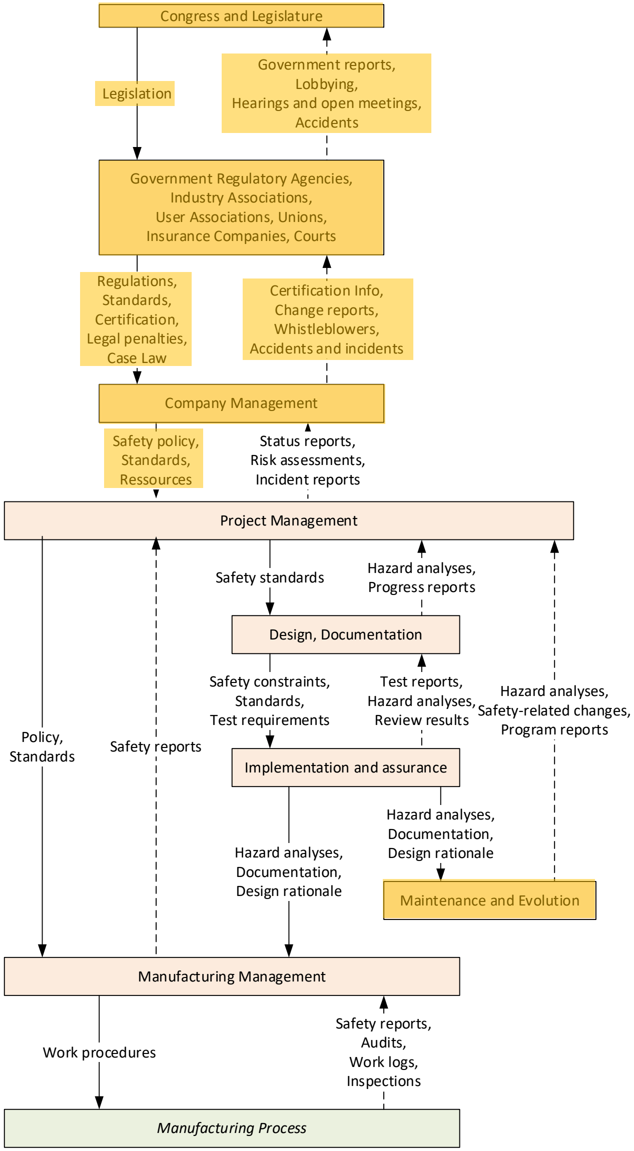
Capture everything on one huge HCS diagram 👎

Use one model with multiple diagrams 👍

Complementing Views – Example System Development and Operation



Leveson, N.G., *Engineering a safer world: Systems thinking applied to safety*. 2012, Cambridge MA, USA: MIT Press.



Congress and Legislature

Legislation

Government reports,
Lobbying,
Hearings and open meetings,
Accidents

Government Regulatory Agencies,
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts

