

The Brühl accident

An accident analysis using STAMP -
Systems Theory Accident Modeling and Processes

2. Bieleeschweig Workshop

Christian Brinkmann

Braunschweig, 01.07.2003



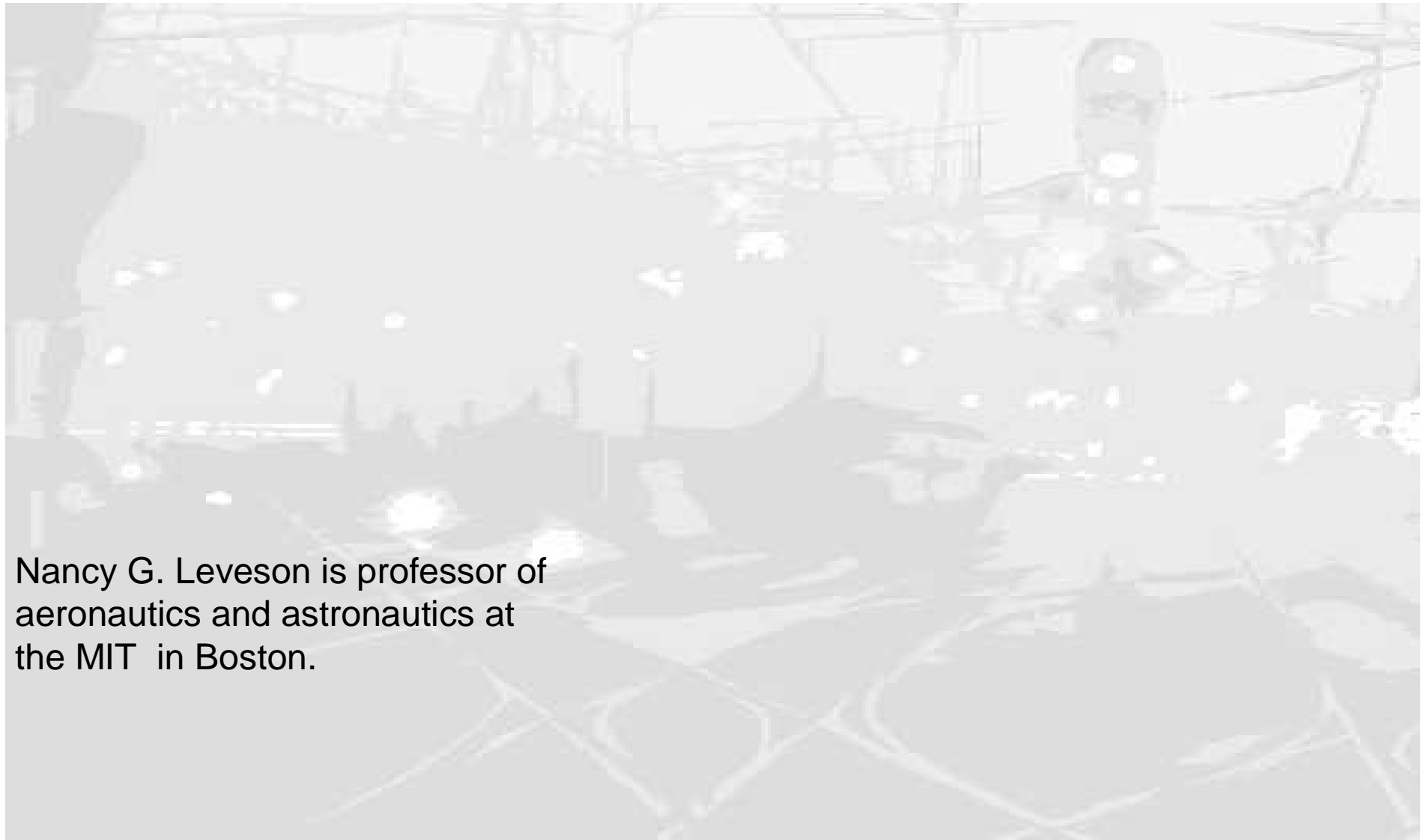


1. An introduction to STAMP

- 
1. An introduction to STAMP
 2. An analysis of the Brühl accident using STAMP

1. An introduction to STAMP
2. An analysis of the Brühl accident using STAMP
3. Results and experiences

1. An introduction to STAMP
2. An analysis of Brühl using STAMP
3. Results and experiences



Nancy G. Leveson is professor of aeronautics and astronautics at the MIT in Boston.



Nancy G. Leveson is professor of aeronautics and astronautics at the MIT in Boston.



Nancy G. Leveson is professor of aeronautics and astronautics at the MIT in Boston.

Papers

by Nancy Leveson (MIT Boston):

May 2002

1. „A New Foundation for System Safety“
2. “The Analysis of a Friendly Fire Accident using a Systems Model of Accidents“

January 2003

3. “A New Accident Model for Engineering Safer Systems”

April 2003

4. “Applying STAMP in accident analysis”

by Chris Johnson (Univ. of Glasgow):

4. “The ESA/NASA SOHO Mission interruption: Using the Stamp Accident Analysis Technique for a Software Related ‘Mishap’.”

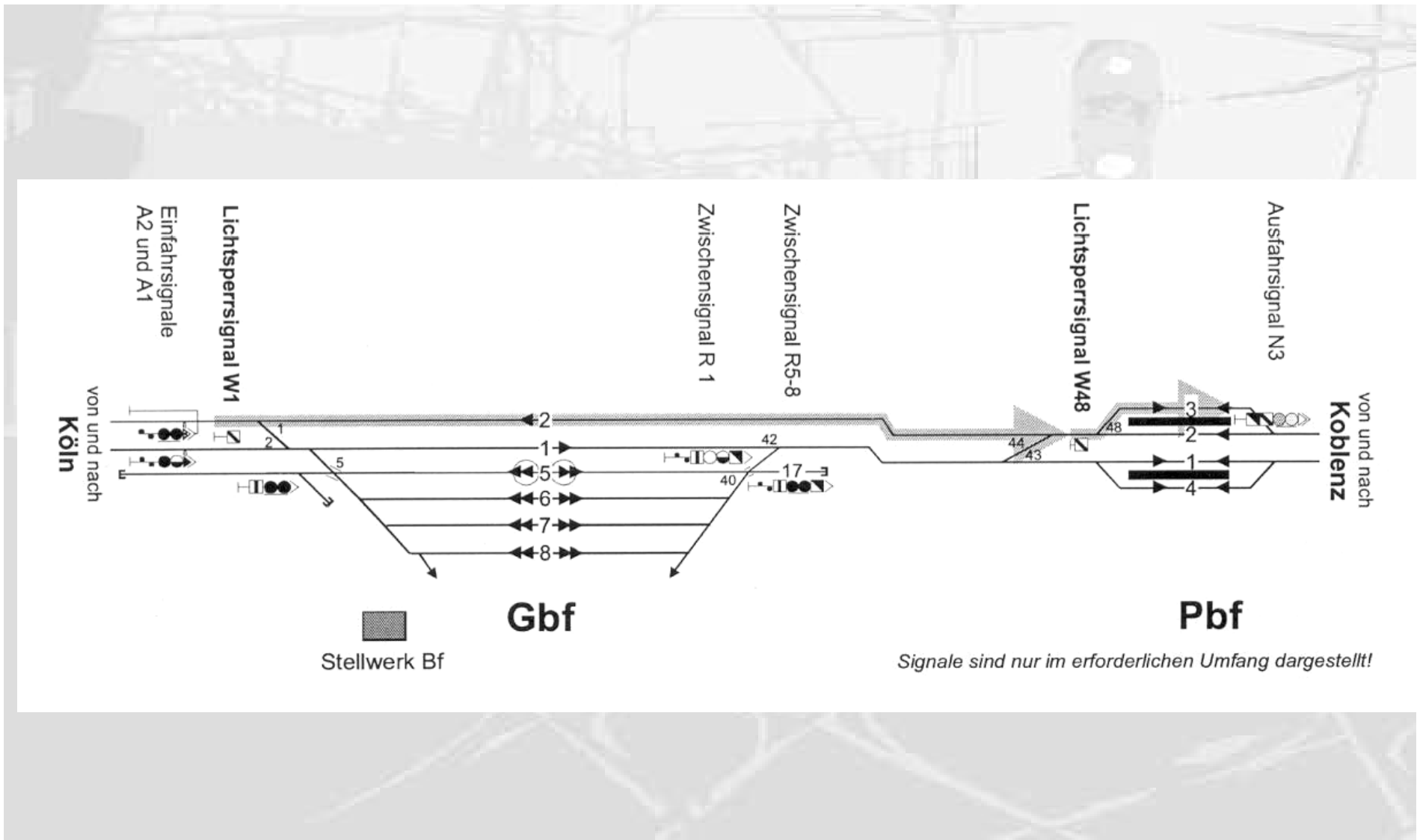
<http://sunnyday.mit.edu/papers.html>

www.dcs.gla.ac.uk/~johnson/papers/

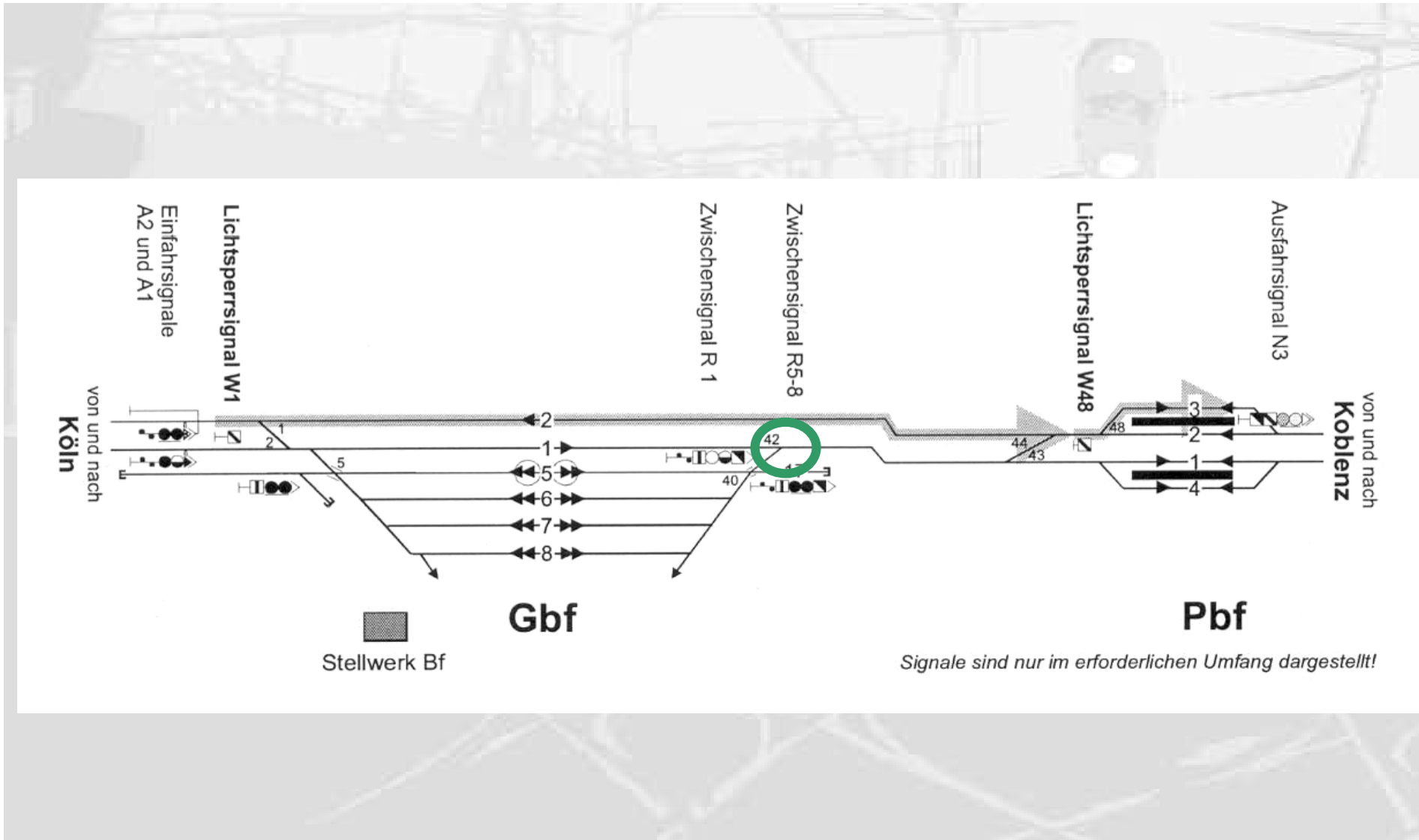
Brühl location



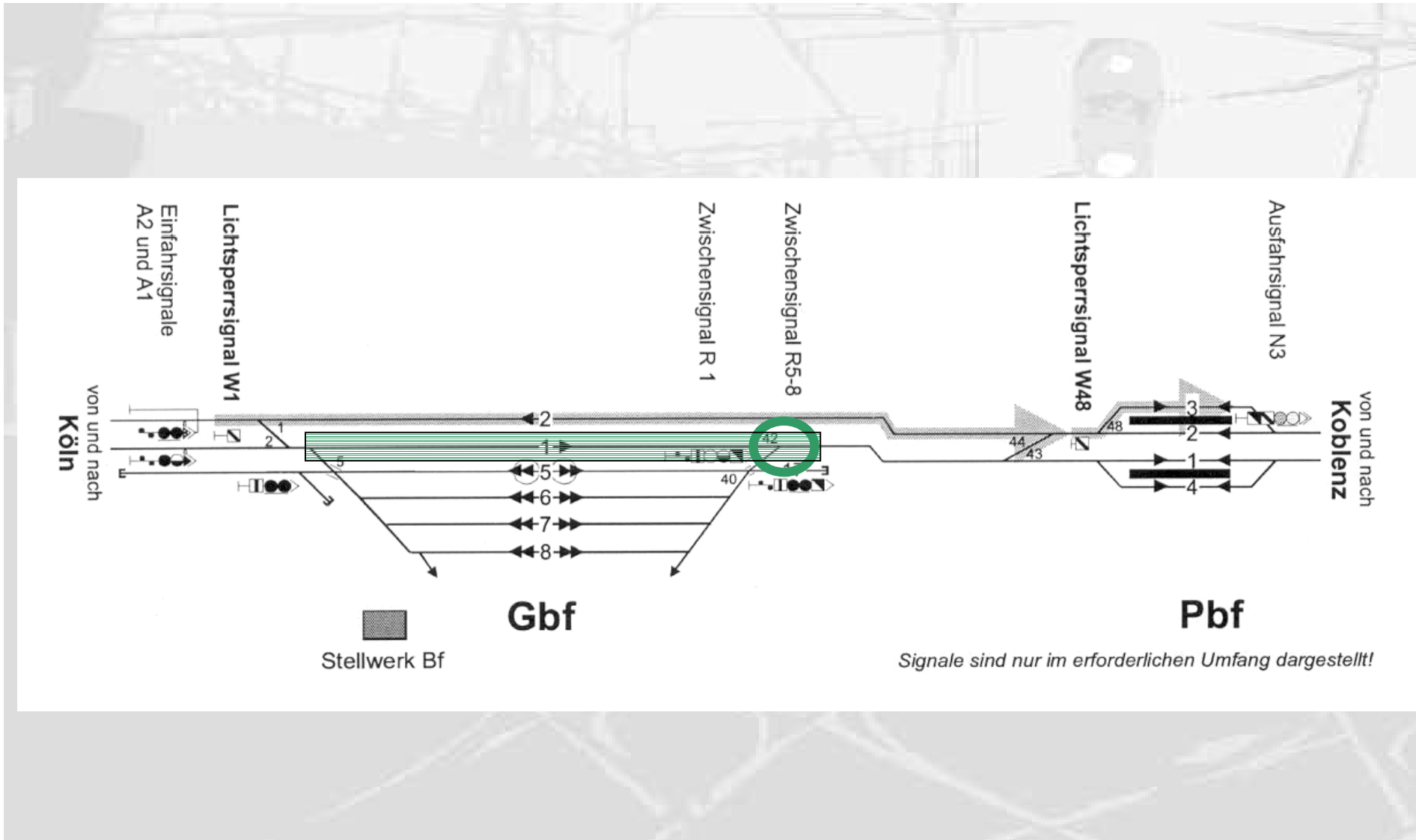
Brühl location



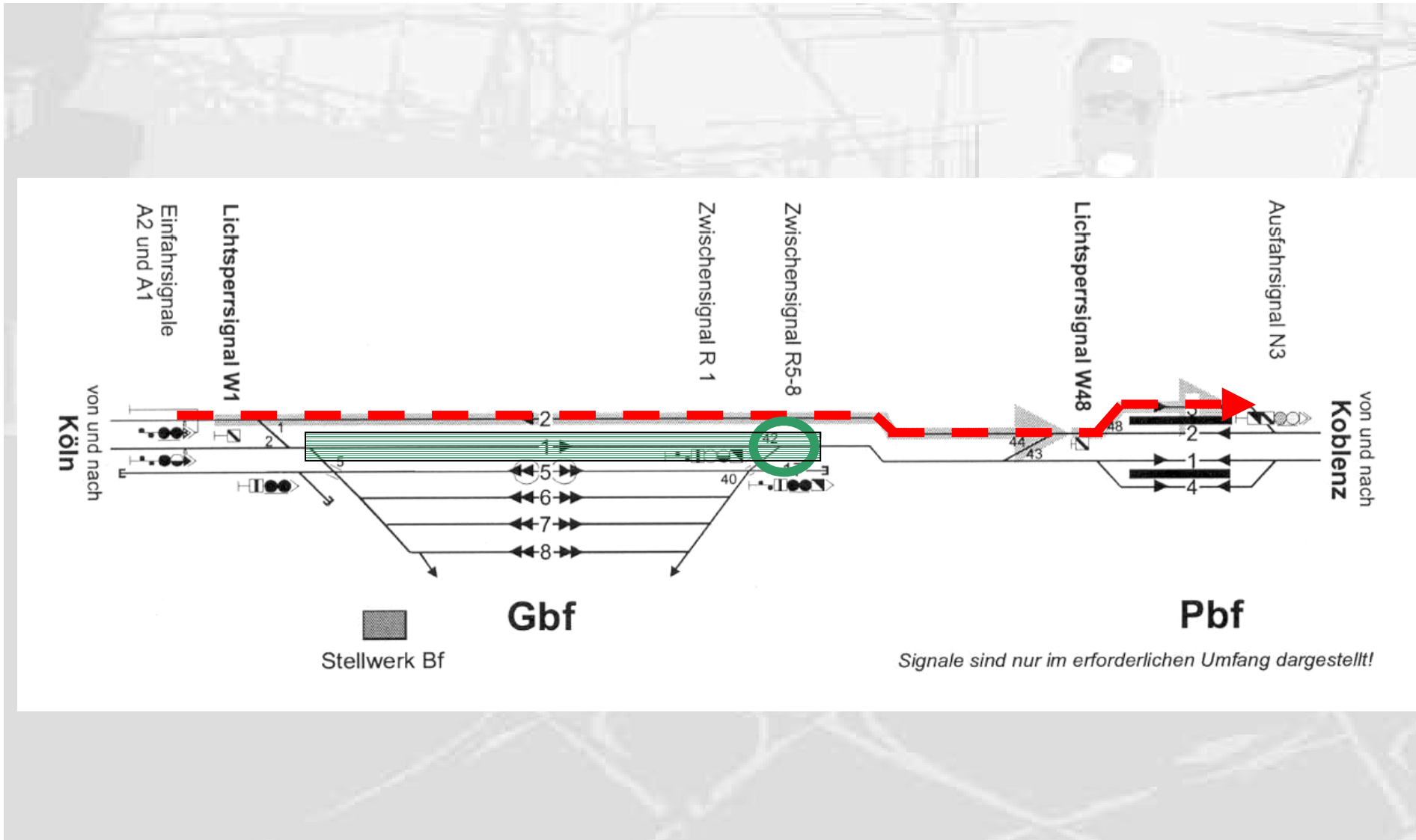
Brühl location



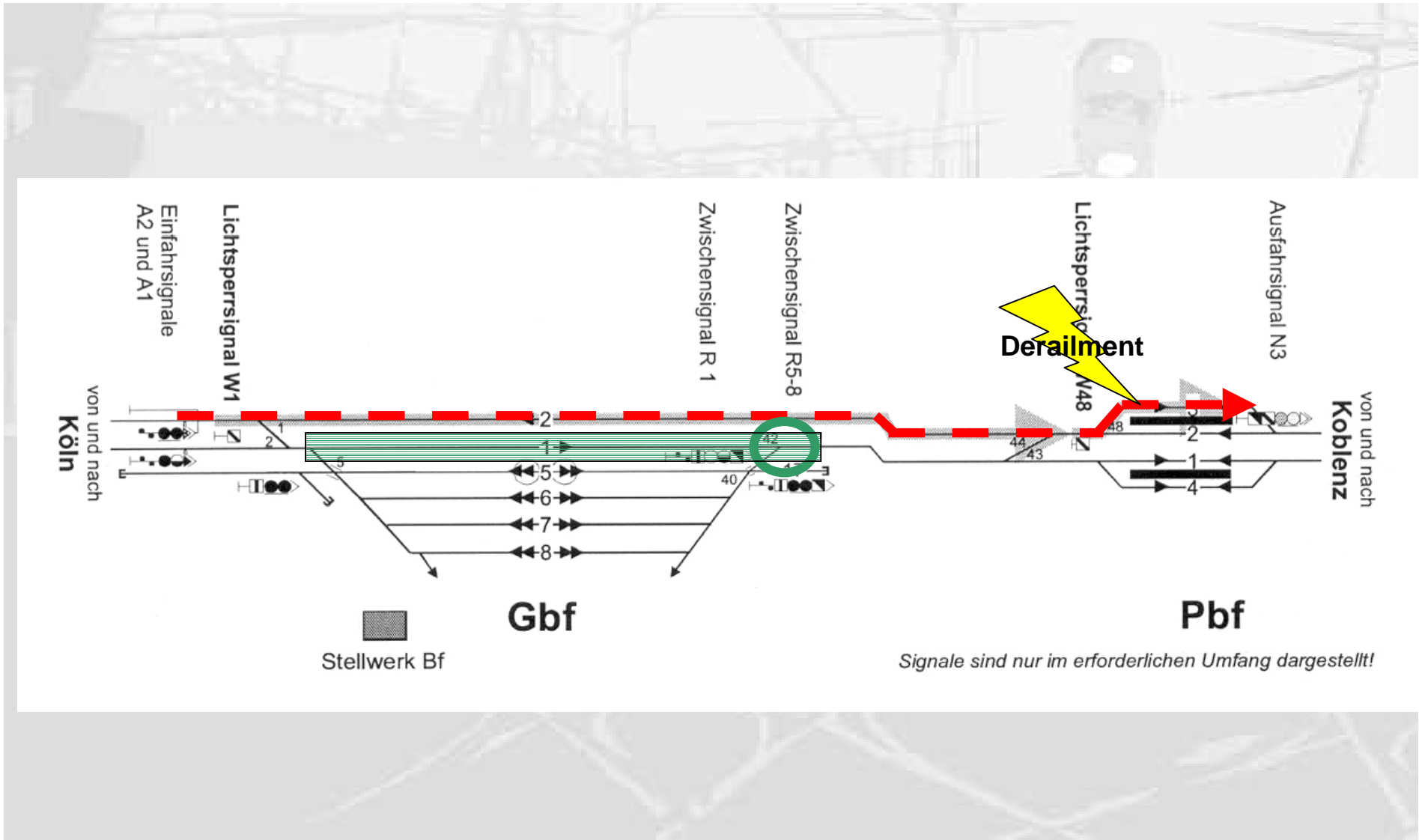
Brühl location



Brühl location



Brühl location



The need for a new model



The need for a new model

Rasmussen:



Rasmussen:

“The stage for an accidental course of events very likely is prepared through time by the normal efforts of many actors in their respective daily work context, responding to the standing request to be more productive and less costly.