Regulations,
Standards,
Certification,
Legal penalties,
Case Law

Certification Info,
Change reports,
Whistleblowers,
Accidents and incidents

Company Management

Safety policy,
Standards,
Ressources

Status reports,
Risk assessments,
Incident reports

Project Management

Safety standards

Hazard analyses,
Progress reports

Design, Documentation

Safety constraints,
Standards,
Test requirements

Test reports,
Hazard analyses,
Review results

Hazard analyses,
Safety-related changes,
Program reports

Policy,
Standards

Safety reports

Implementation and assurance

Hazard analyses,
Documentation,
Design rationale

Hazard analyses,
Documentation,
Design rationale

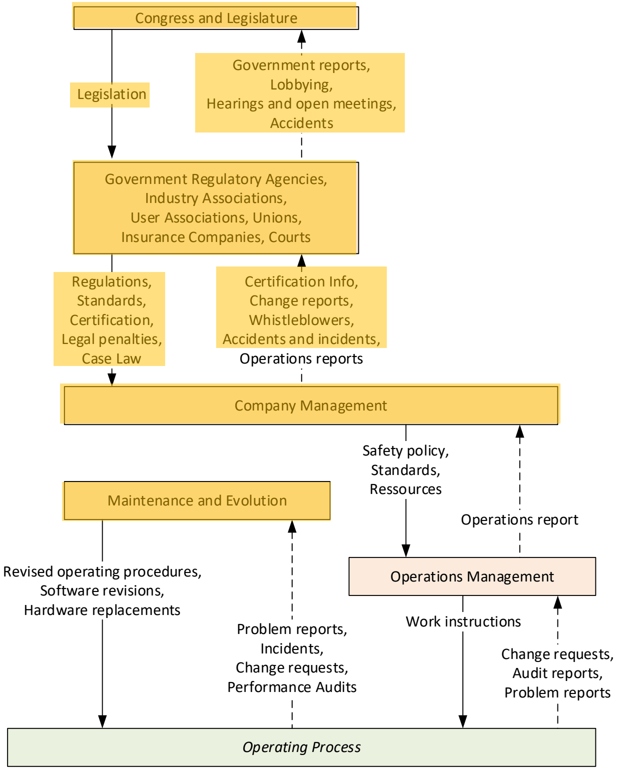
Maintenance and Evolution

Manufacturing Management

Work procedures

Safety reports,
Audits,
Work logs,
Inspections

Manufacturing Process



Congress and Legislature

Legislation

Government reports,
Lobbying,
Hearings and open meetings,
Accidents

Government Regulatory Agencies,
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts

Regulations,
Standards,
Certification,
Legal penalties,
Case Law

Certification Info,
Change reports,
Whistleblowers,
Accidents and incidents,
Operations reports

Company Management

Safety policy,
Standards,
Ressources

Operations report

Maintenance and Evolution

Revised operating procedures,
Software revisions,
Hardware replacements

Problem reports,
Incidents,
Change requests,
Performance Audits

Operations Management

Work instructions

Change requests,
Audit reports,
Problem reports

Operating Process

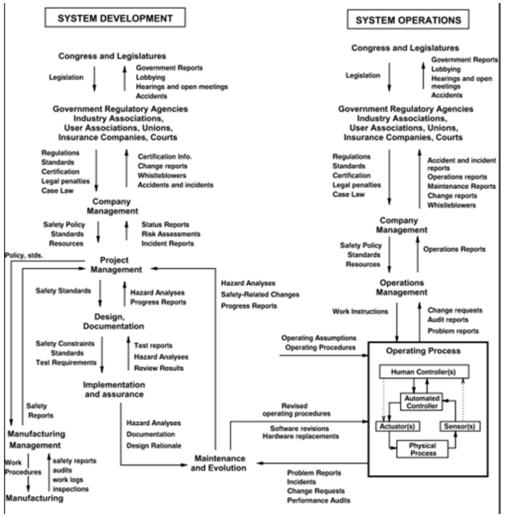
Elements appearing on both diagrams

Complementing Views – Example System Development and Operation

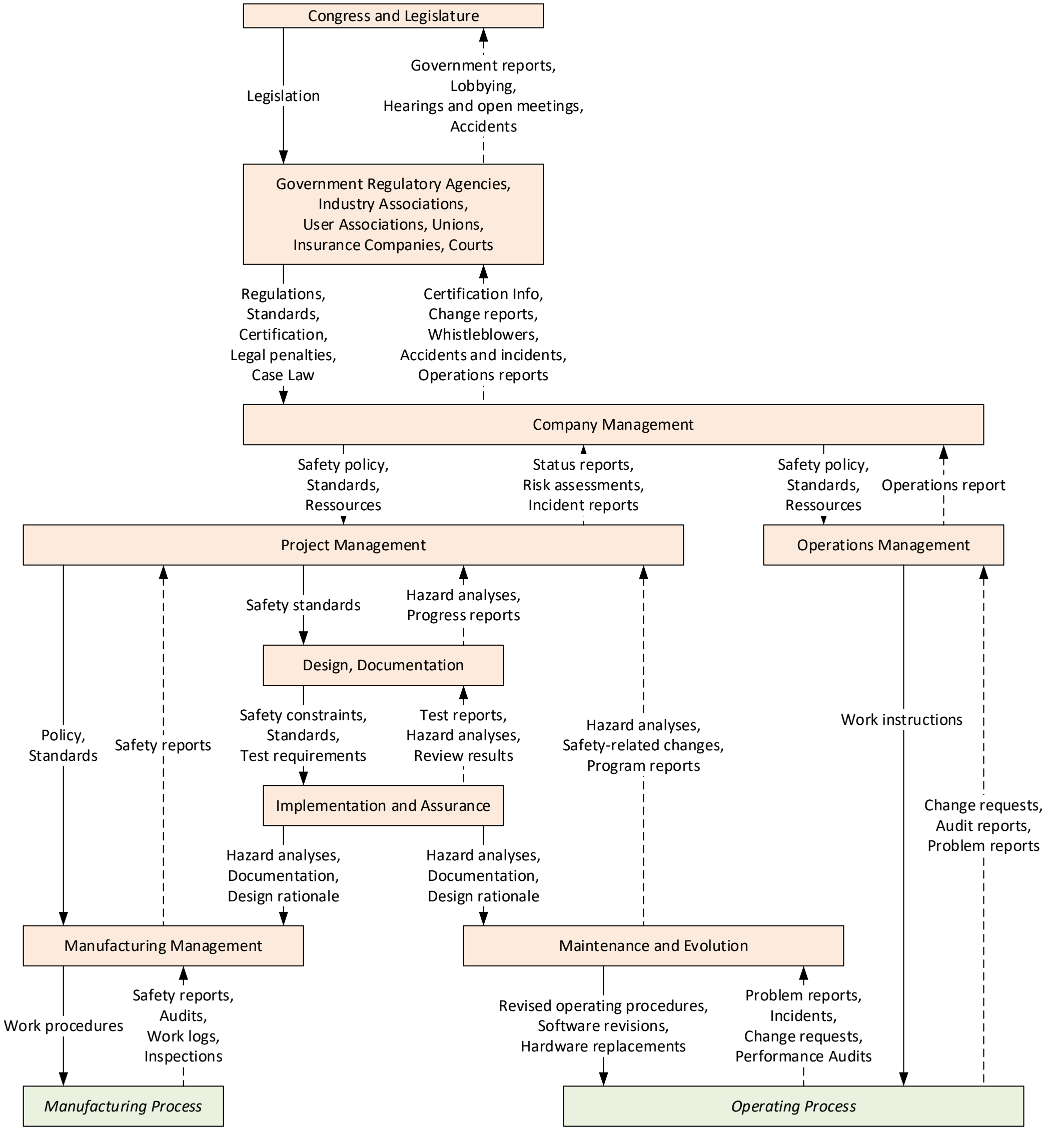
Zurich University of Applied Sciences

School of Engineering

IAMP Institute of Applied Mathematics and Physics



Leveson, N.G., *Engineering a safer world: Systems thinking applied to safety*. 2012, Cambridge MA, USA: MIT Press.



Congress and Legislature
Legislation
Government reports, Lobbying, Hearings and open meetings, Accidents
Government Regulatory Agencies, Industry Associations, User Associations, Unions, Insurance Companies, Courts
Regulations, Standards, Certification, Legal penalties, Case Law
Certification Info, Change reports, Whistleblowers, Accidents and incidents, Operations reports
Company Management
Safety policy, Standards, Ressources
Status reports, Risk assessments, Incident reports
Safety policy, Standards, Ressources
Operations report
Project Management
Operations Management
Safety standards
Hazard analyses, Progress reports
Design, Documentation
Safety constraints, Standards, Test requirements
Test reports, Hazard analyses, Review results
Policy, Standards
Safety reports
Hazard analyses, Safety-related changes, Program reports
Work instructions
Change requests, Audit reports, Problem reports
Implementation and Assurance
Hazard analyses, Documentation, Design rationale
Hazard analyses, Documentation, Design rationale
Manufacturing Management
Maintenance and Evolution
Work procedures
Safety reports, Audits, Work logs, Inspections
Revised operating procedures, Software revisions, Hardware replacements
Problem reports, Incidents, Change requests, Performance Audits
Manufacturing Process
Operating Process

Ruleset for Complementing Views

12 rules identified:

- The same controller may appear on multiple diagrams.
- A diagram may represent only a subset of the control actions generated/received by a controller.
- STPA Step 1 needs to be performed for all control actions irrespective of which diagram they are on.
- Every element (controller, controlled process, control action, or feedback) must appear at least on one diagram.
- …