Rasmussen:

“The stage for an accidental course of events very likely is prepared through time by the normal efforts of many actors in their respective daily work context, responding to the standing request to be more productive and less costly.

Ultimately, a quite normal variation in somebody’s behavior can then release an accident. Had this ‘root cause’ been avoided by some additional safety measure, the accident would very likely be released by another cause at another point in time. In other words, an explanation of the accident in terms of events, acts and errors is not very useful for design of improved systems.”

What is different?



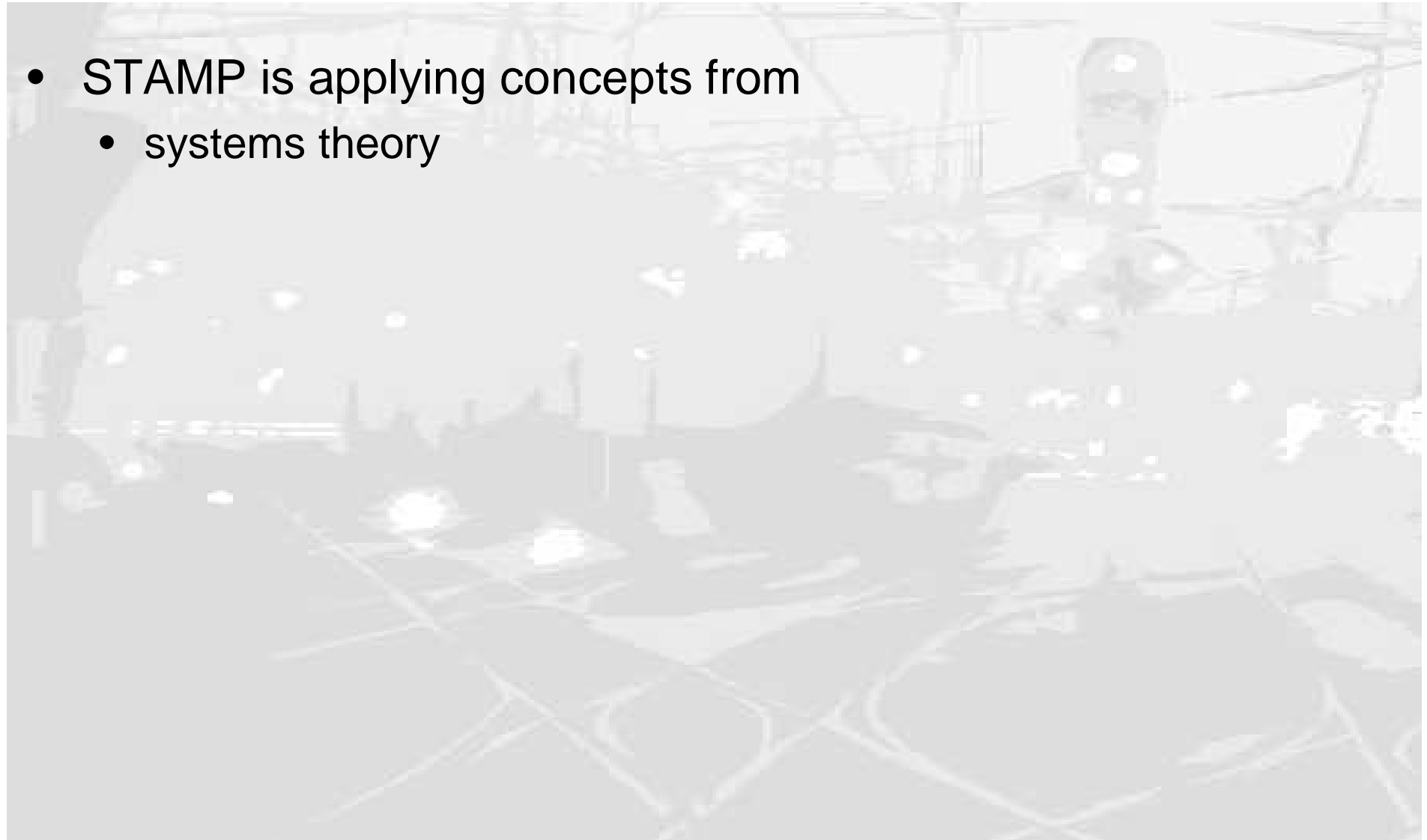
What is different?

- STAMP is applying concepts from



What is different?

- STAMP is applying concepts from
 - systems theory



What is different?

- STAMP is applying concepts from
 - systems theory
 - control theory

What is different?

- STAMP is applying concepts from
 - systems theory
 - control theoryto accident analysis

What is different?

- STAMP is applying concepts from
 - systems theory
 - control theoryto accident analysis
- The basic elements are

What is different?

- STAMP is applying concepts from
 - systems theory
 - control theoryto accident analysis
- The basic elements are
 - constraints

What is different?

- STAMP is applying concepts from
 - systems theory
 - control theoryto accident analysis
- The basic elements are
 - constraints
 - control loops

What is different?

- STAMP is applying concepts from
 - systems theory
 - control theoryto accident analysis
- The basic elements are
 - constraints
 - control loops
 - control structures

What is different?

- STAMP is applying concepts from
 - systems theory
 - control theoryto accident analysis
- The basic elements are
 - constraints
 - control loops
 - control structures
- STAMP does not require causal reasoning