Use Case: Levels of Abstraction

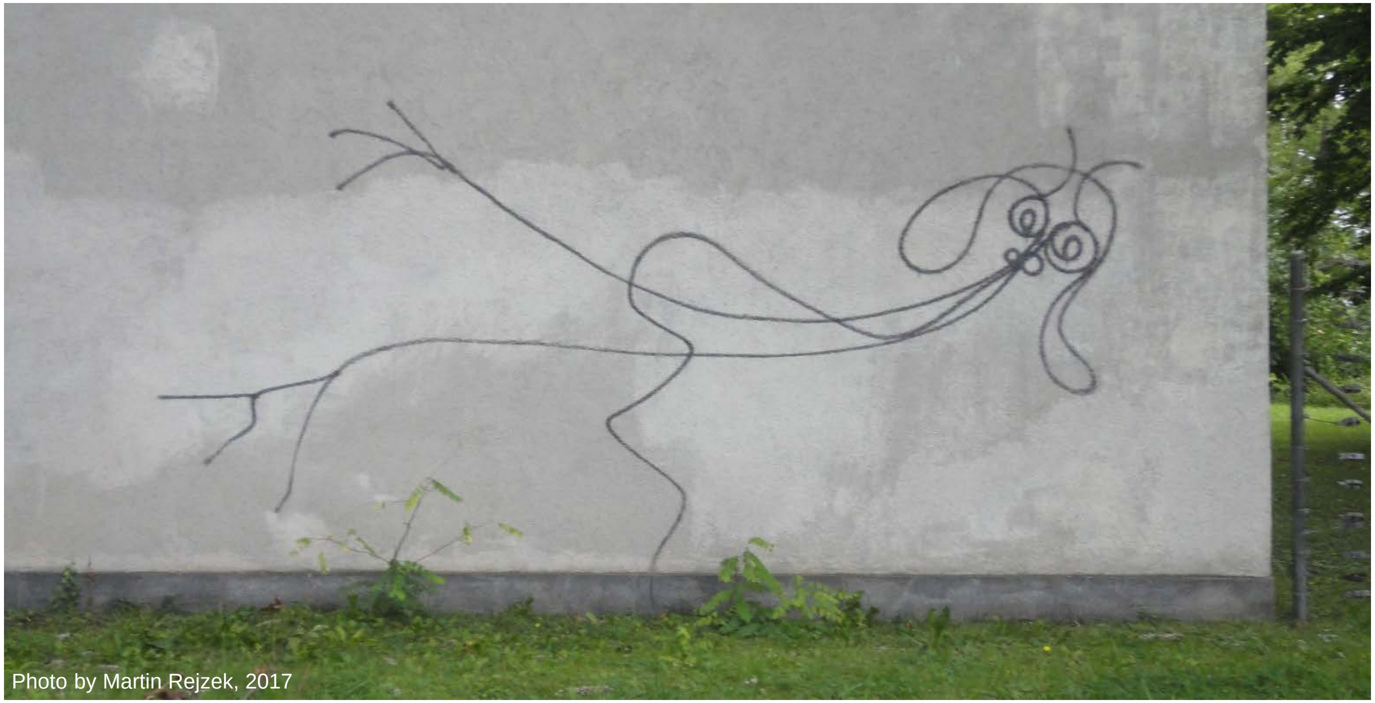
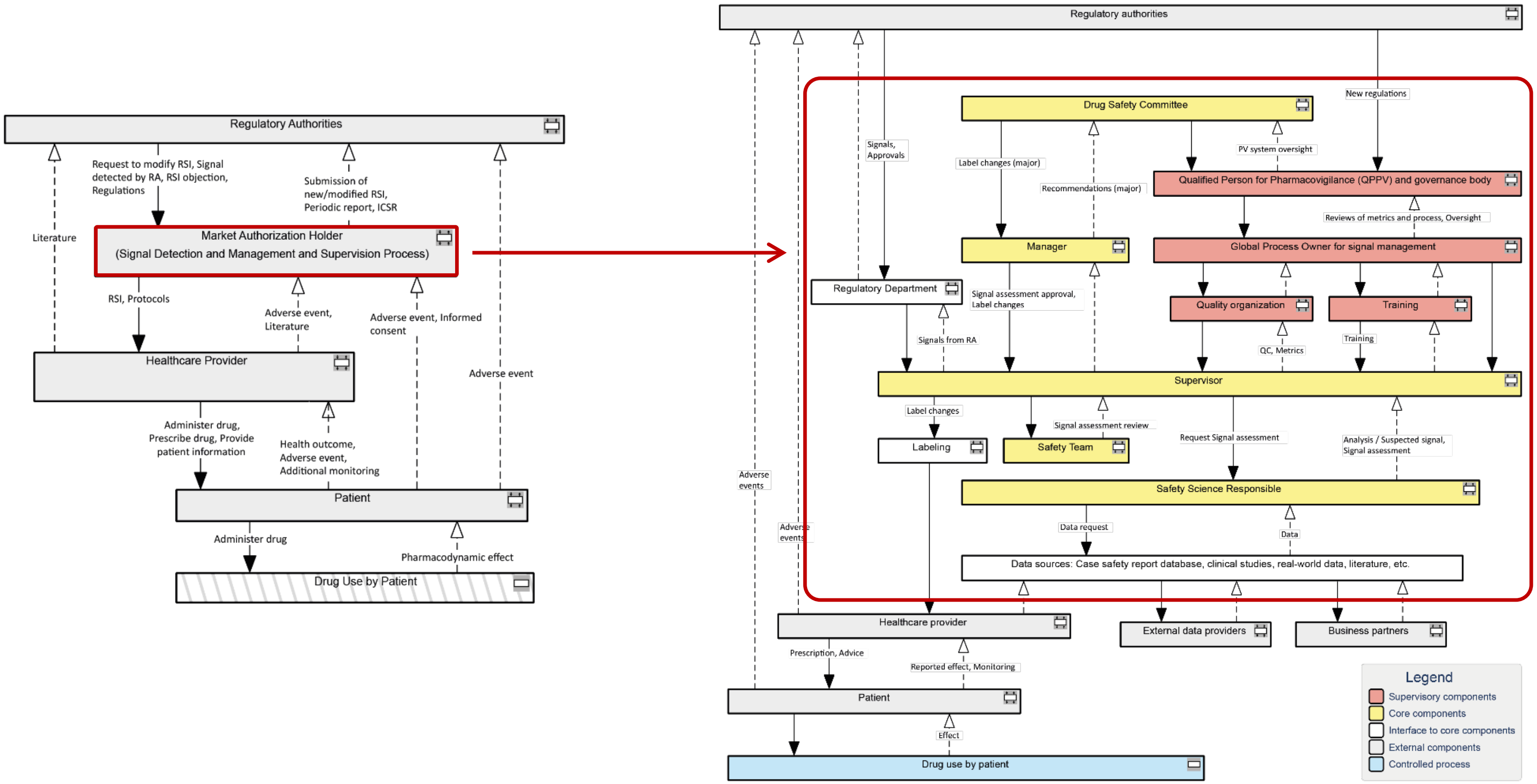