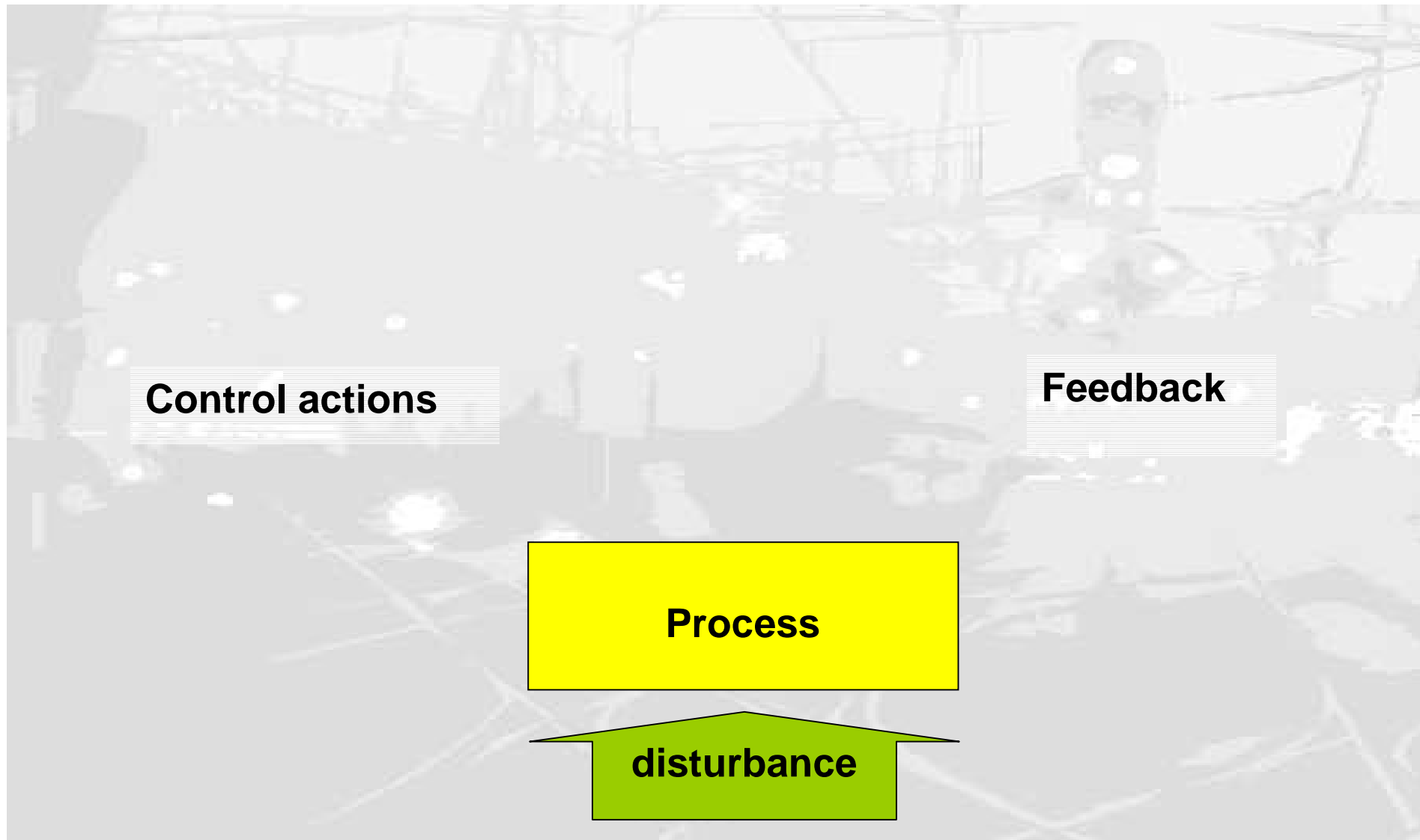
Control loop



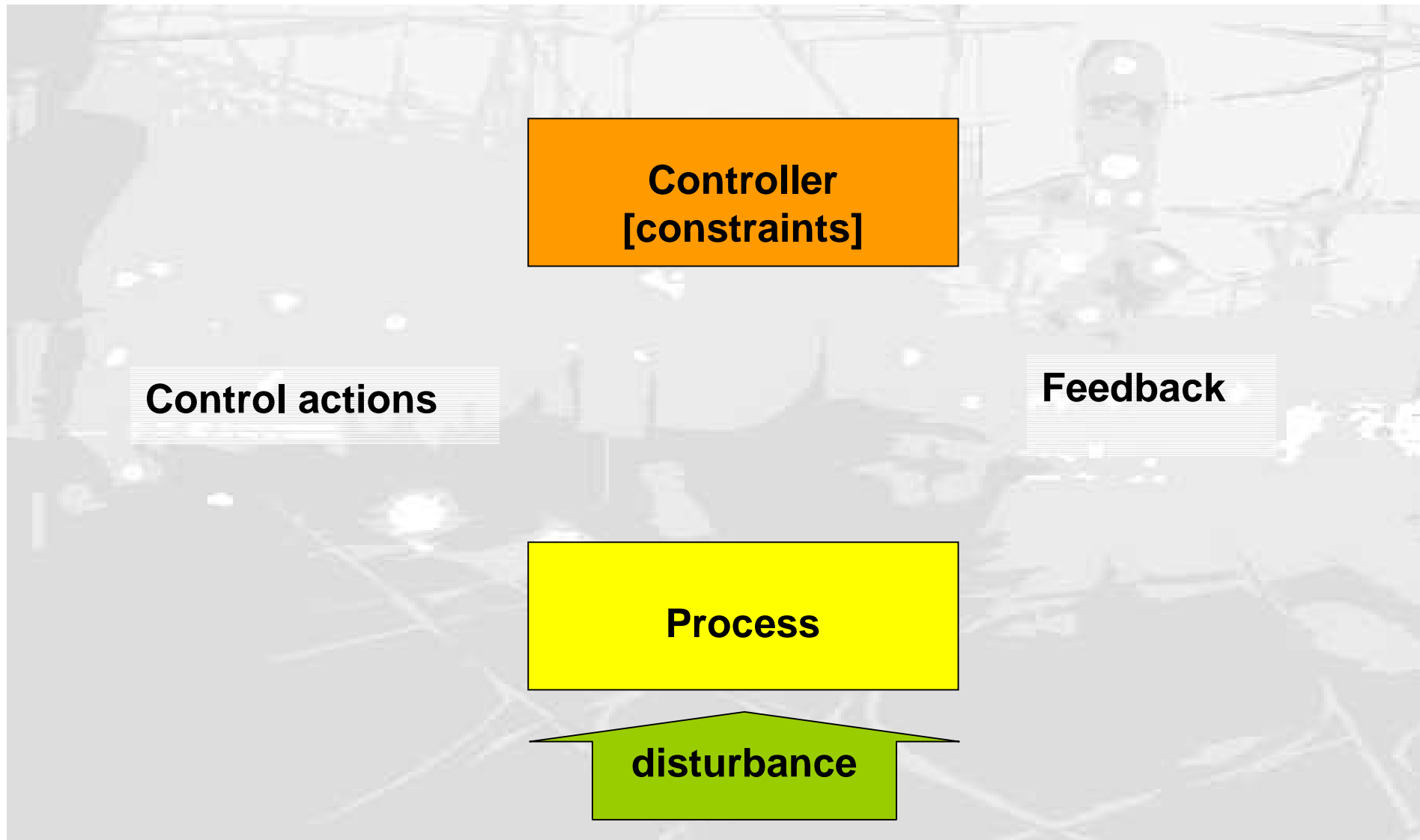
Control loop



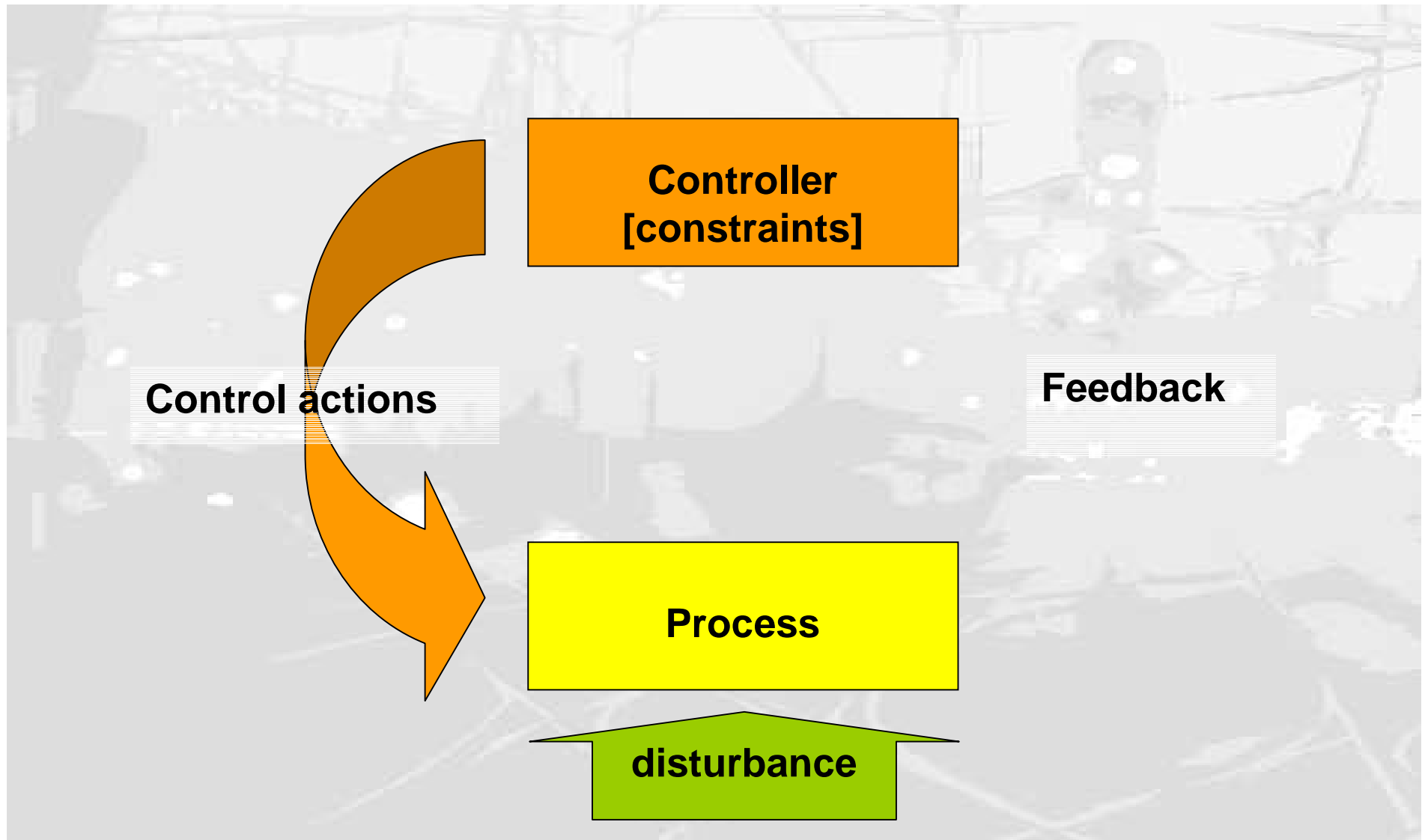
Control loop



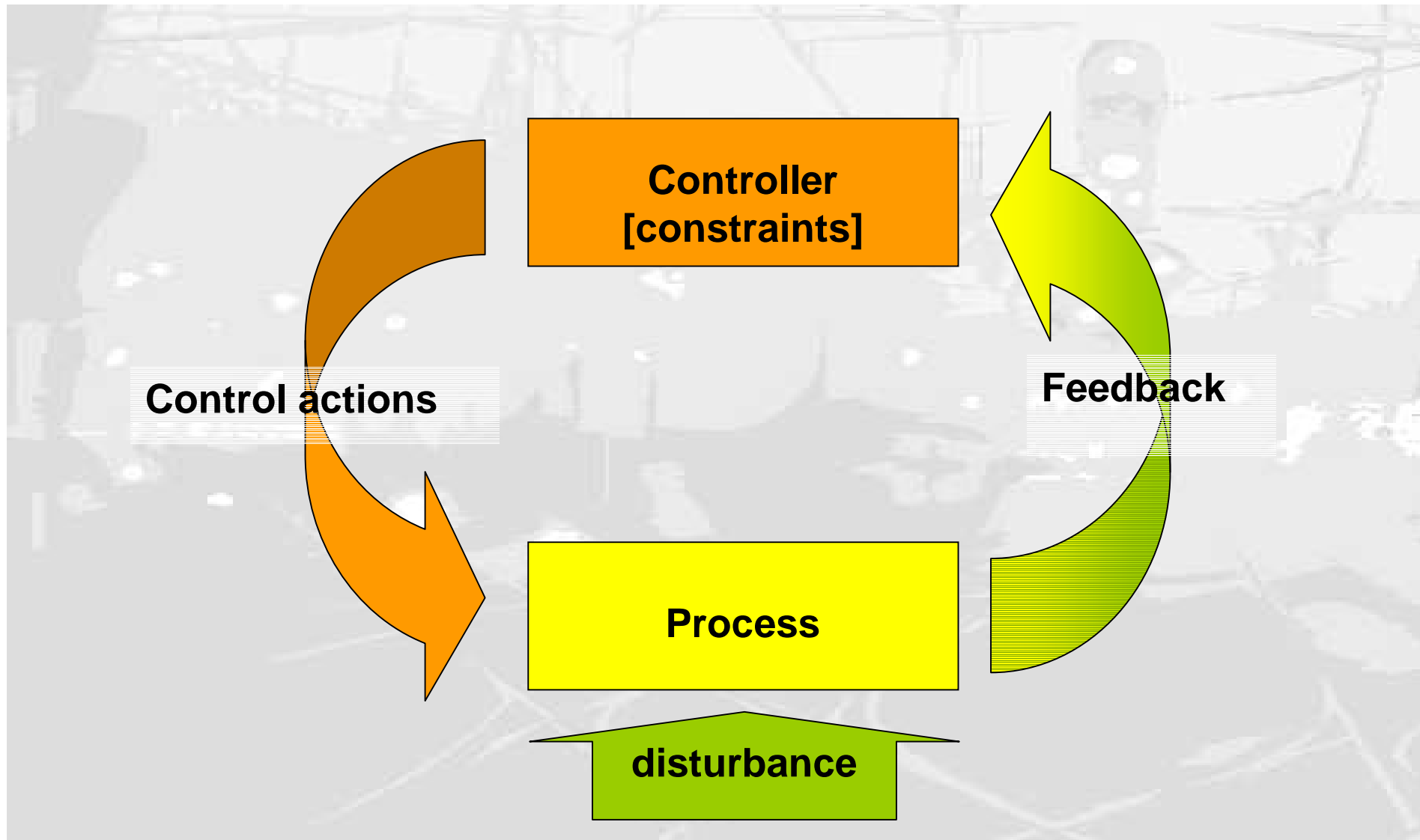
Control loop



Control loop



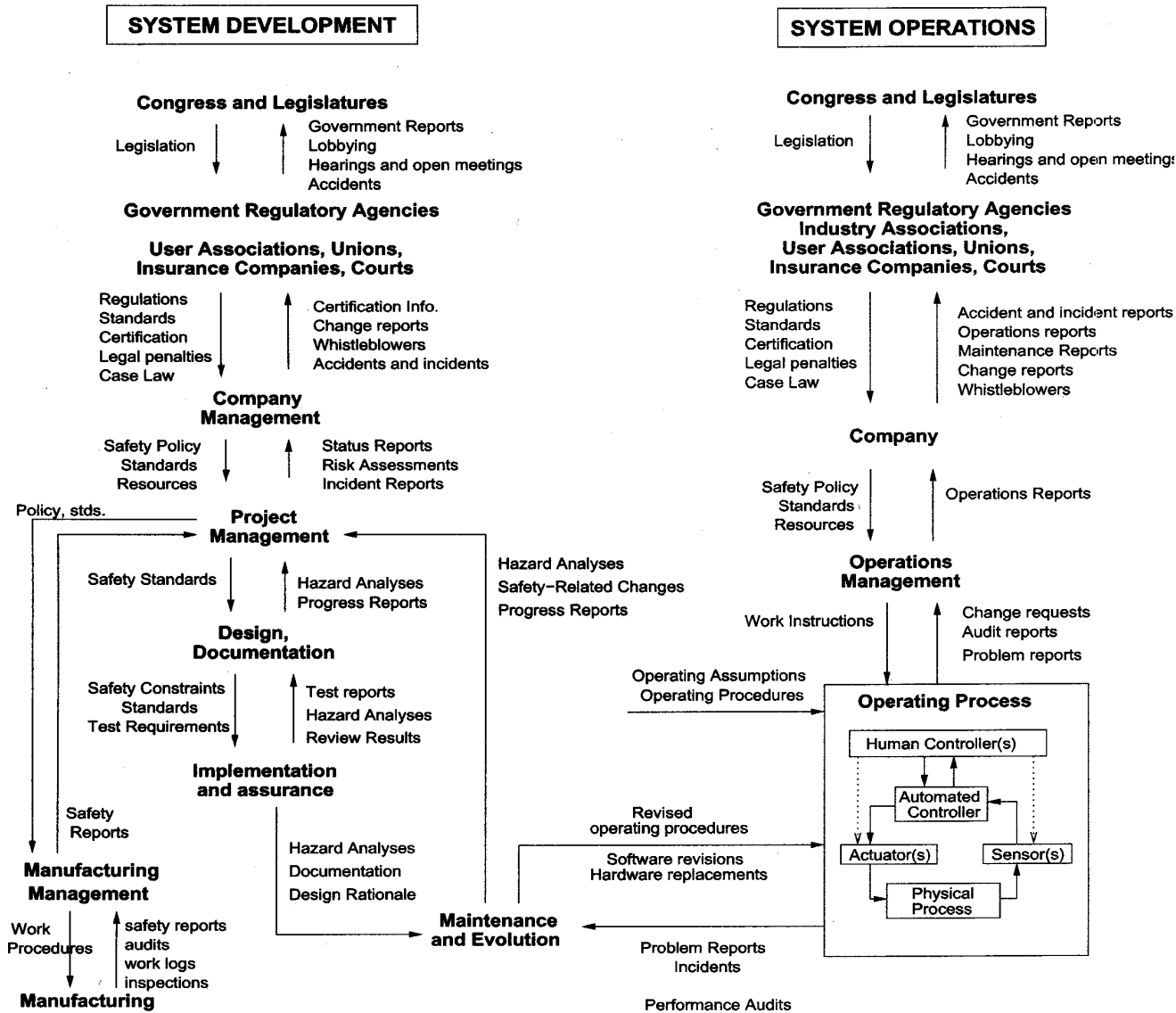
Control loop



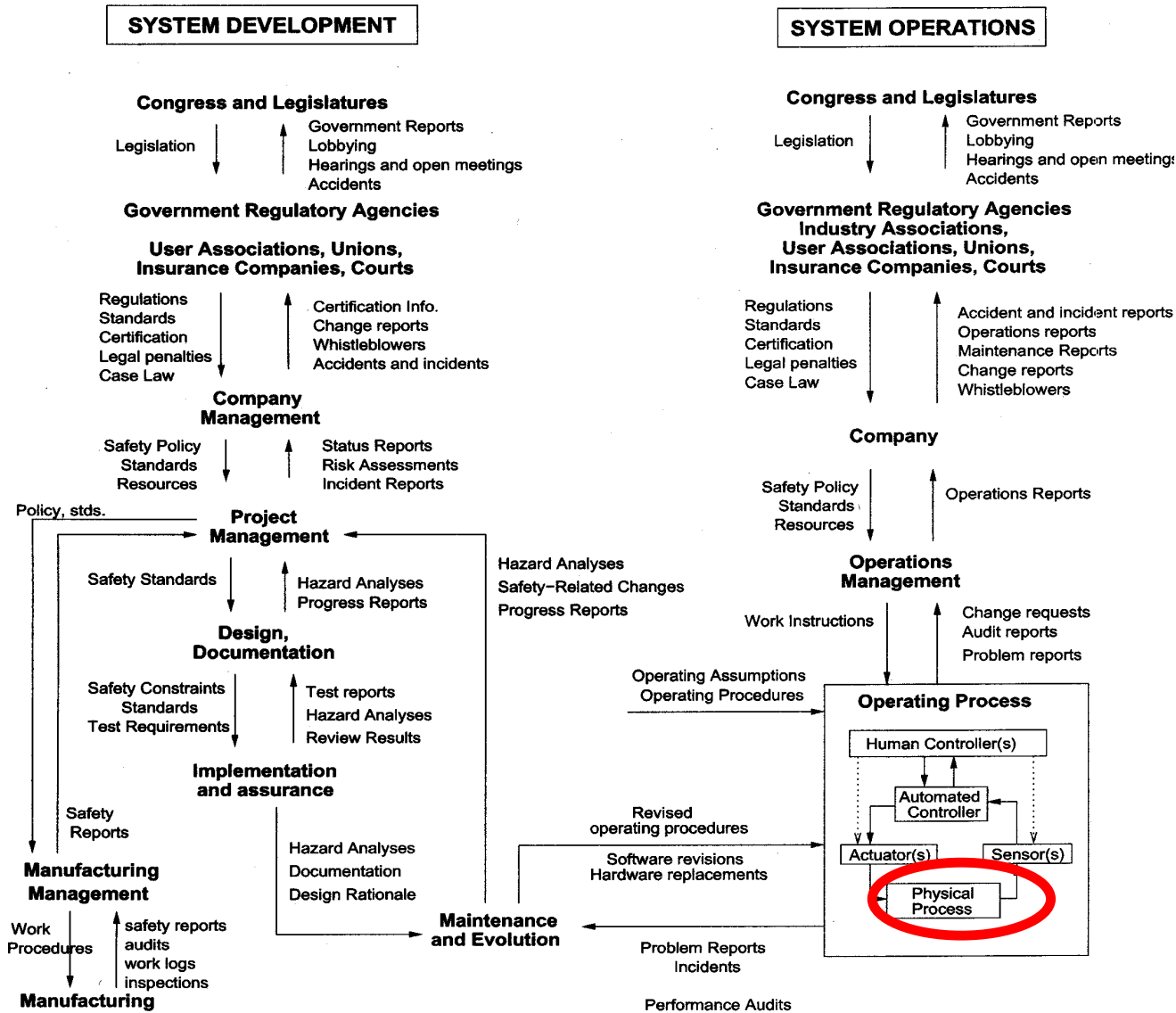
Control structure



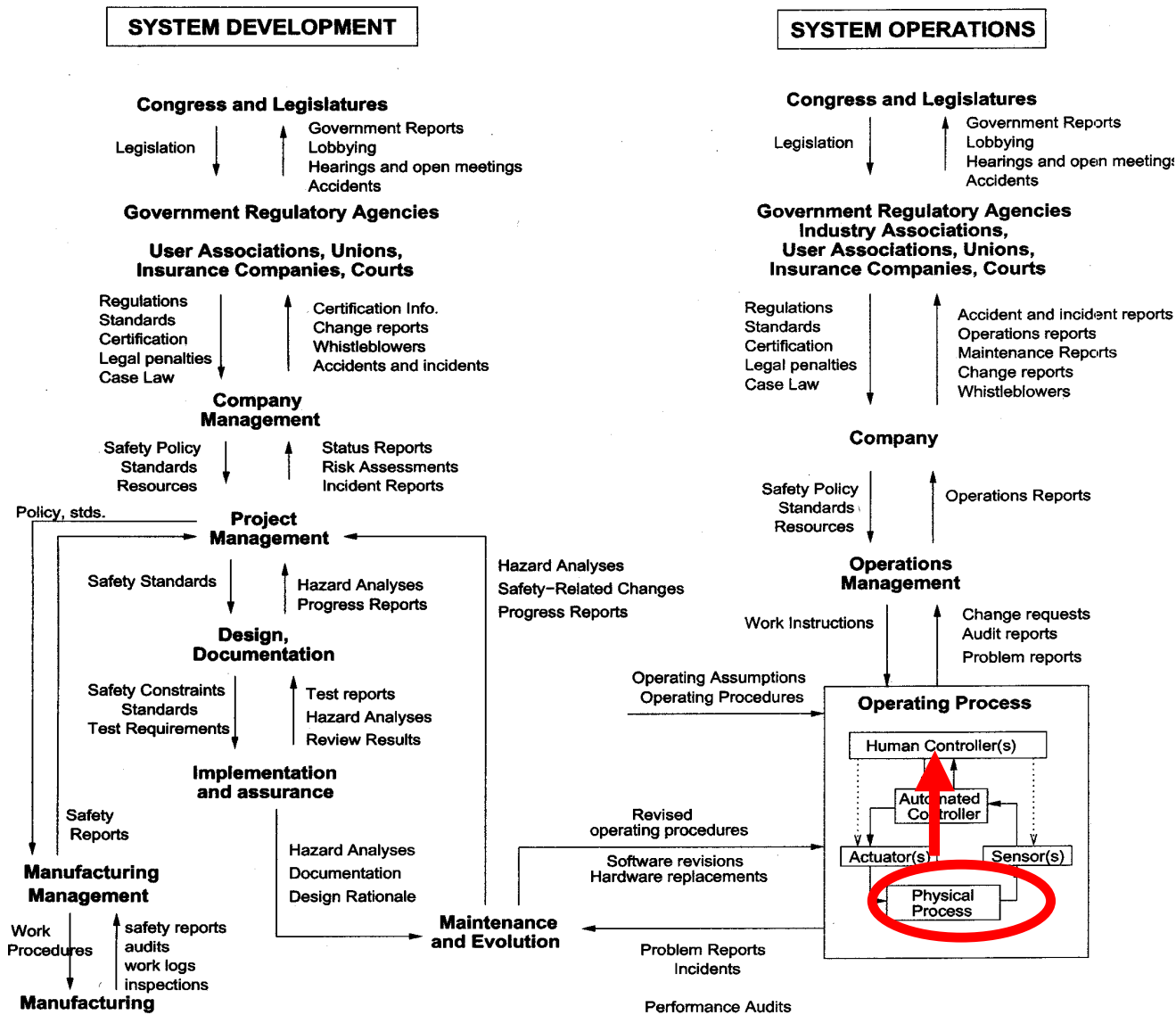
Control structure



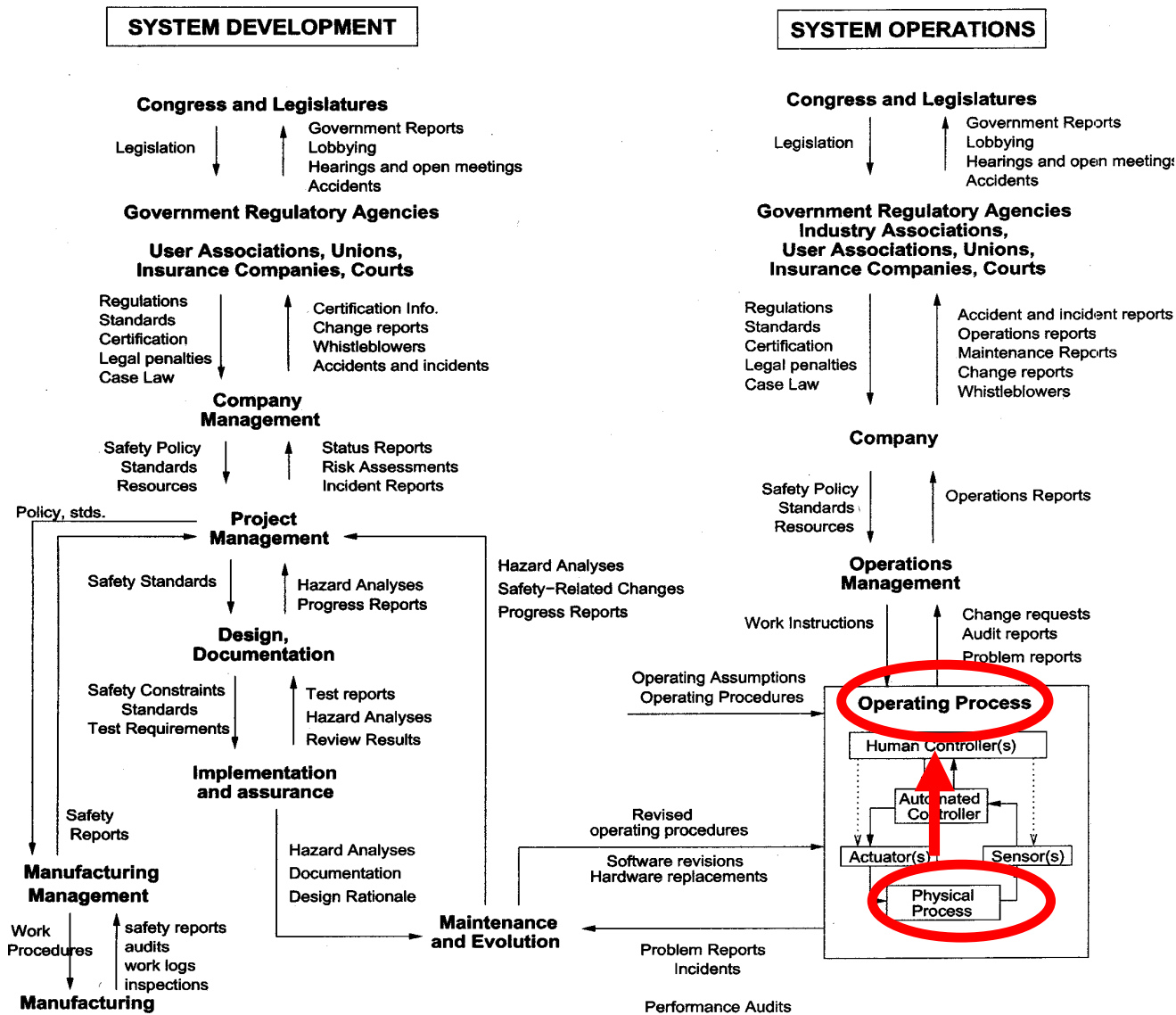
Control structure



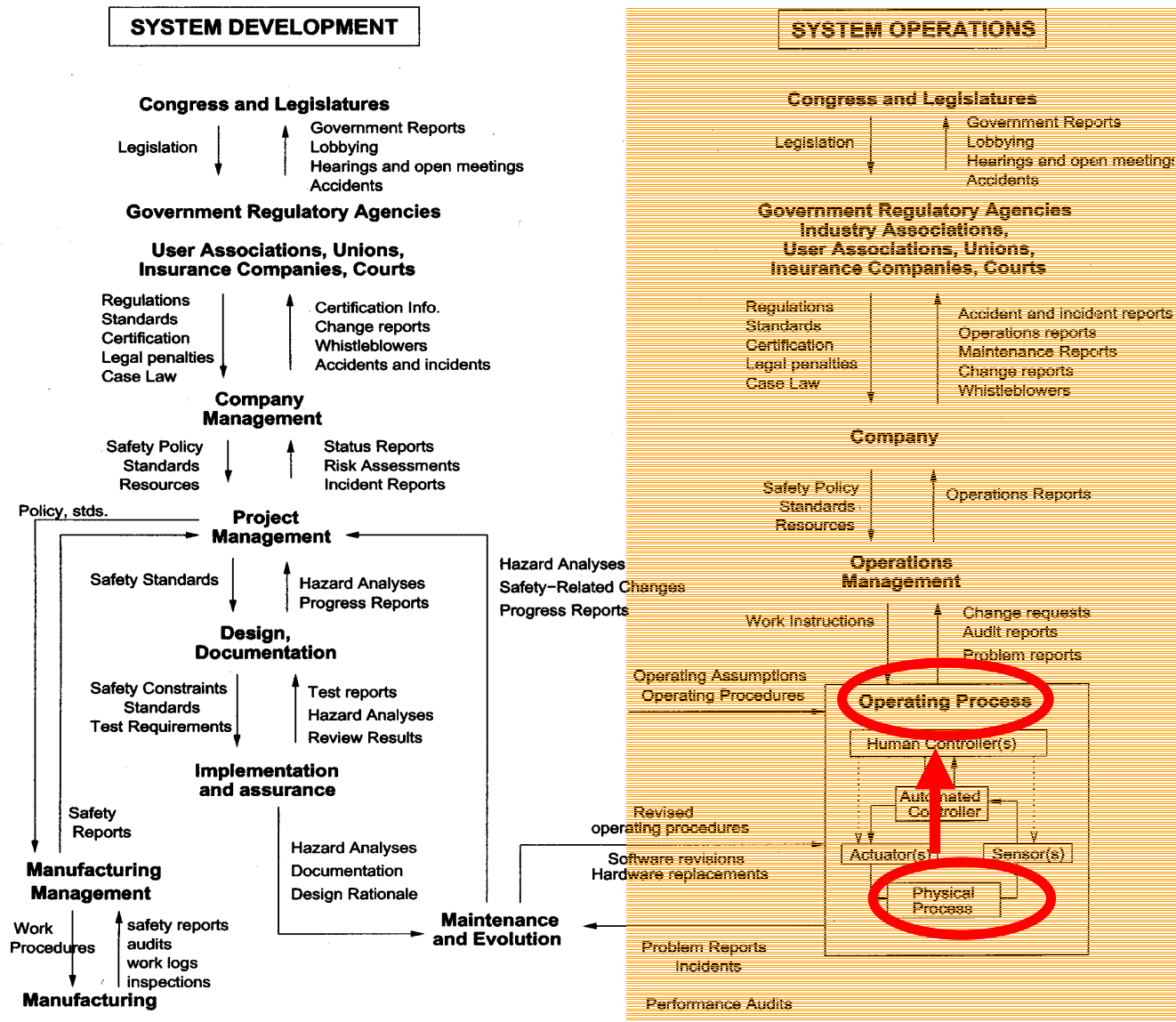
Control structure



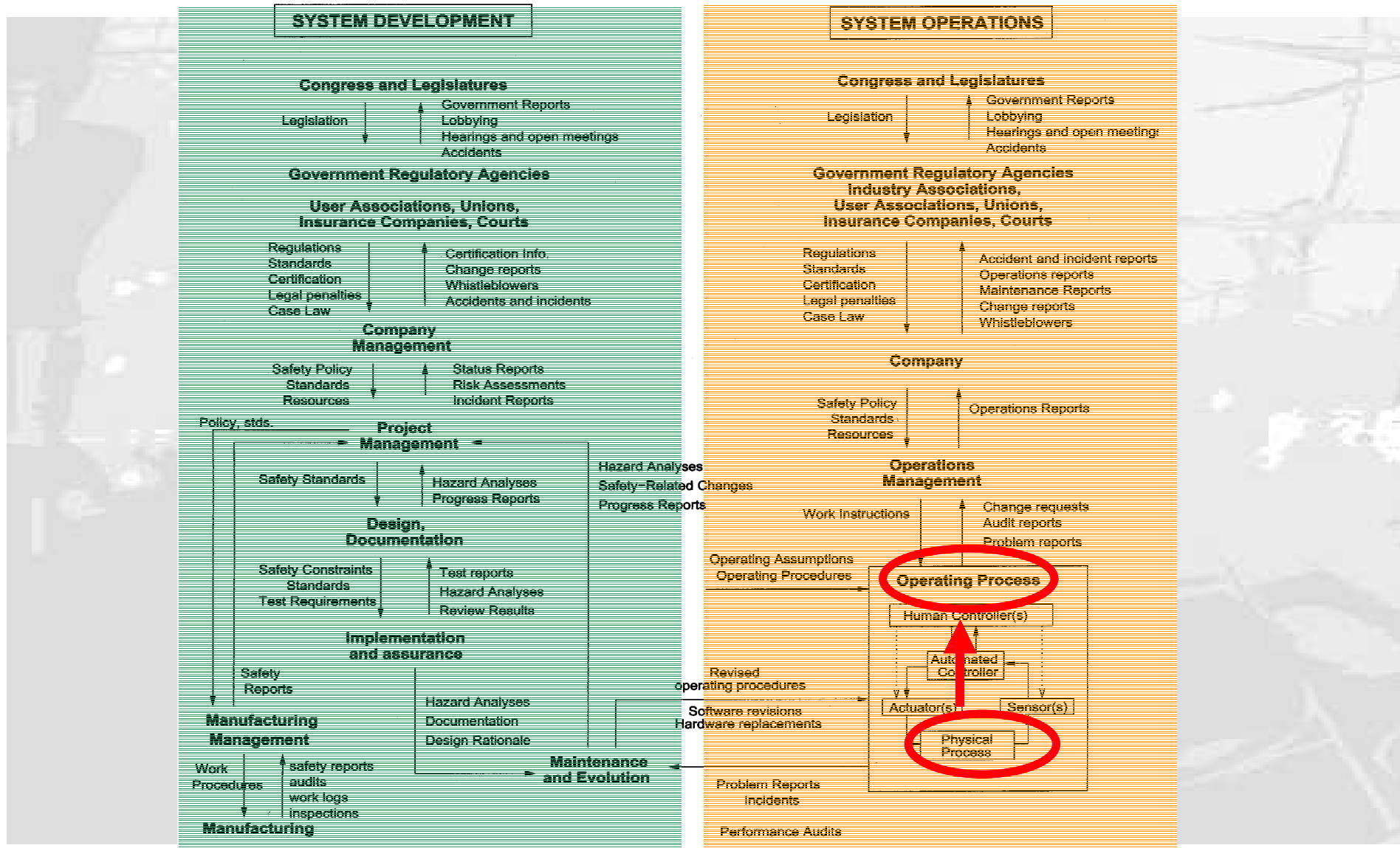
Control structure



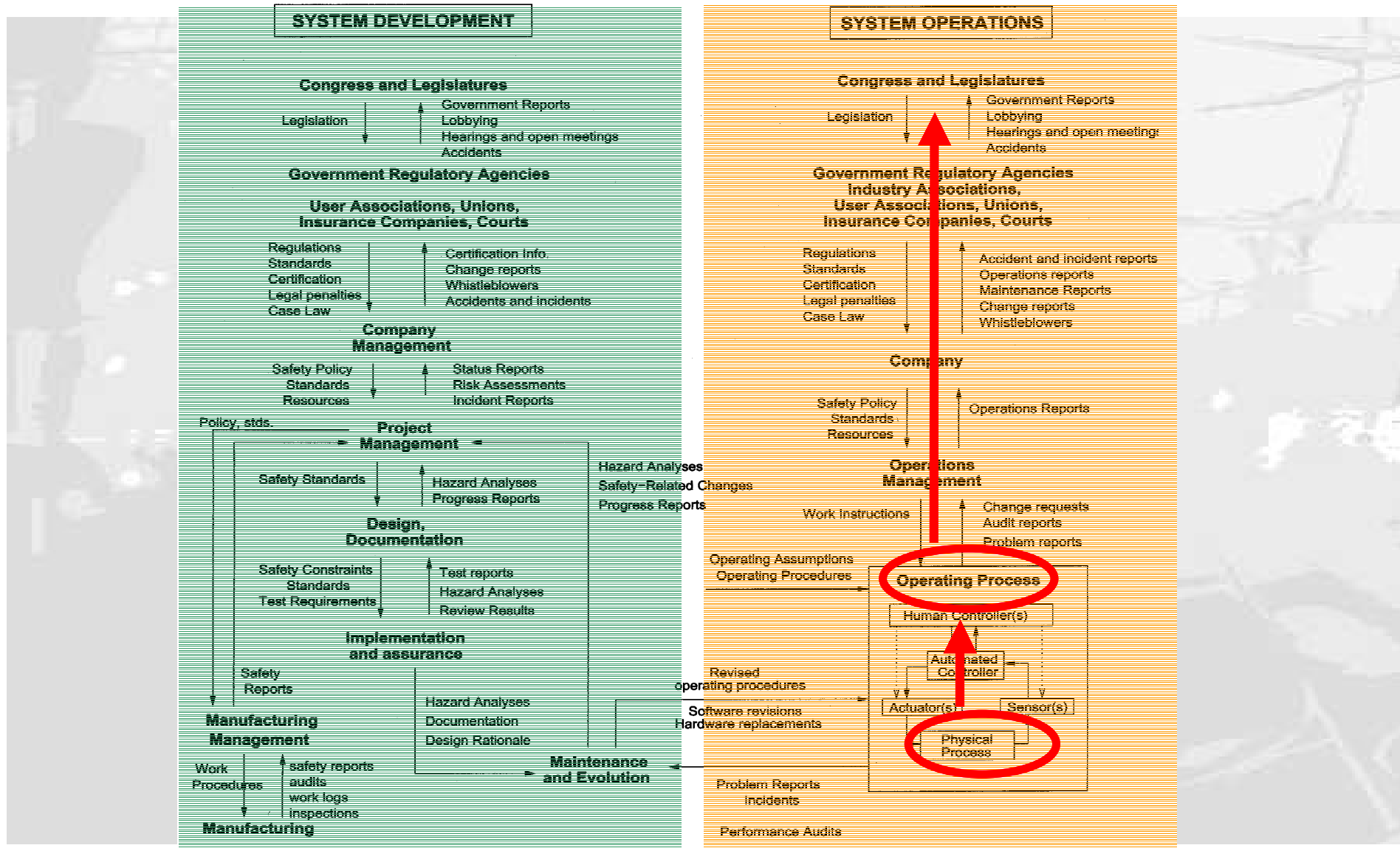
Control structure



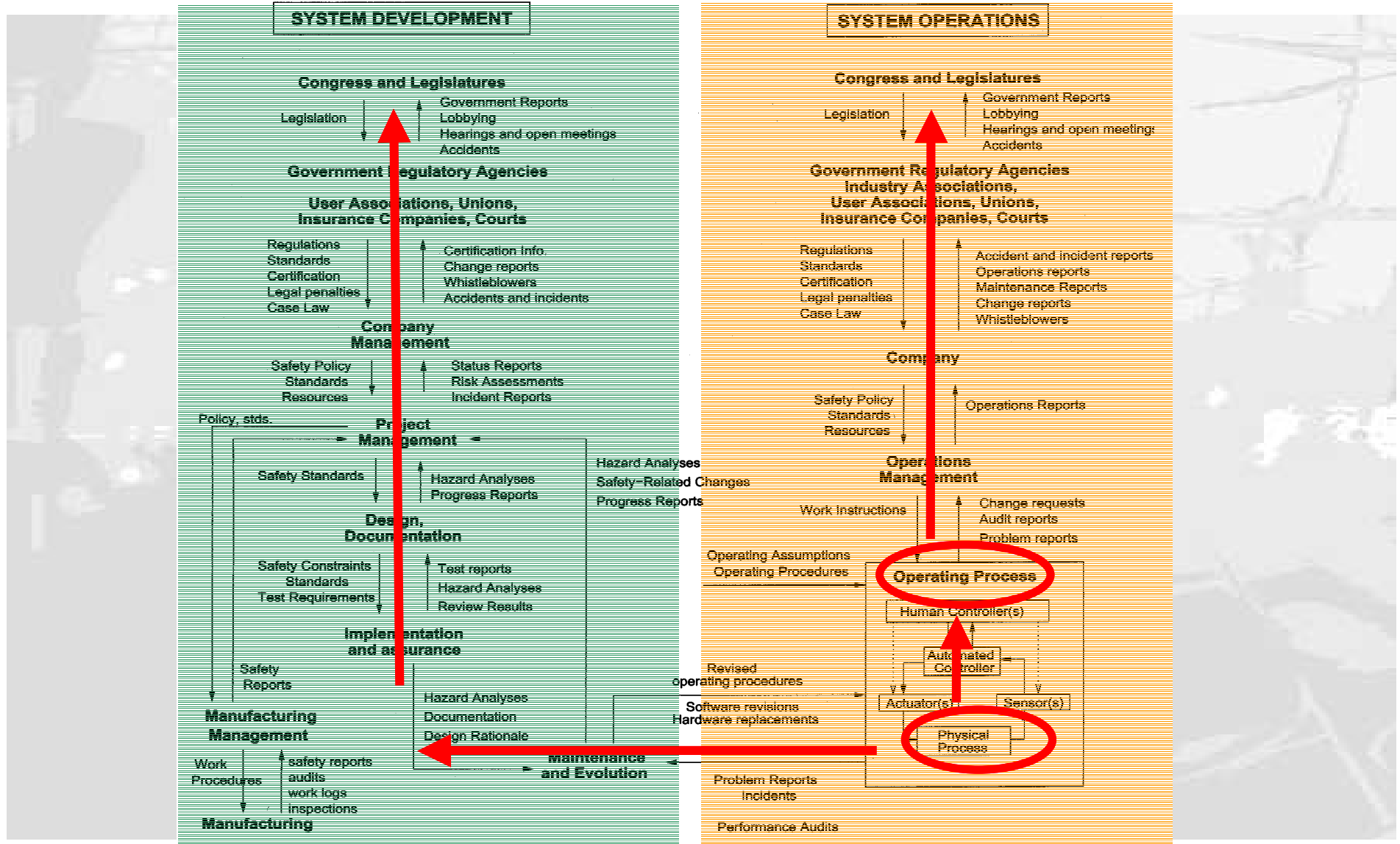
Control structure



Control structure



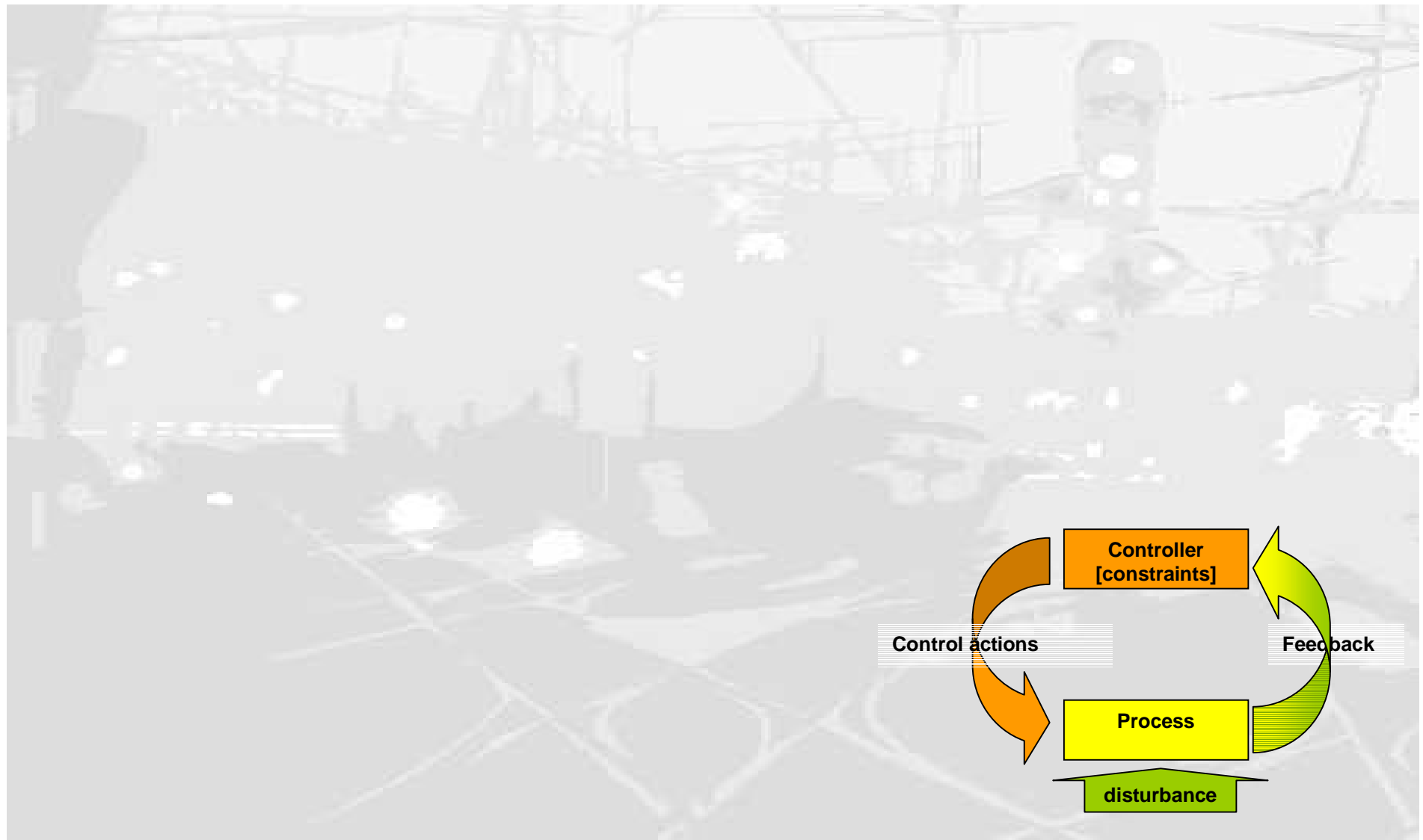
Control structure



Classification of control flaws

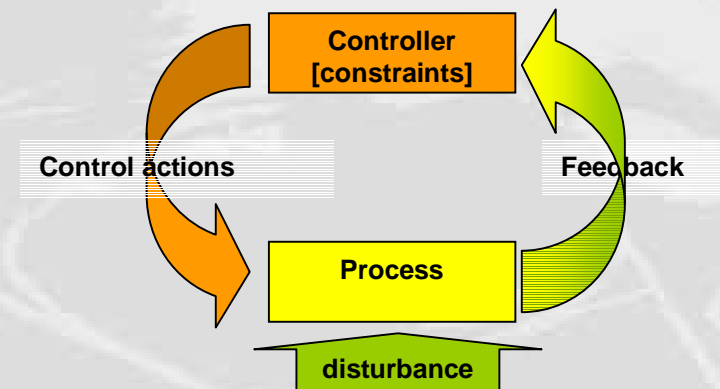


Classification of control flaws



1. Inadequate enforcement of constraints (control actions)

1. Unidentified hazards
2. Inappropriate, ineffective, or missing control actions for identified hazards
 1. ***Design of control algorithm (process) does not enforce constraints***