Photo by Martin Rejzek, 2017

Graffiti by Harald Nägeli at Schönberggasse 9, CH-8001 Zürich

Problem Statement

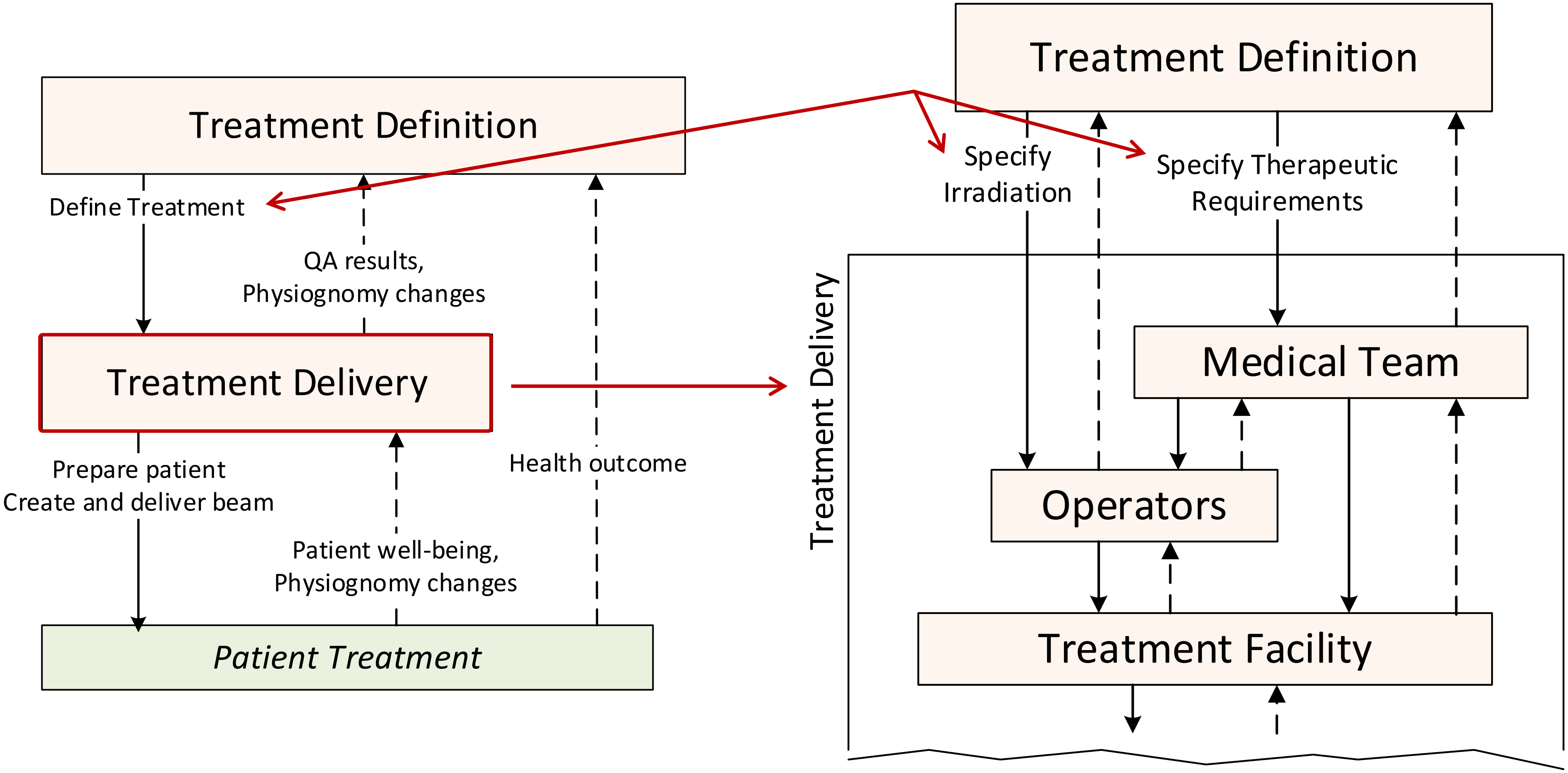
An analyst may want to refine controllers and their control flow


Regulatory Authorities
Request to modify RSI, Signal detected by RA, RSI objection, Regulations
Submission of new/modified RSI, Periodic report, ICSR
Literature
Market Authorization Holder
(Signal Detection and Management and Supervision Process)
RSI, Protocols
Adverse event, Literature
Adverse event, Informed consent
Adverse event
Healthcare Provider
Administer drug, Prescribe drug, Provide patient information
Health outcome, Adverse event, Additional monitoring
Patient
Administer drug
Pharmacodynamic effect
Drug Use by Patient
Regulatory authorities
New regulations
Drug Safety Committee
Signals, Approvals
Label changes (major)
Recommendations (major)
PV system oversight
Qualified Person for Pharmacovigilance (QPPV) and governance body
Reviews of metrics and process, Oversight
Manager
Global Process Owner for signal management
Regulatory Department
Signal assessment approval, Label changes
Signals from RA
Quality organization
Training
QC, Metrics
Training
Supervisor
Label changes
Signal assessment review
Request Signal assessment
Analysis / Suspected signal, Signal assessment
Labeling
Safety Team
Adverse events
Safety Science Responsible
Adverse events
Data request
Data
Data sources: Case safety report database, clinical studies, real-world data, literature, etc.
Healthcare provider
External data providers
Business partners
Prescription, Advice
Reported effect, Monitoring
Patient
Effect
Drug use by patient
Legend
🟥 Supervisory components
🟨 Core components
□ Interface to core components
□ External components
🟦 Controlled process

Adesina A., Hussain Q., Pandit S., Rejzek M., Hochberg A. *Assessing the Value of System Theoretic Process Analysis in a Pharmacovigilance Process: An Example Using Signal Management* In Pharmaceutical Medicine, Springer; July 2017

Levels of Abstraction – Example Radiation Therapy

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



Blandine A.