 2. ***Process models inconsistent, incomplete, or incorrect***
 3. ***Inadequate coordination among controllers and decision makers (boundary and overlap areas)***

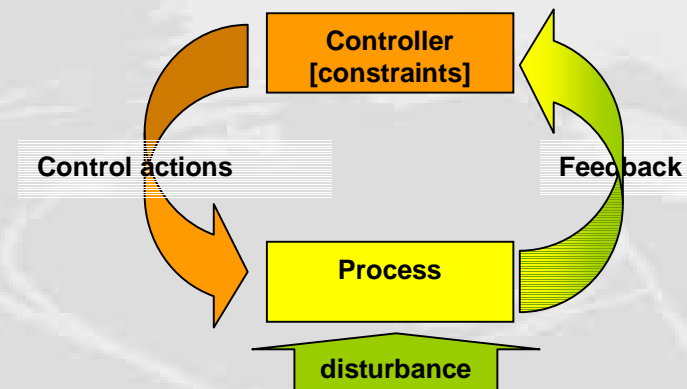


1. Inadequate enforcement of constraints (control actions)

1. Unidentified hazards
2. Inappropriate, ineffective, or missing control actions for identified hazards
 1. ***Design of control algorithm (process) does not enforce constraints***
 2. ***Process models inconsistent, incomplete, or incorrect***
 3. ***Inadequate coordination among controllers and decision makers (boundary and overlap areas)***

2. Inadequate execution of control action

1. Communication flaw
2. Inadequate actuator operation
3. Time lag



1. Inadequate enforcement of constraints (control actions)

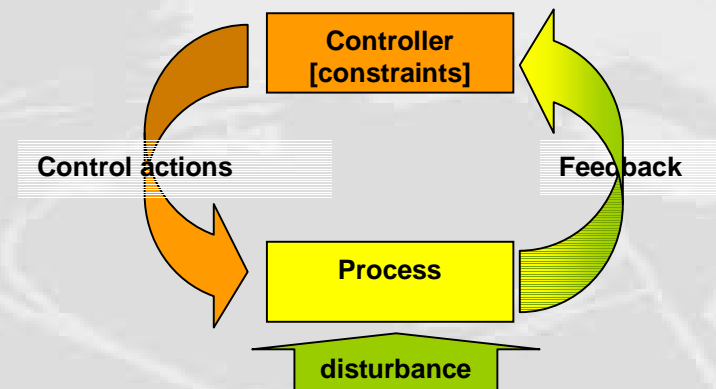
1. Unidentified hazards
2. Inappropriate, ineffective, or missing control actions for identified hazards
 1. ***Design of control algorithm (process) does not enforce constraints***
 2. ***Process models inconsistent, incomplete, or incorrect***
 3. ***Inadequate coordination among controllers and decision makers (boundary and overlap areas)***

2. Inadequate execution of control action

1. Communication flaw
2. Inadequate actuator operation
3. Time lag

3. Inadequate or missing feedback

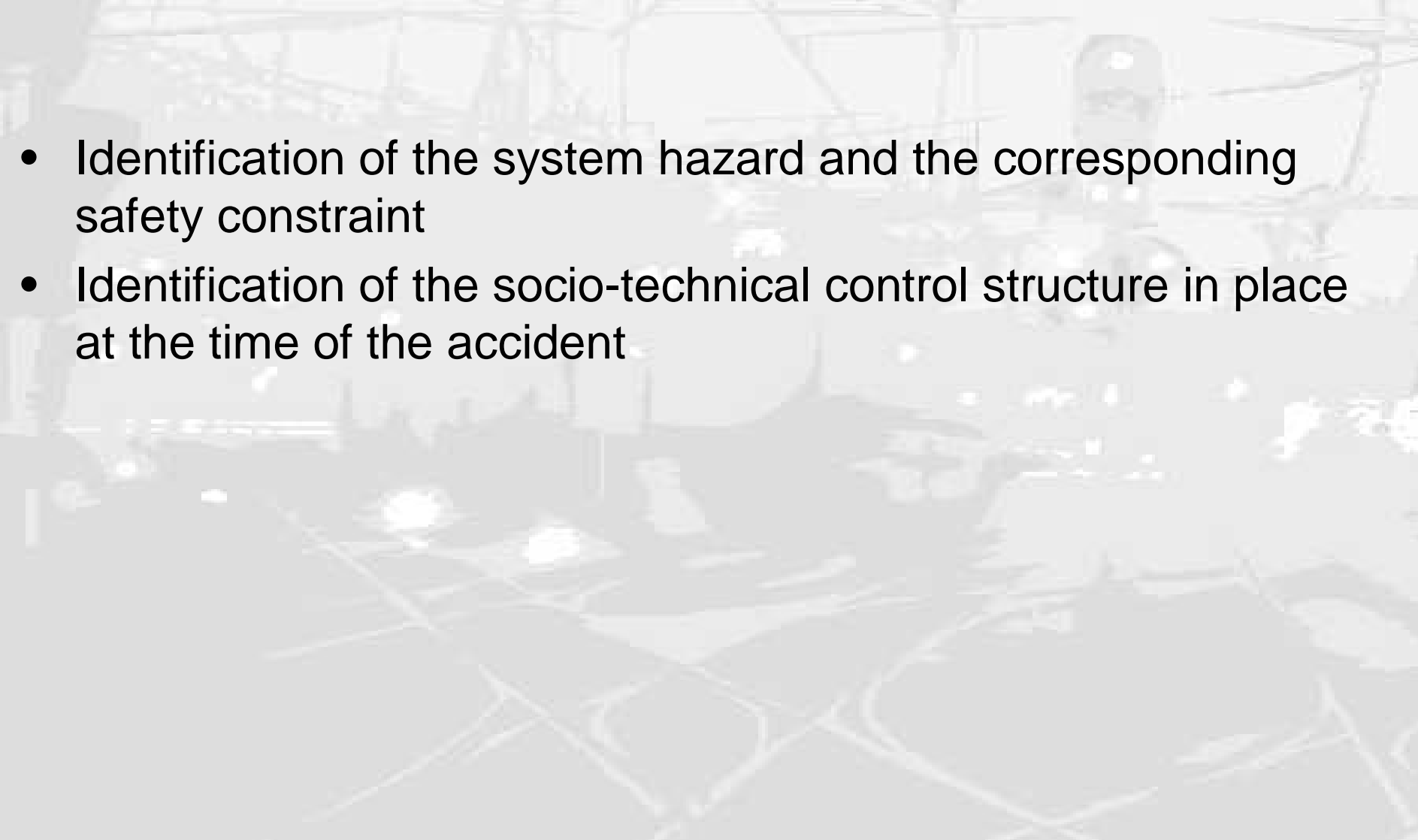
1. Not provided in system design
2. Communication flaw
3. Inadequate sensor operation
4. Time lag

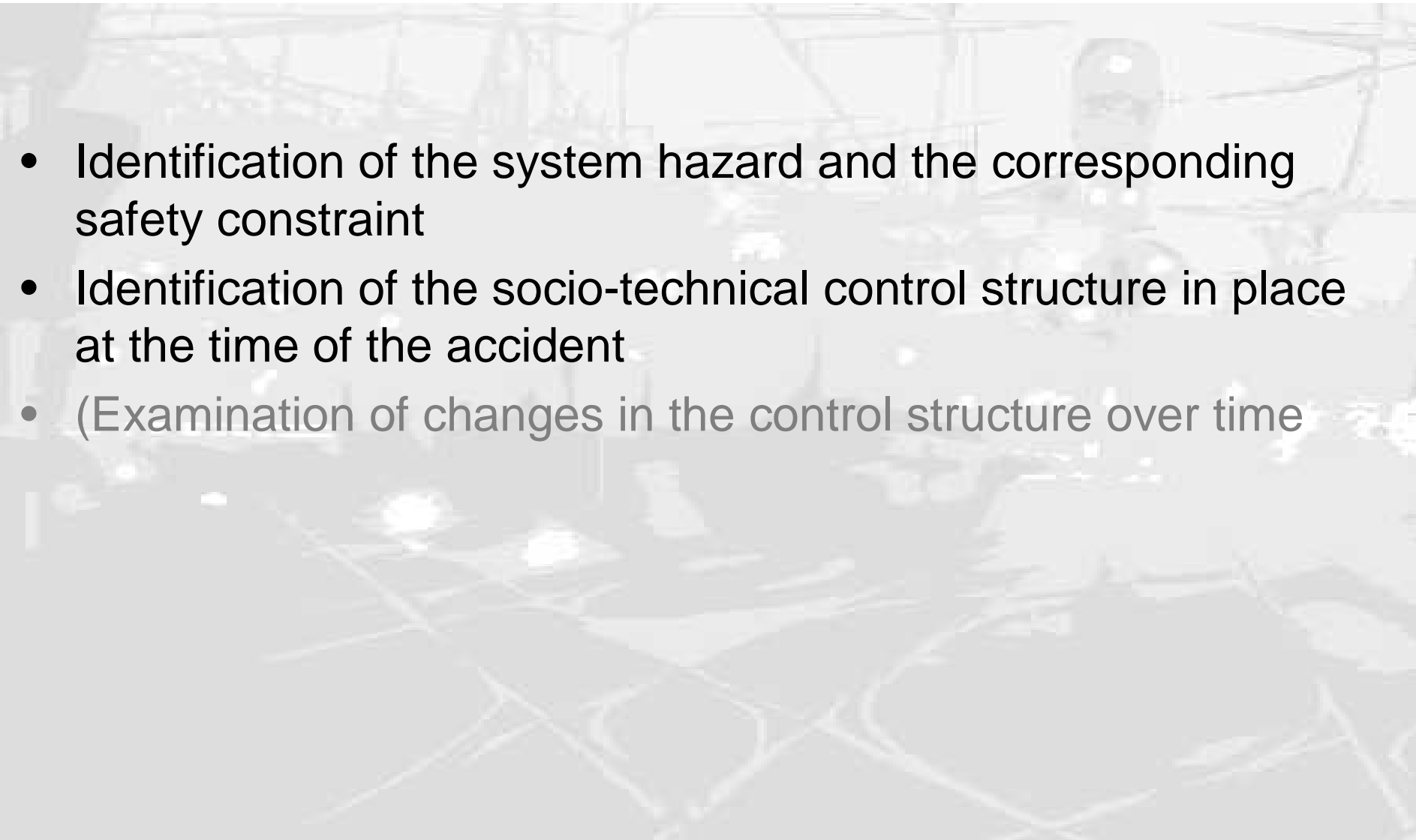


Proposed analysis procedure



- Identification of the system hazard and the corresponding safety constraint

- 
- Identification of the system hazard and the corresponding safety constraint
 - Identification of the socio-technical control structure in place at the time of the accident

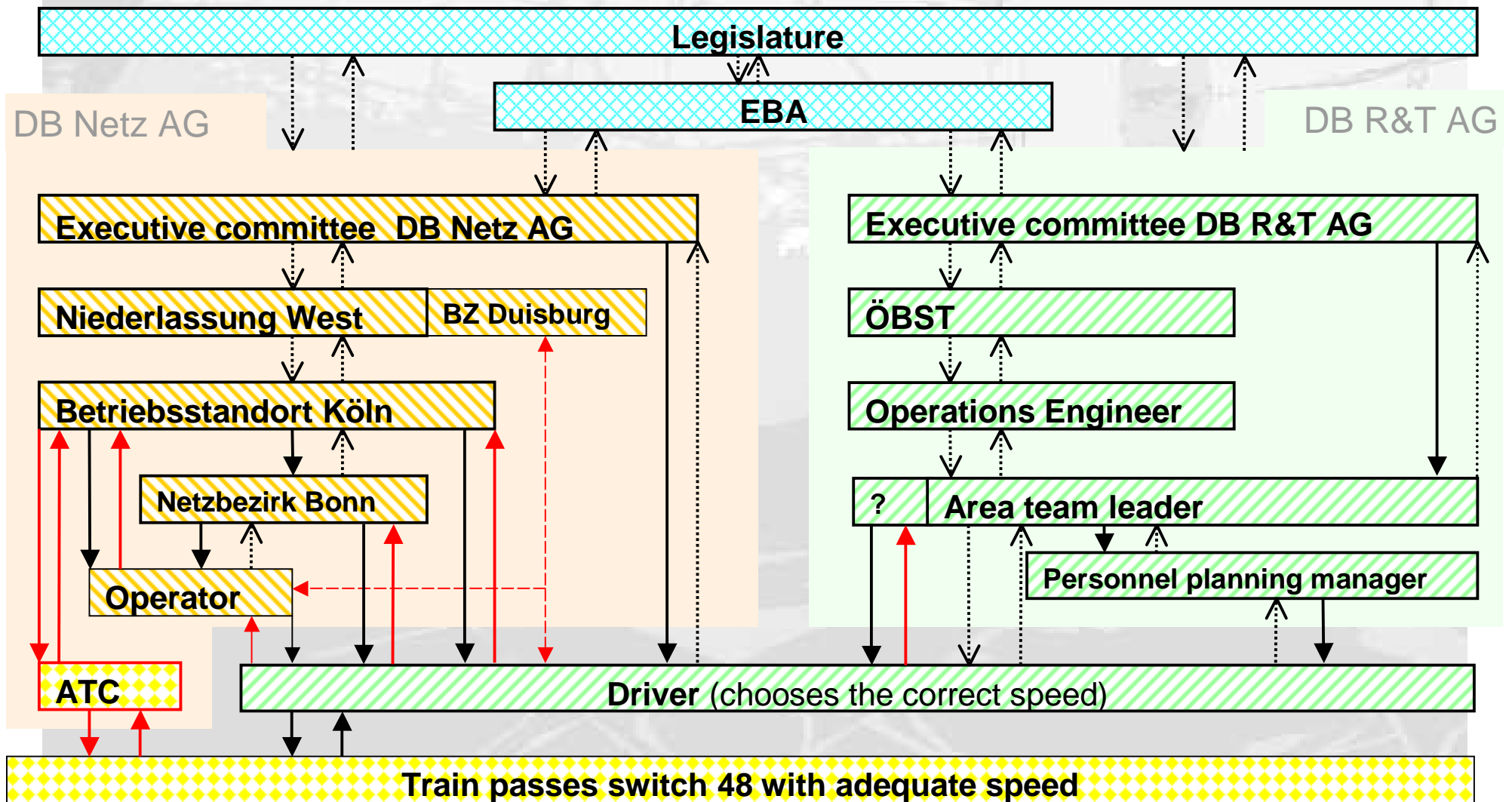
- 
- Identification of the system hazard and the corresponding safety constraint
 - Identification of the socio-technical control structure in place at the time of the accident
 - (Examination of changes in the control structure over time

- Identification of the system hazard and the corresponding safety constraint
- Identification of the socio-technical control structure in place at the time of the accident
- (Examination of changes in the control structure over time
- Visualization of these changes using a system dynamics model)

- Identification of the system hazard and the corresponding safety constraint
- Identification of the socio-technical control structure in place at the time of the accident
- (Examination of changes in the control structure over time
- Visualization of these changes using a system dynamics model)
- Documentation of the results for each process of the control structure

1. An introduction to STAMP
2. An analysis of Brühl using STAMP
3. Results and experiences

Control structure operation



1) Visual Analysis

- There are two separate control structures within the operations structure
- The driver is being controlled by six different control loops
- Many feedback channels are missing
- Official reports focus on lower levels in the control structure