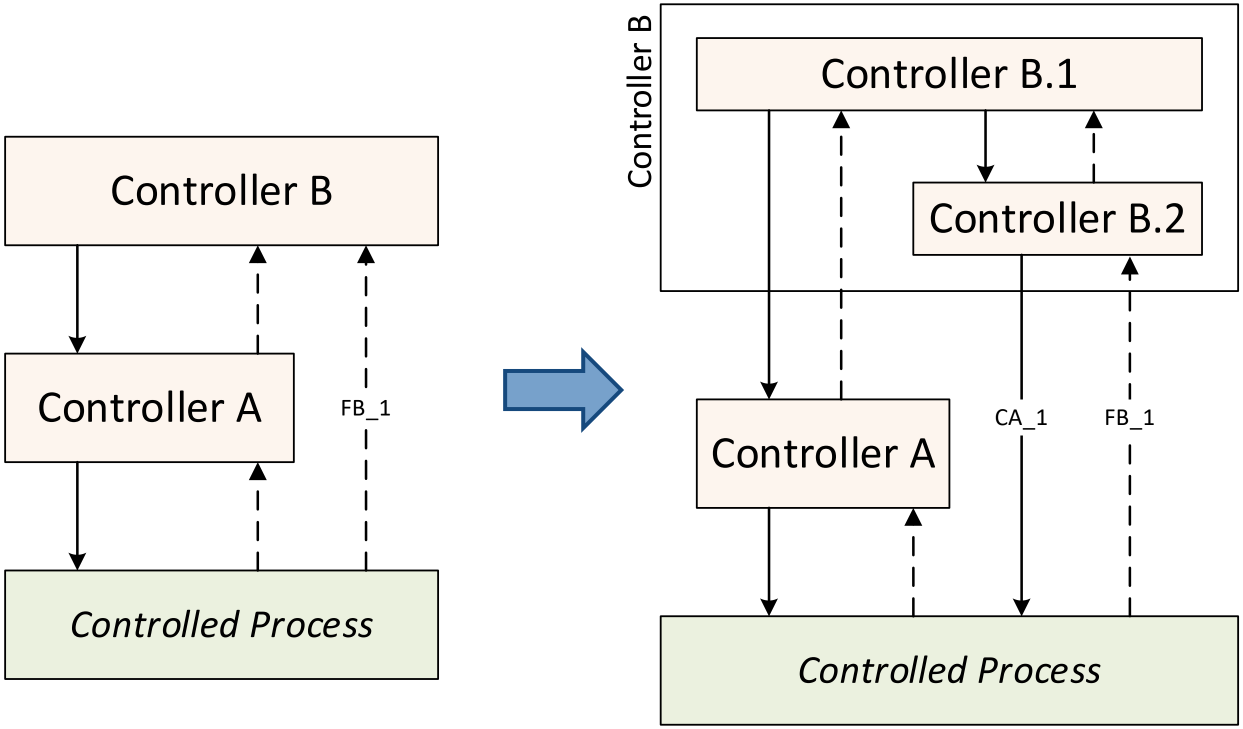
STPA Applied to the Risk Review of Complex Systems: An Example from the Medical Device Industry

MIT Ph.D Dissertation, 2012 (adaptation shown)

Ruleset for Levels of Abstraction

22 rules and consistency considerations identified:

- A feedback may have multiple sinks.
- If a feedback has multiple sinks, they must be related to each other by a parent-child relationship.
- …



Conclusion

Does using multiple diagrams (views) involve risks?

- If the analyst starts to focus separately on individual “pieces” and forgets the “holistic view”

As always, there are pros and cons:

👍 Pros:

- Overview
- Traceable refinement process
- Possibility to highlight certain aspects
- Allows to explicitly go into details

👎 Cons:

- Risk to forget “holistic view”
- Need to manage consistency → Software

Outlook

Apply shown concepts *a-priori* to parts of European Spallation Source (ESS) in Lund, Sweden

- 5 MW linear proton accelerator with tungsten target
- A rather complex socio-technological system
- Apply STPA (in combination with other methods) in the context of Machine Protection

Visualization by ESS

Contact:

Martin Rejzek
martin.rejzek@zhaw.ch

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