2) In depth Analysis

- Analysis of each control loop
- Classification of Control Flaws

Control structure operation

DB Netz AG

DB R&T AG

ATC

Control structure operation

DB Netz AG

DB R&T AG

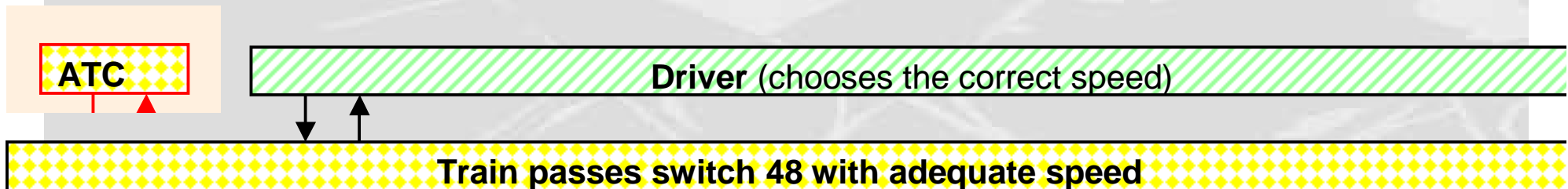
ATC

Train passes switch 48 with adequate speed

Control structure operation

DB Netz AG

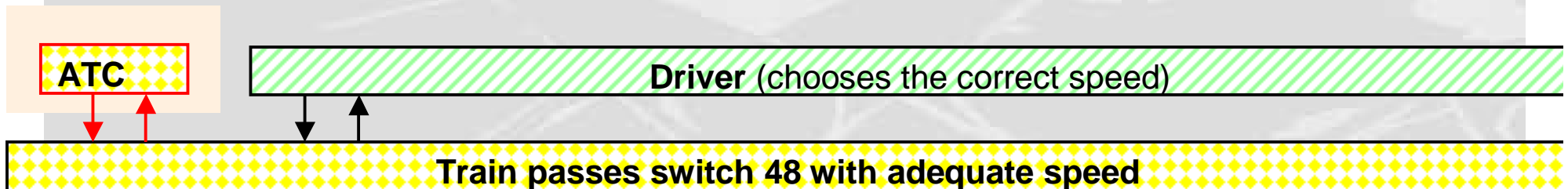
DB R&T AG



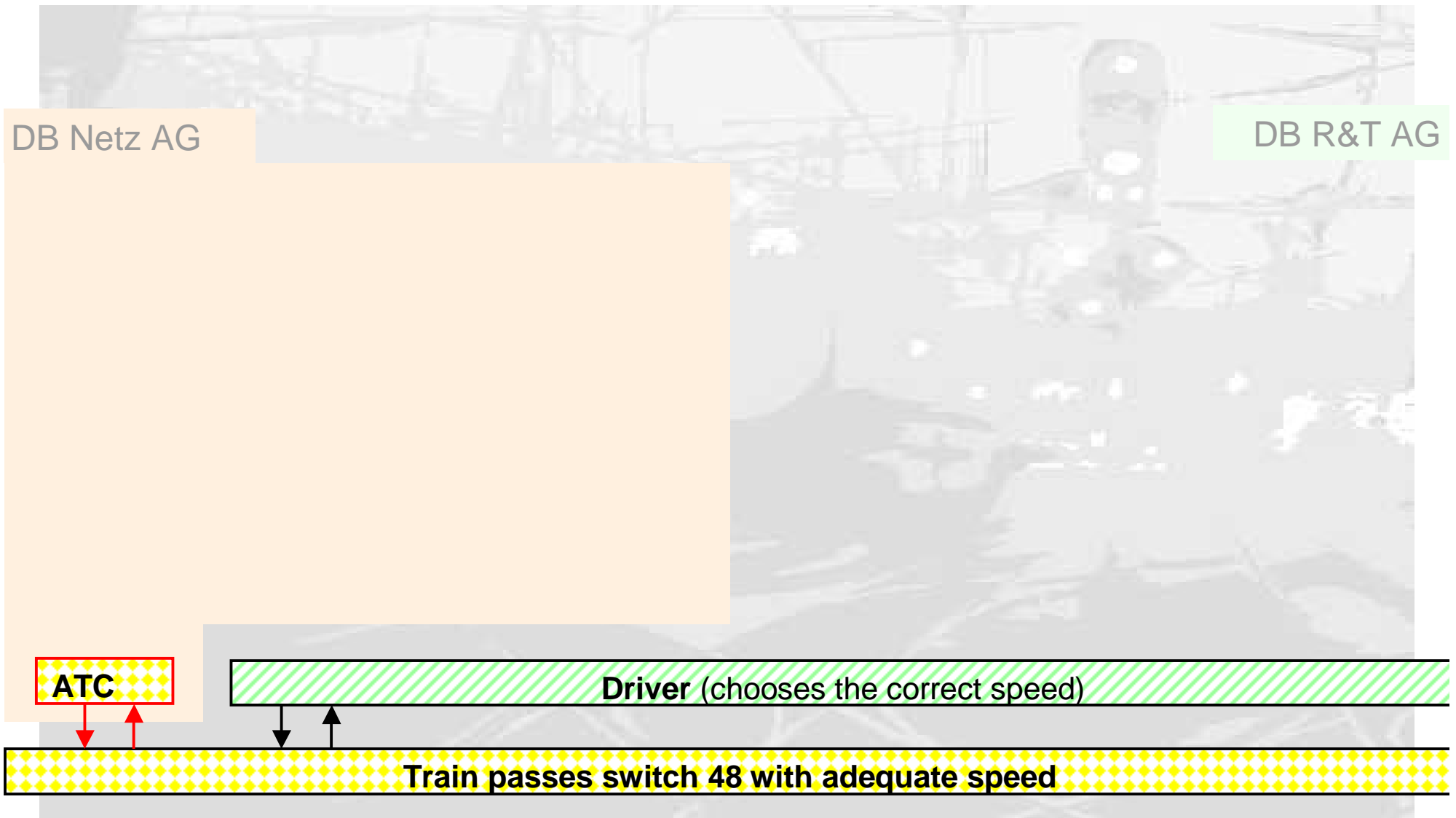
Control structure operation

DB Netz AG

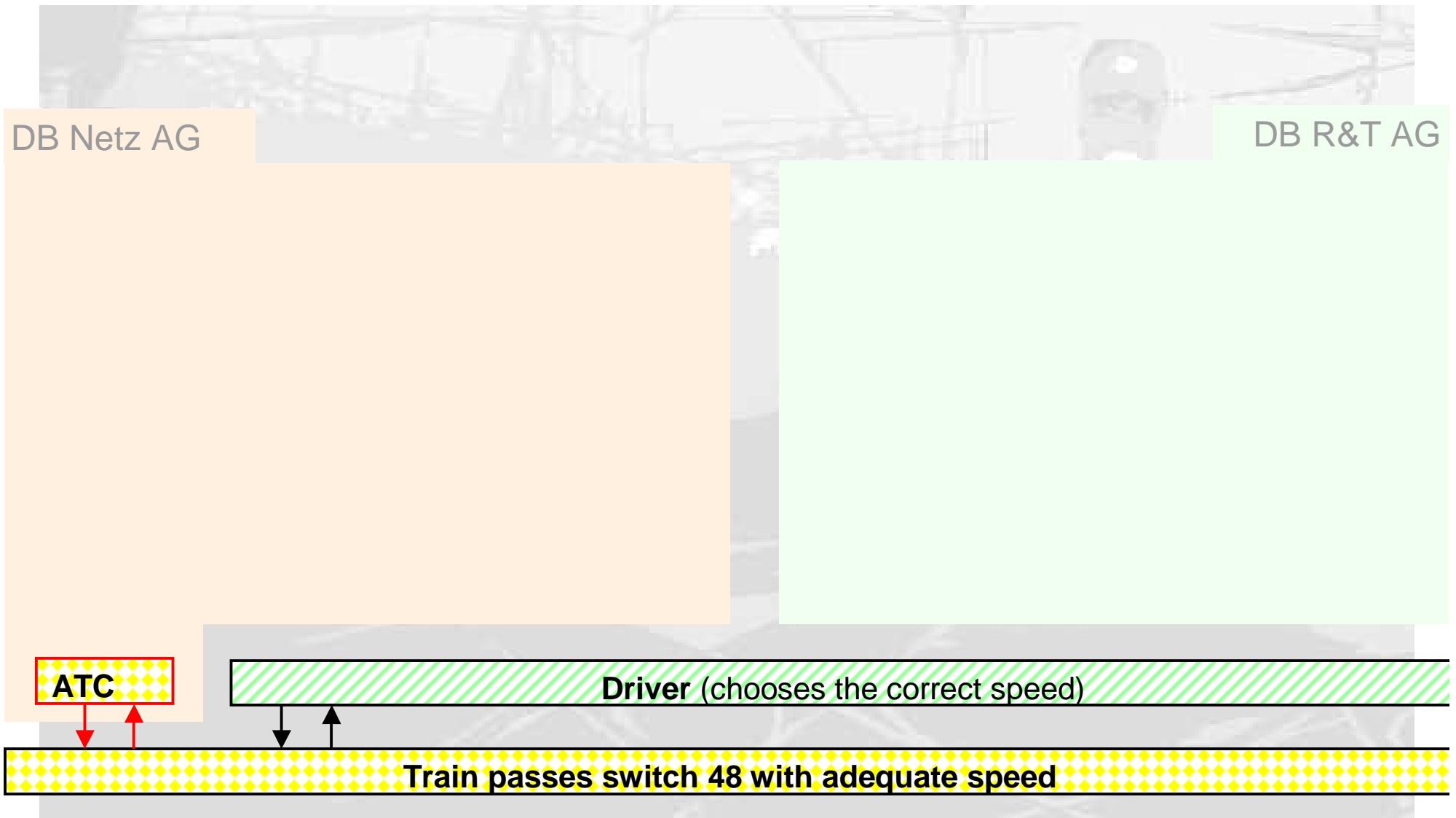
DB R&T AG



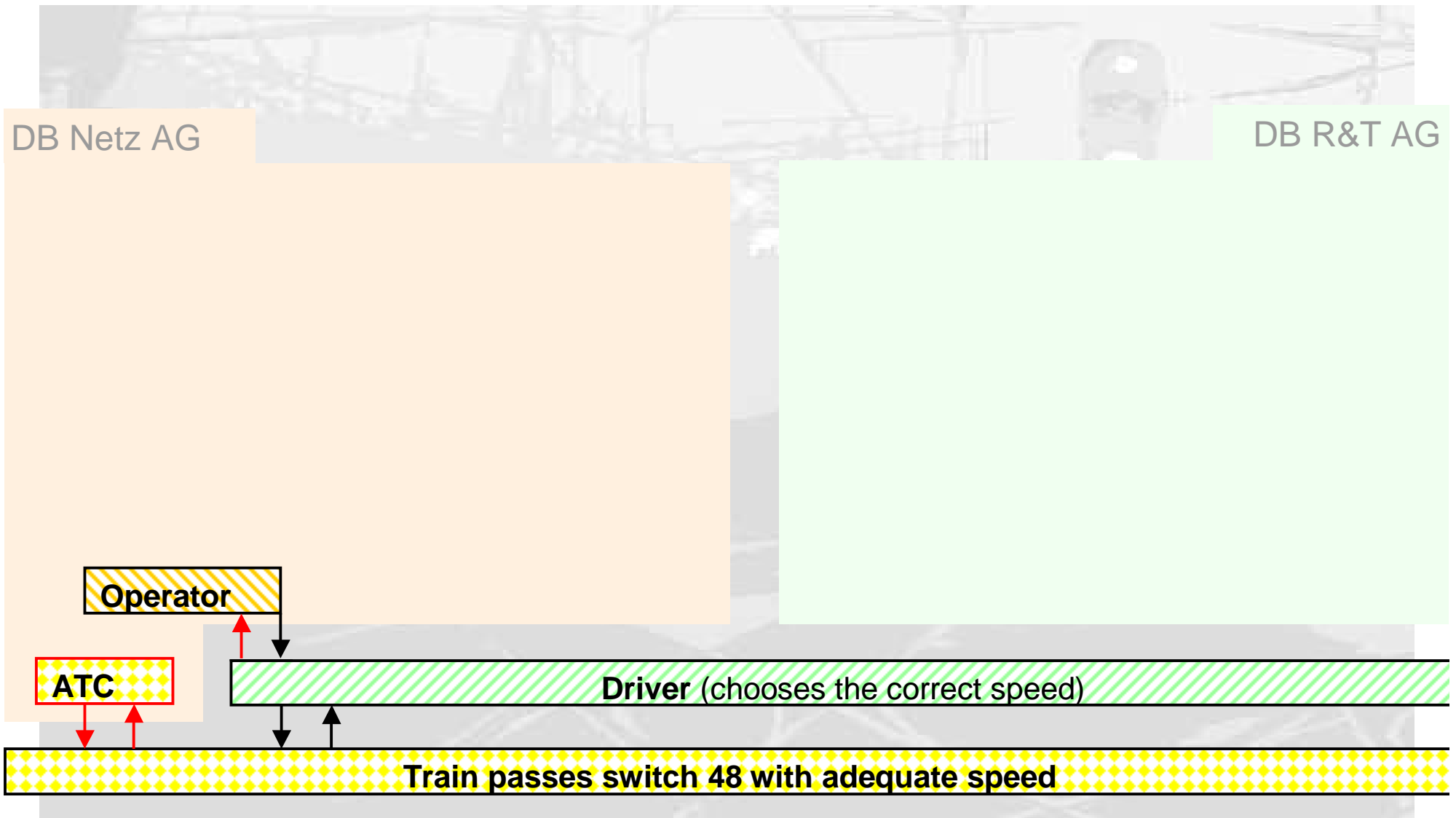
Control structure operation



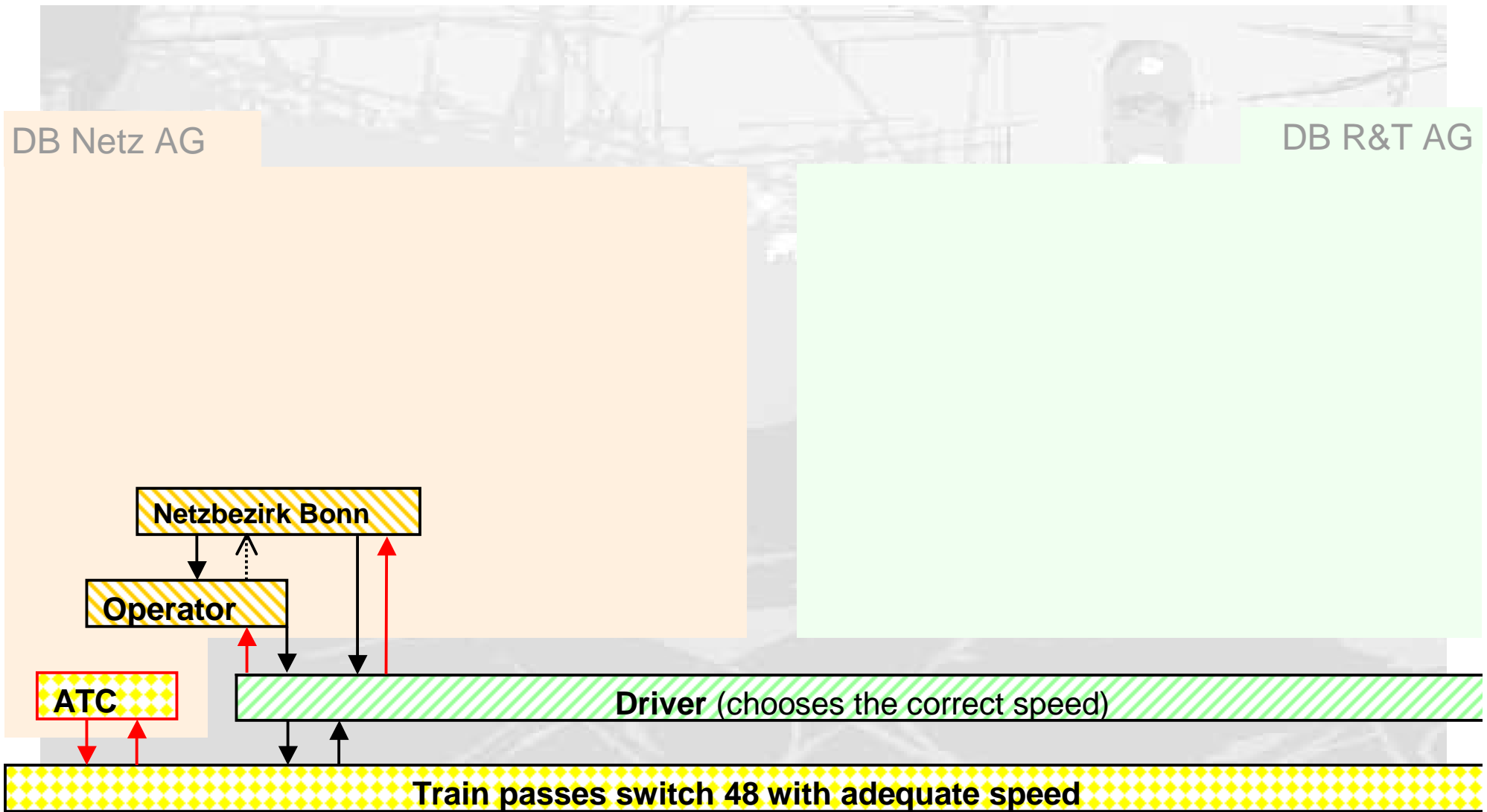
Control structure operation



Control structure operation



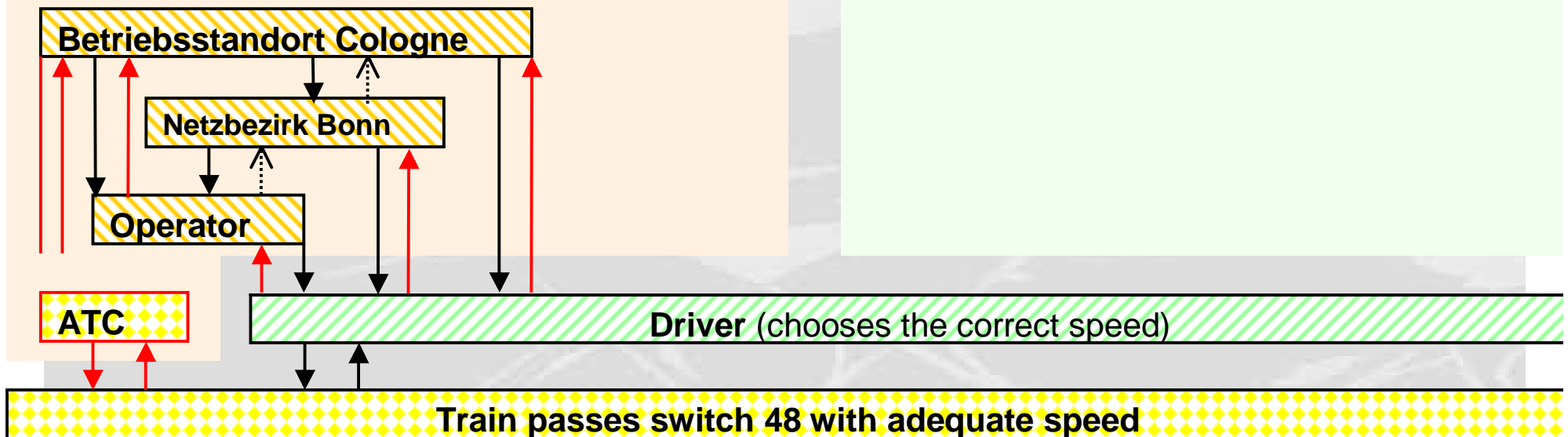
Control structure operation



Control structure operation

DB Netz AG

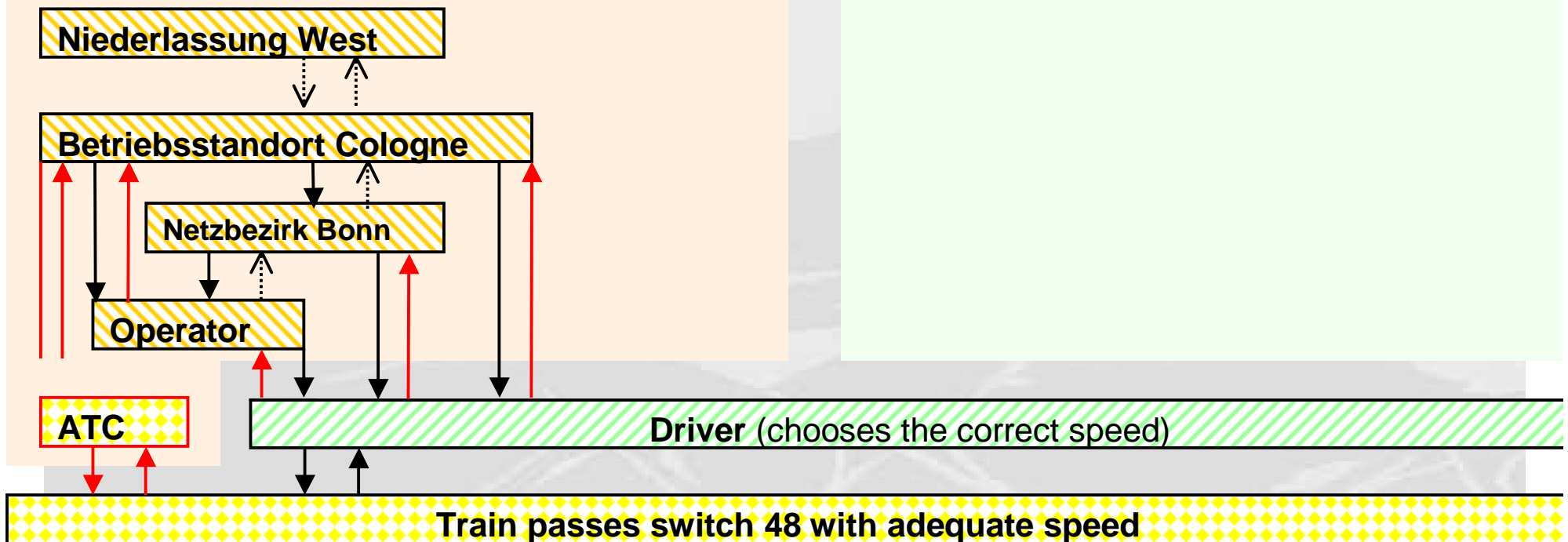
DB R&T AG



Control structure operation

DB Netz AG

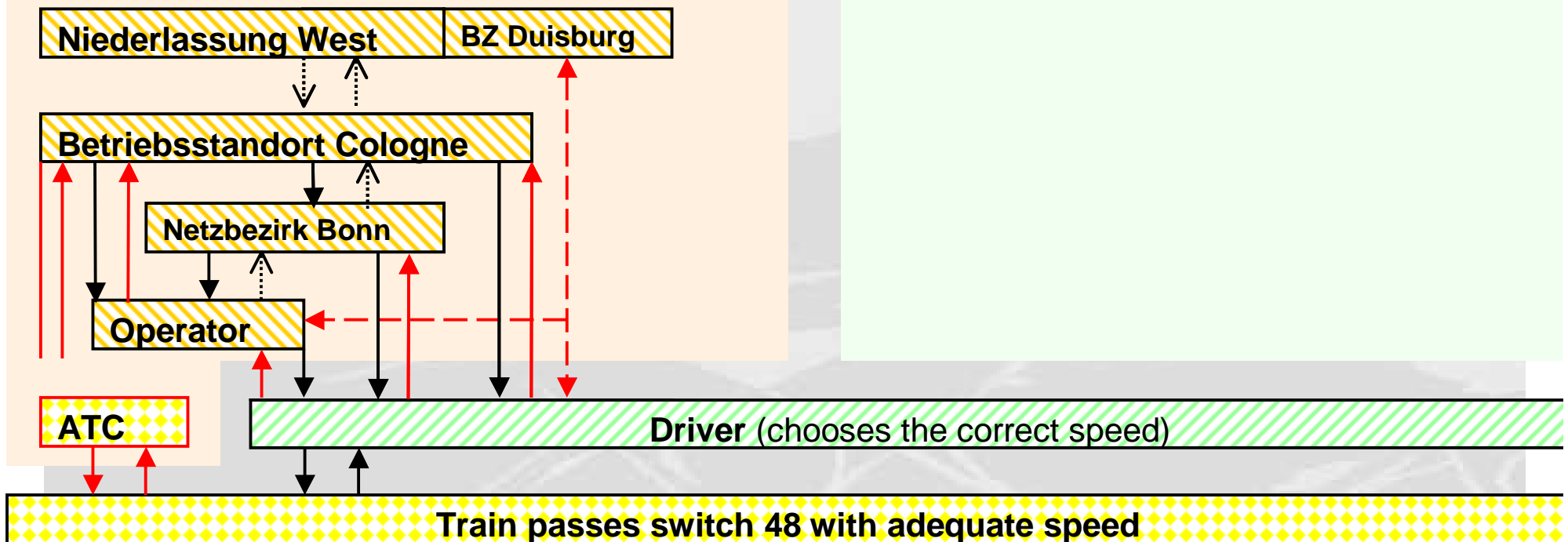
DB R&T AG



Control structure operation

DB Netz AG

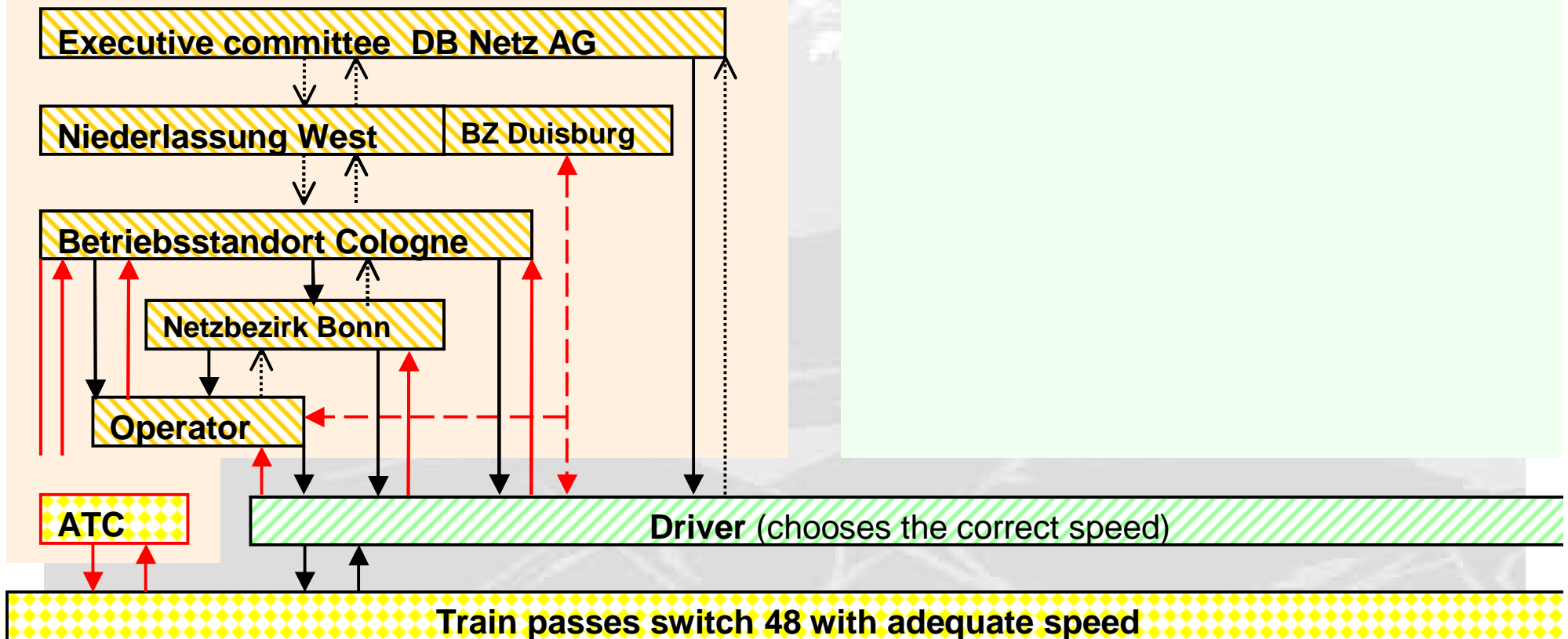
DB R&T AG



Control structure operation

DB Netz AG

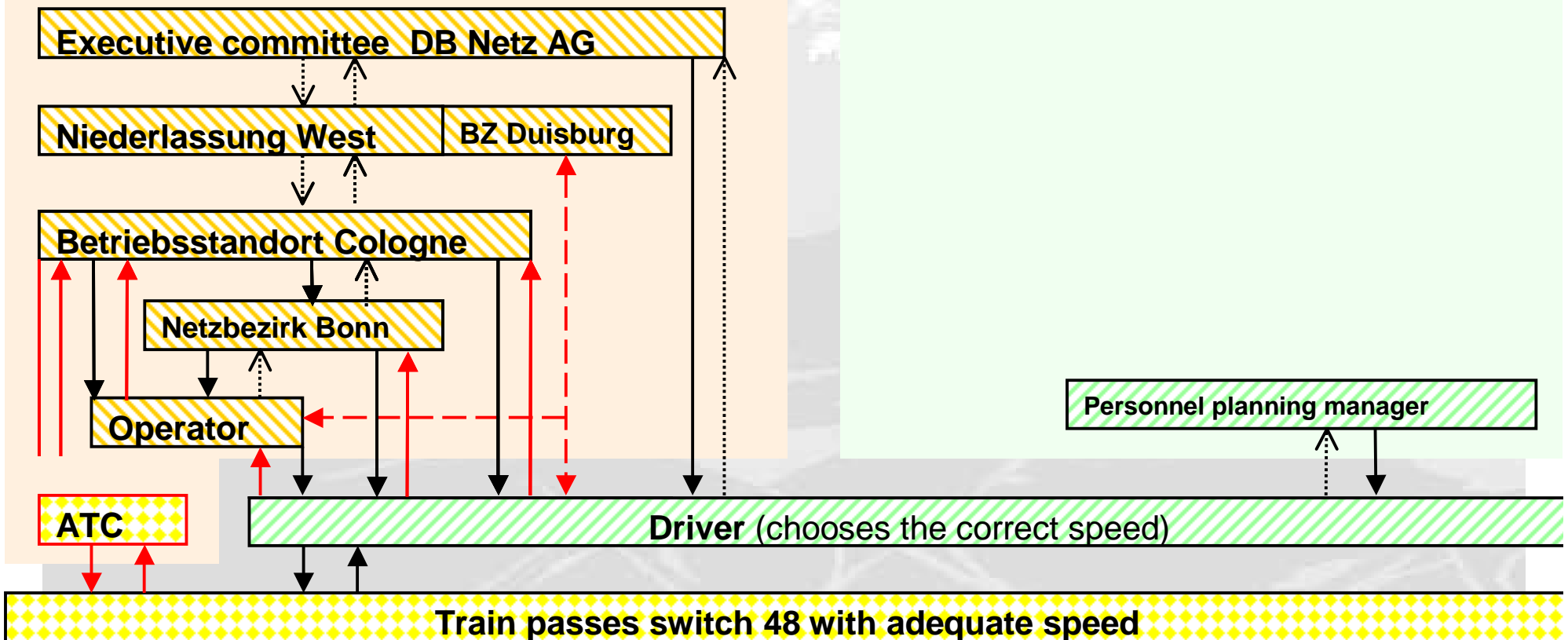
DB R&T AG



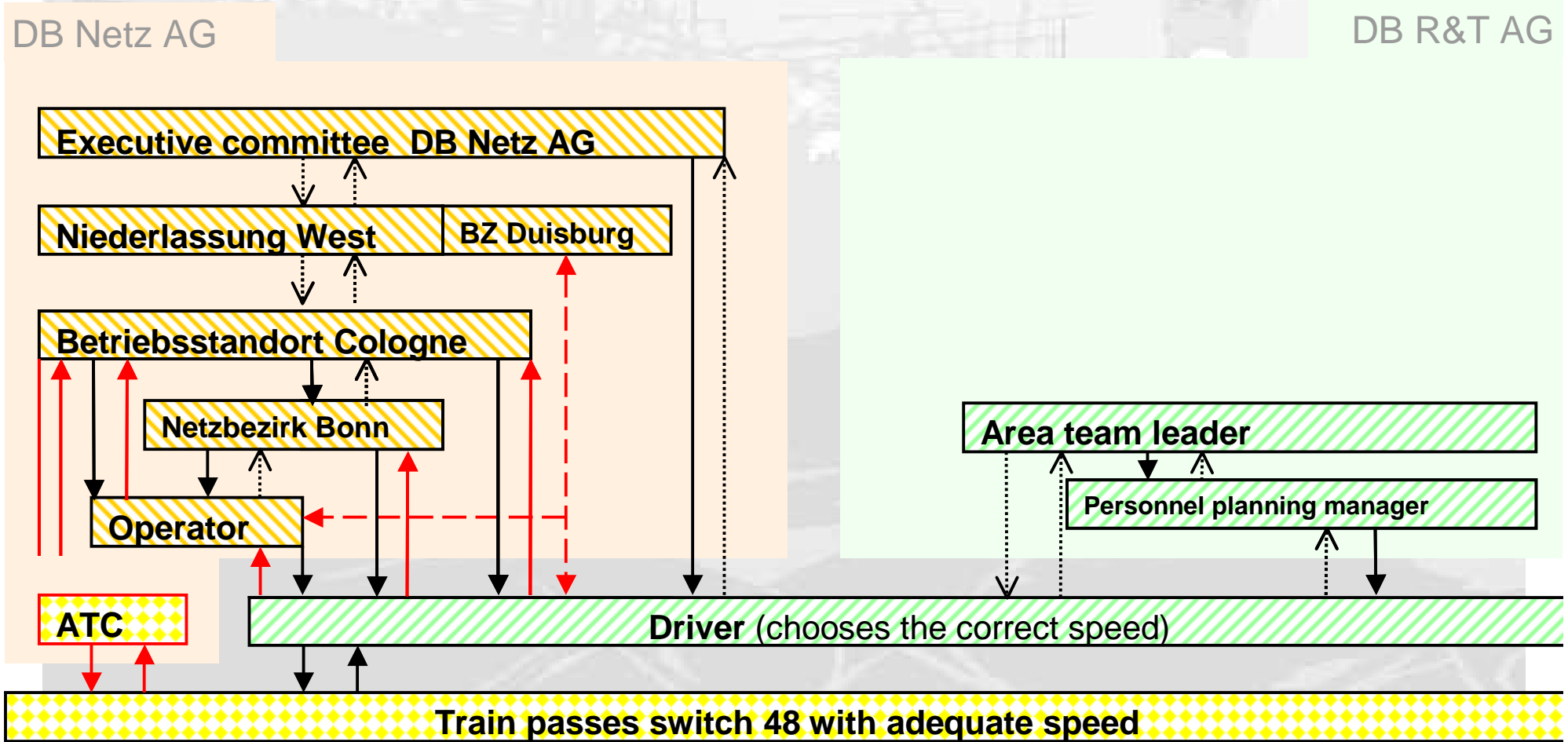
Control structure operation

DB Netz AG

DB R&T AG



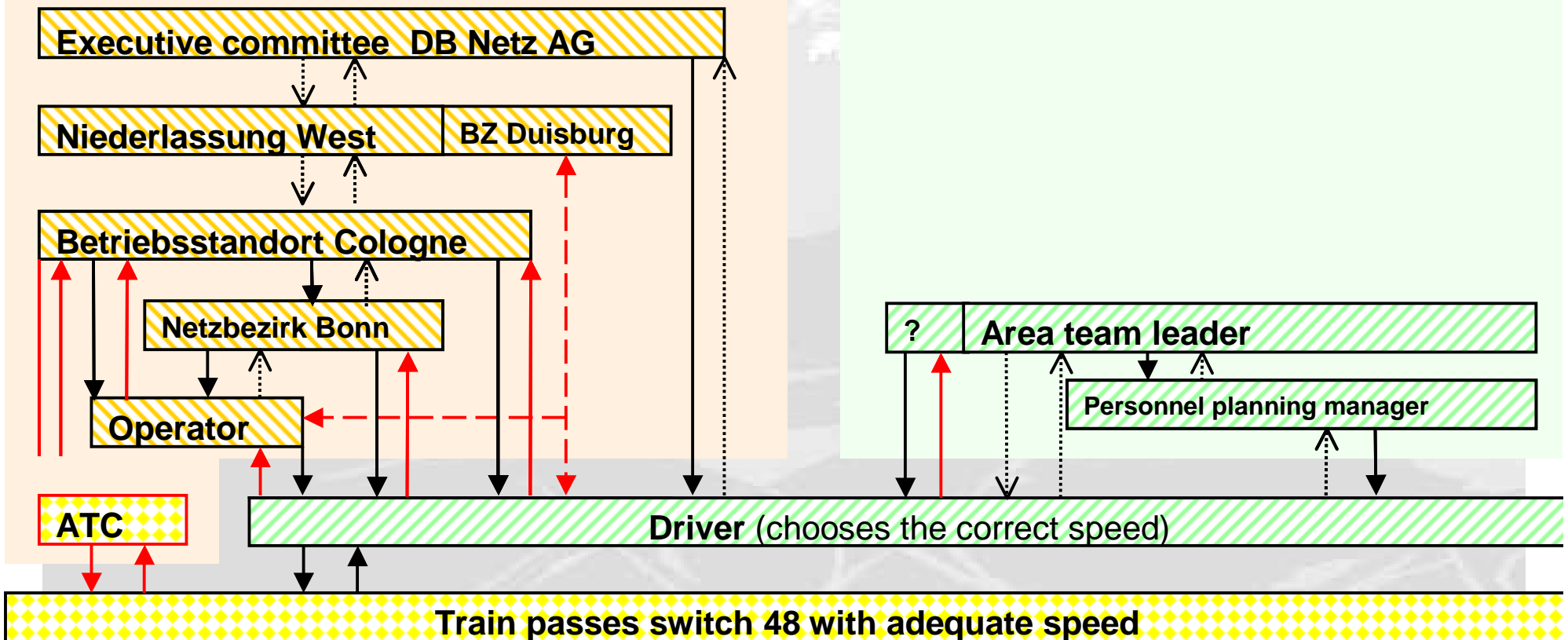
Control structure operation



Control structure operation

DB Netz AG

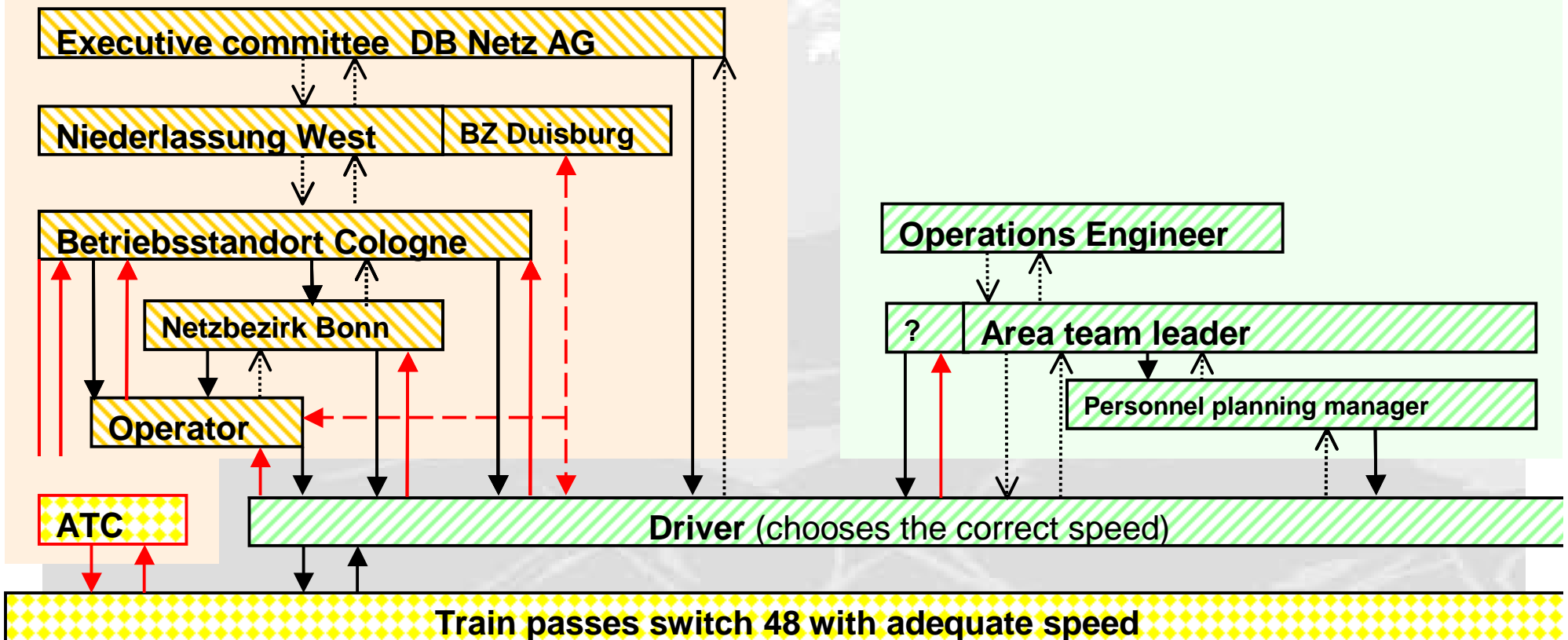
DB R&T AG



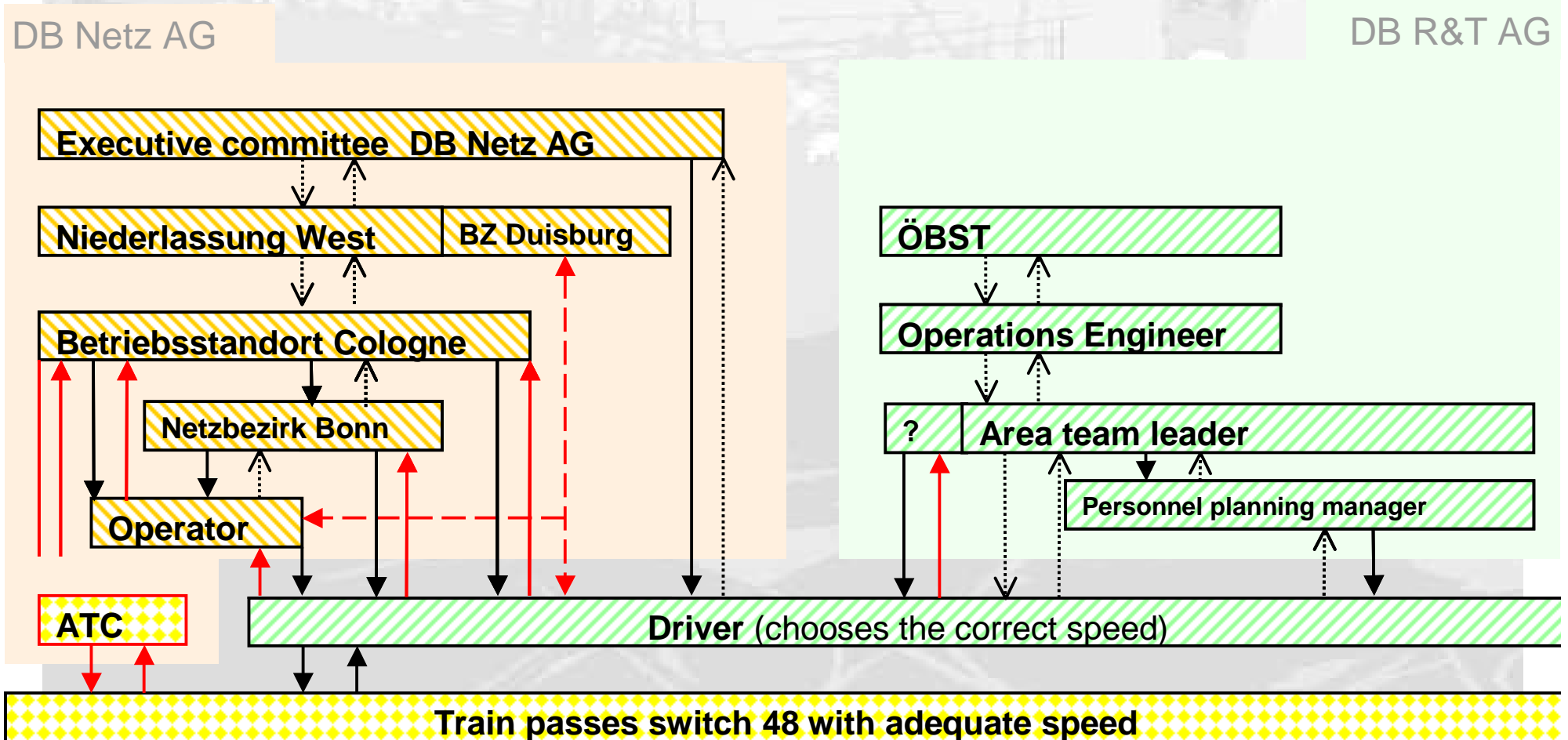
Control structure operation

DB Netz AG

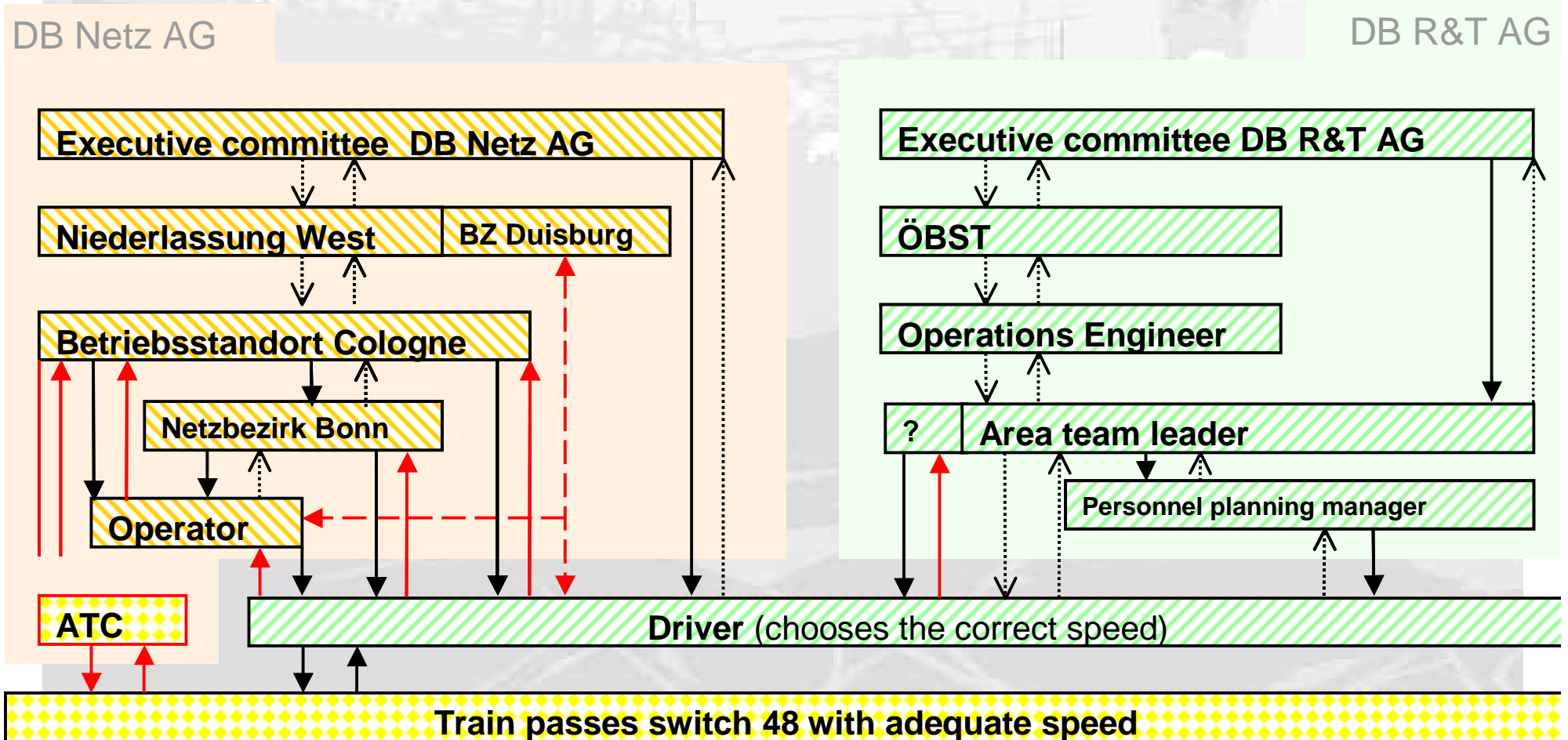
DB R&T AG



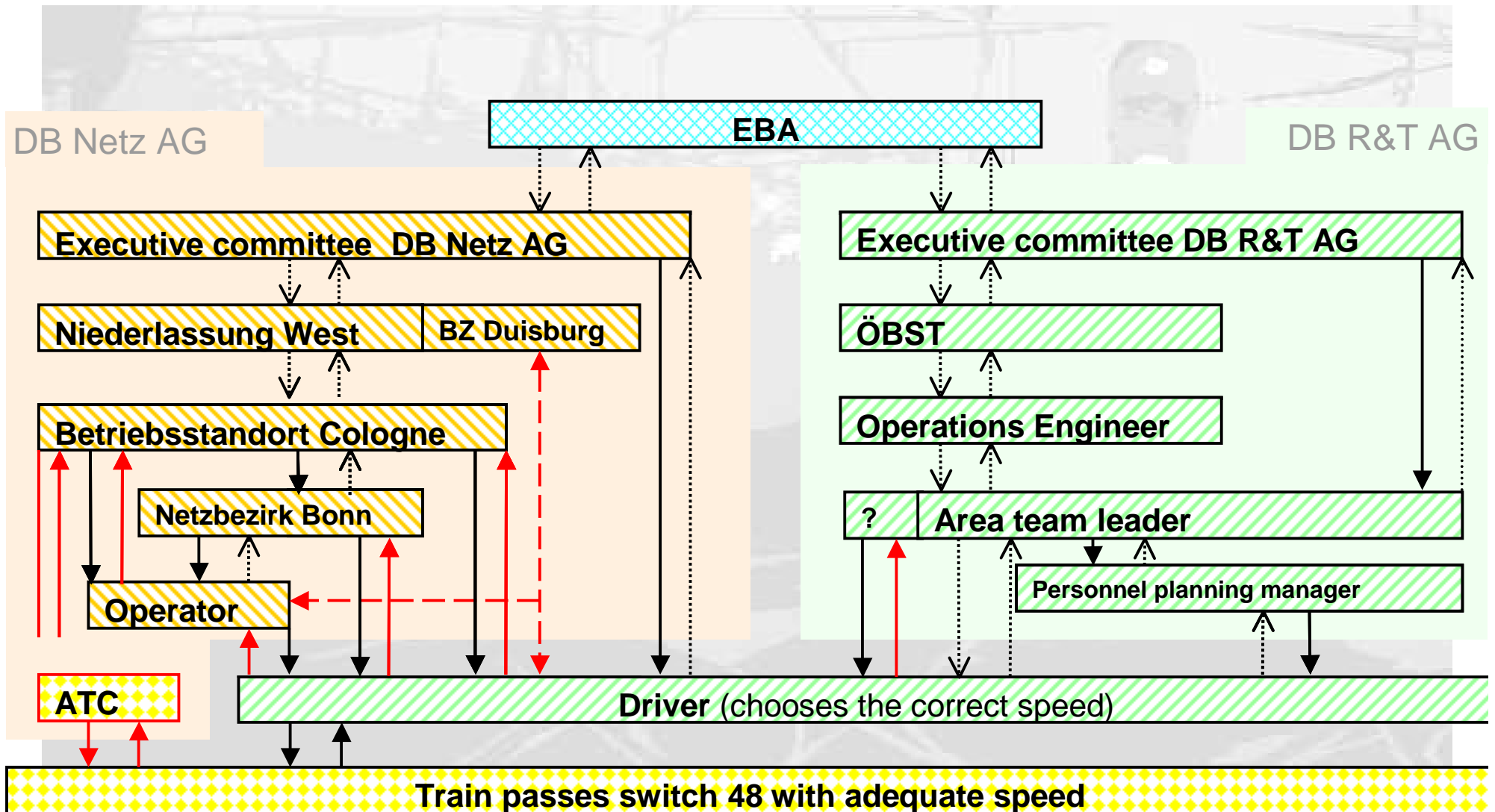
Control structure operation



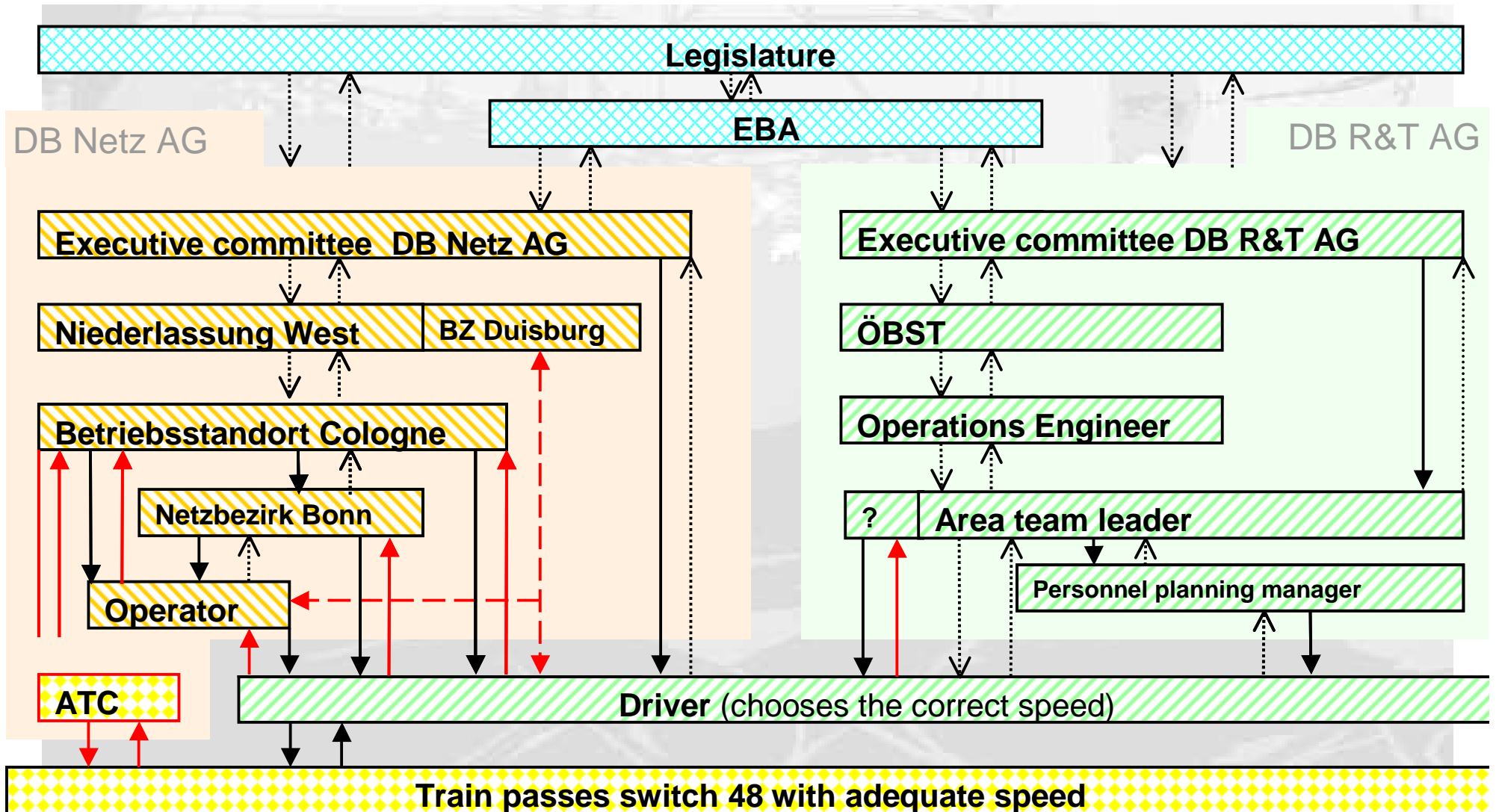
Control structure operation



Control structure operation

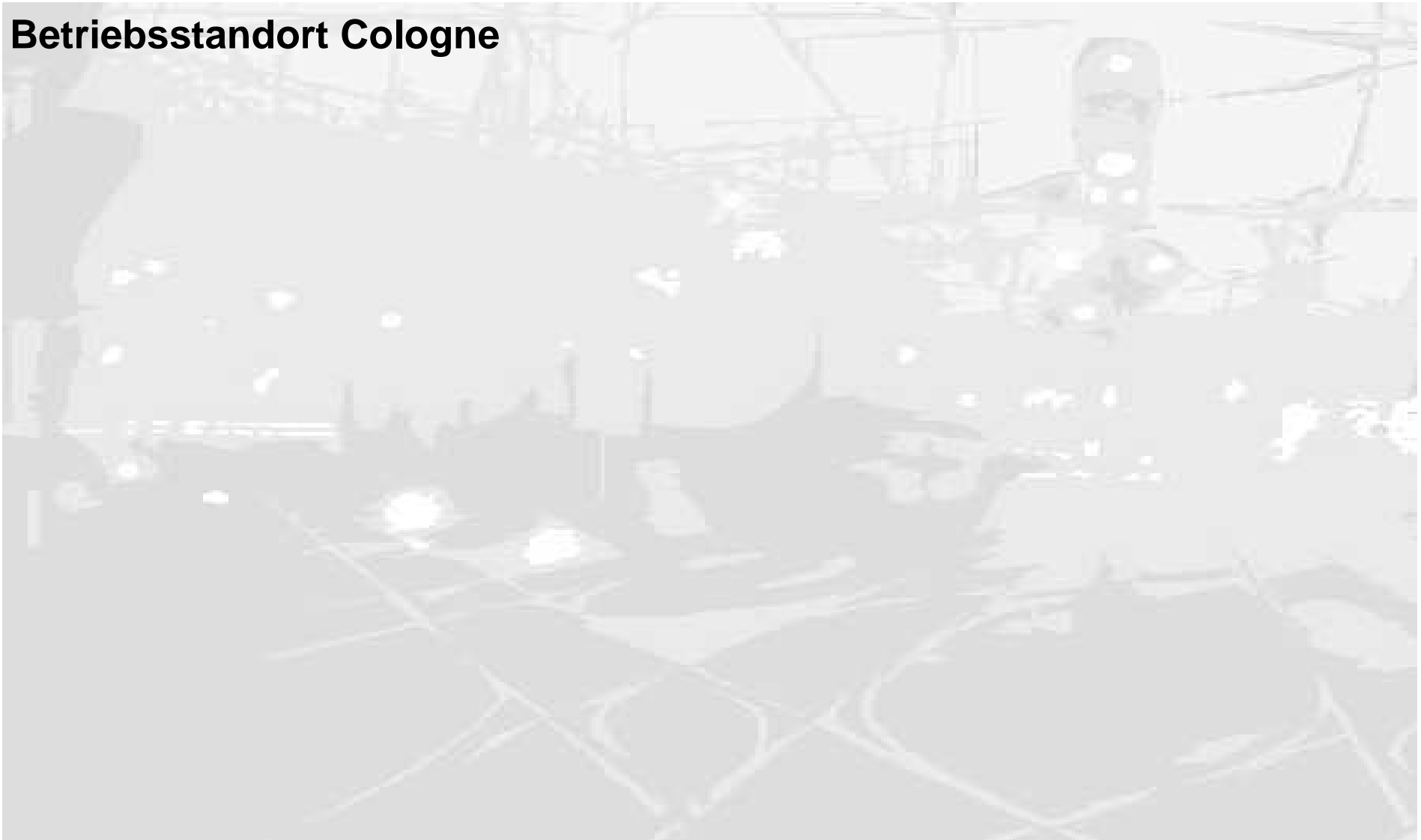


Control structure operation



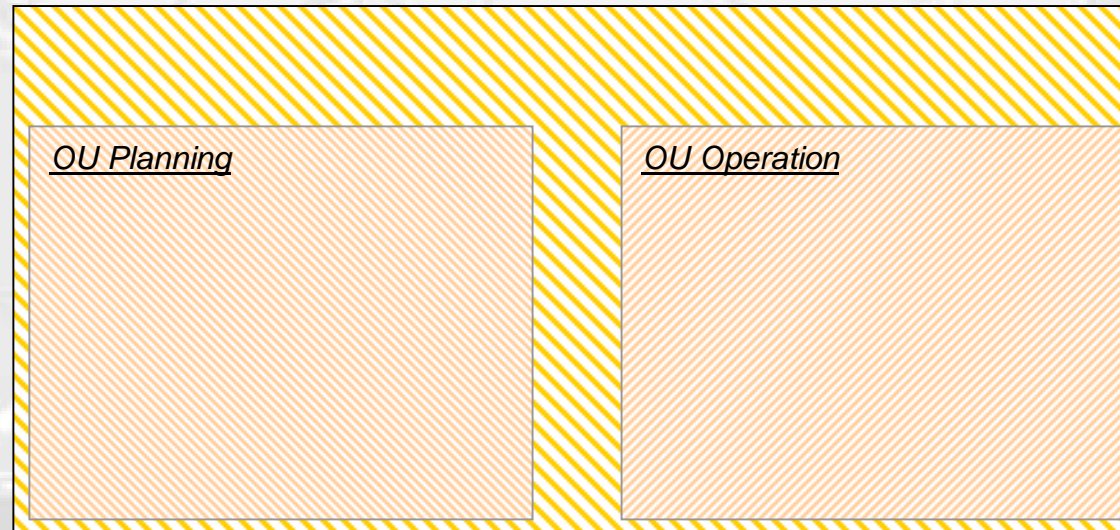
Zooming in on a detail

Betriebsstandort Cologne



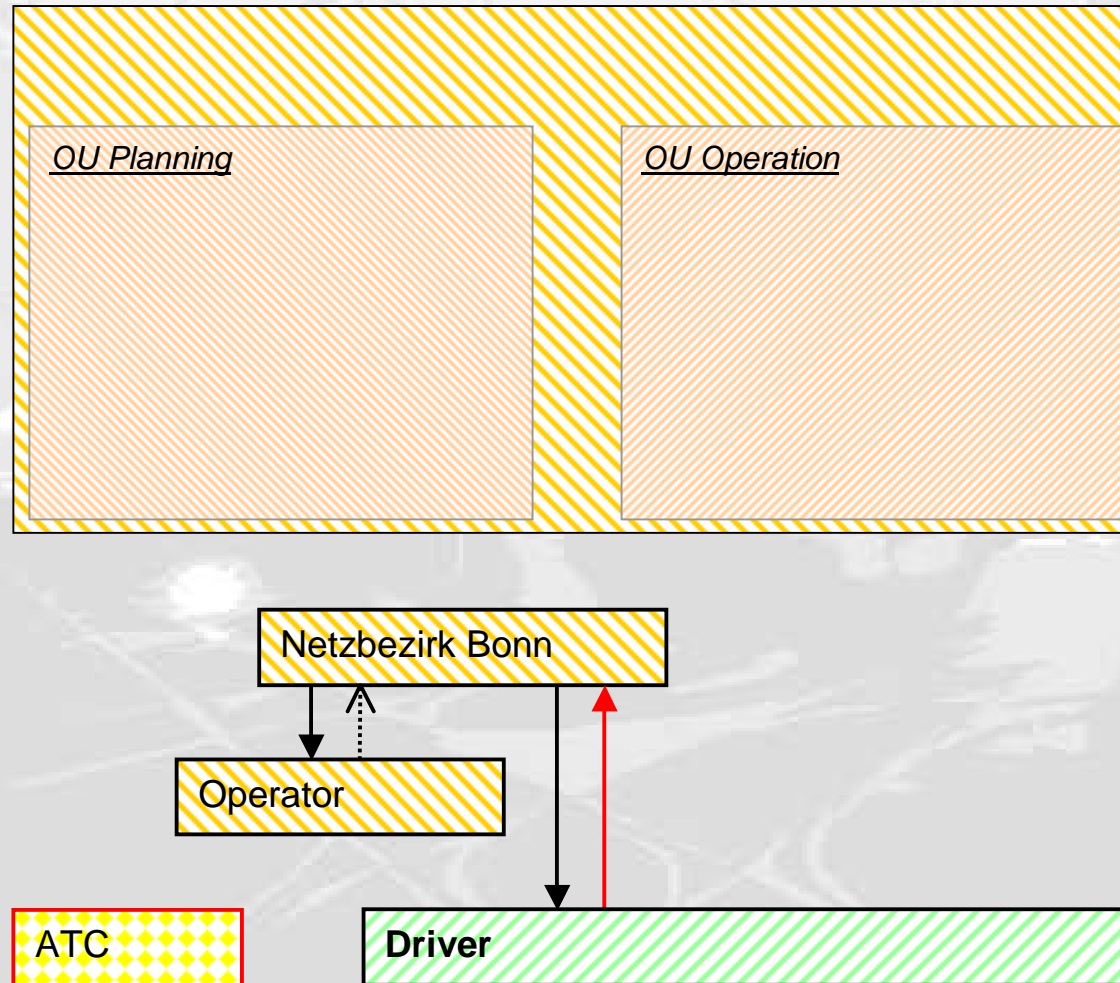
Zooming in on a detail

Betriebsstandort Cologne



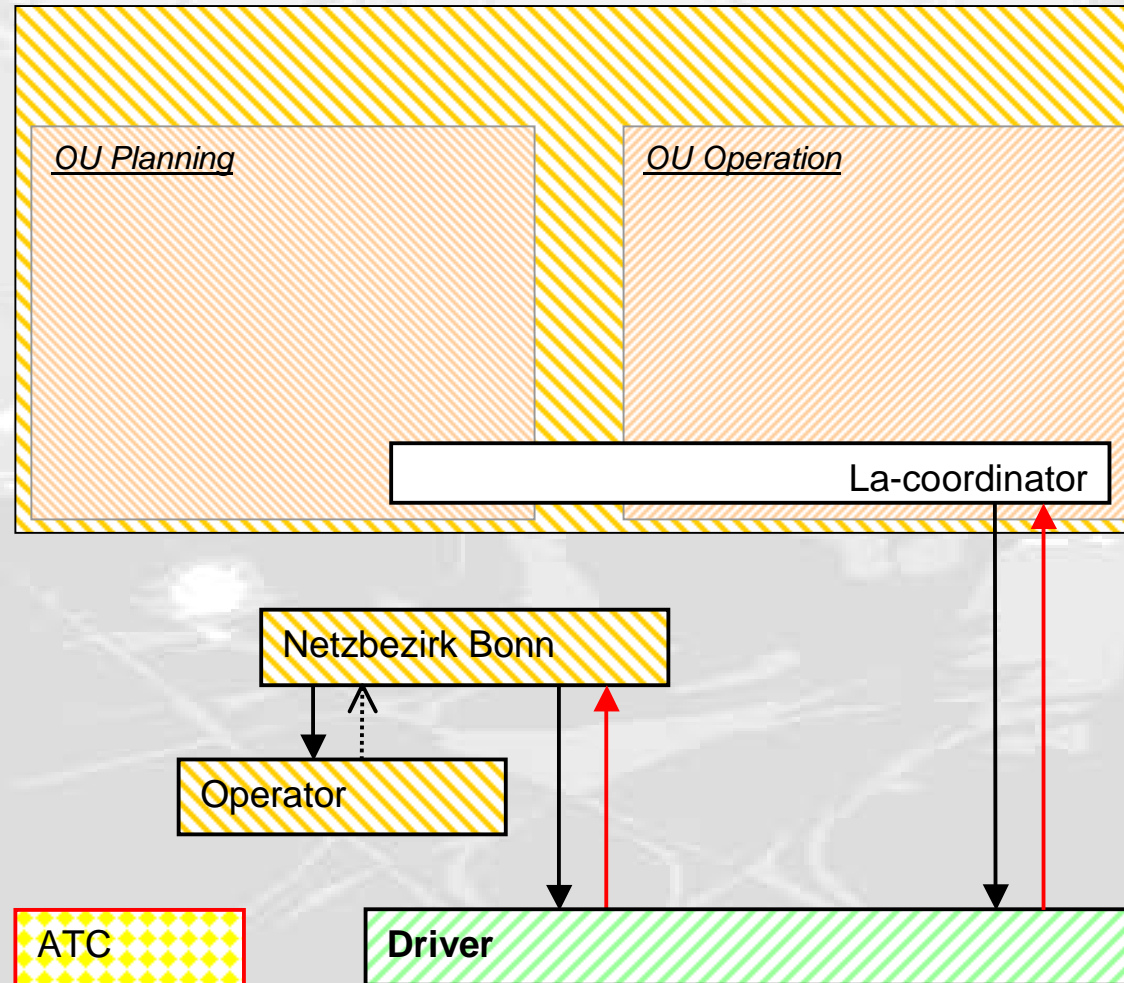
Zooming in on a detail

Betriebsstandort Cologne



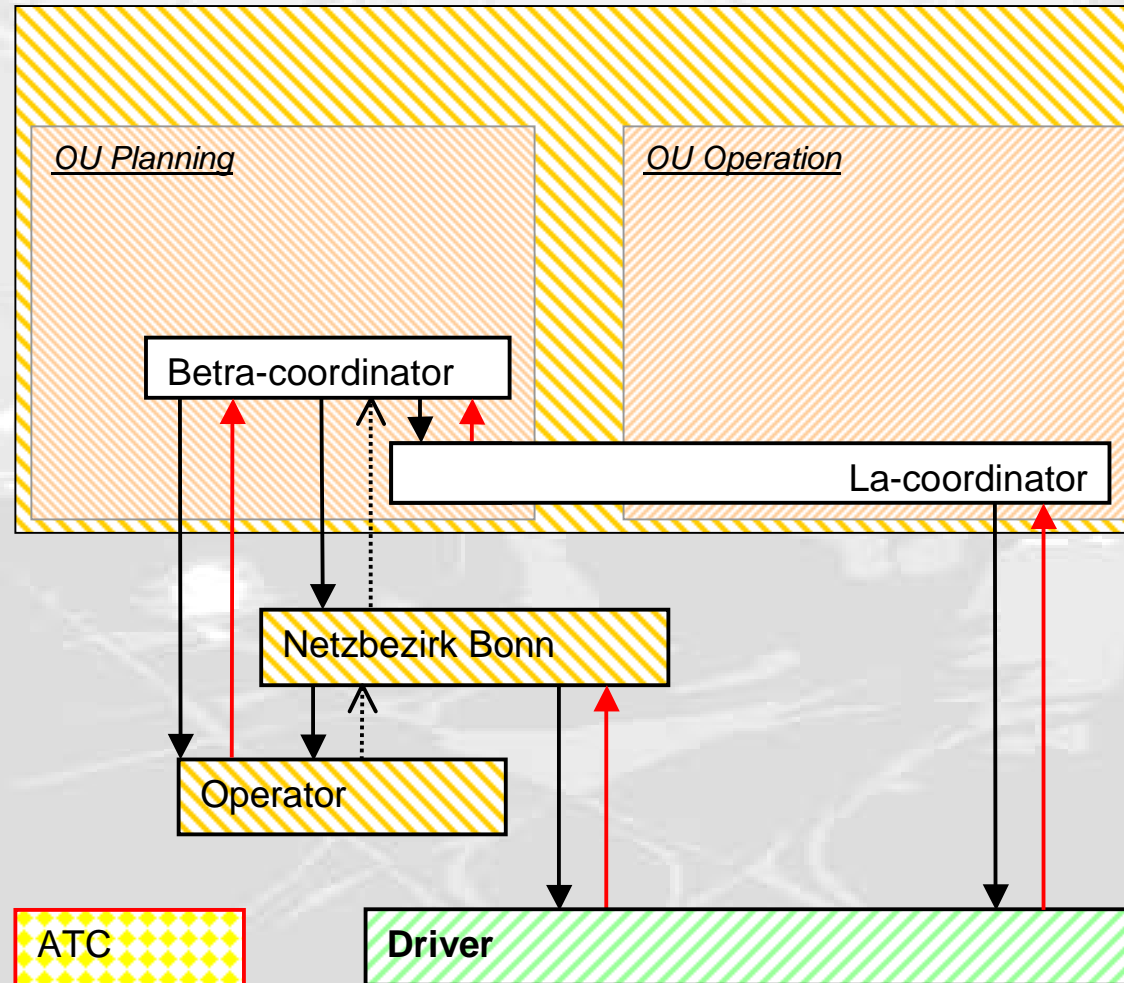
Zooming in on a detail

Betriebsstandort Cologne



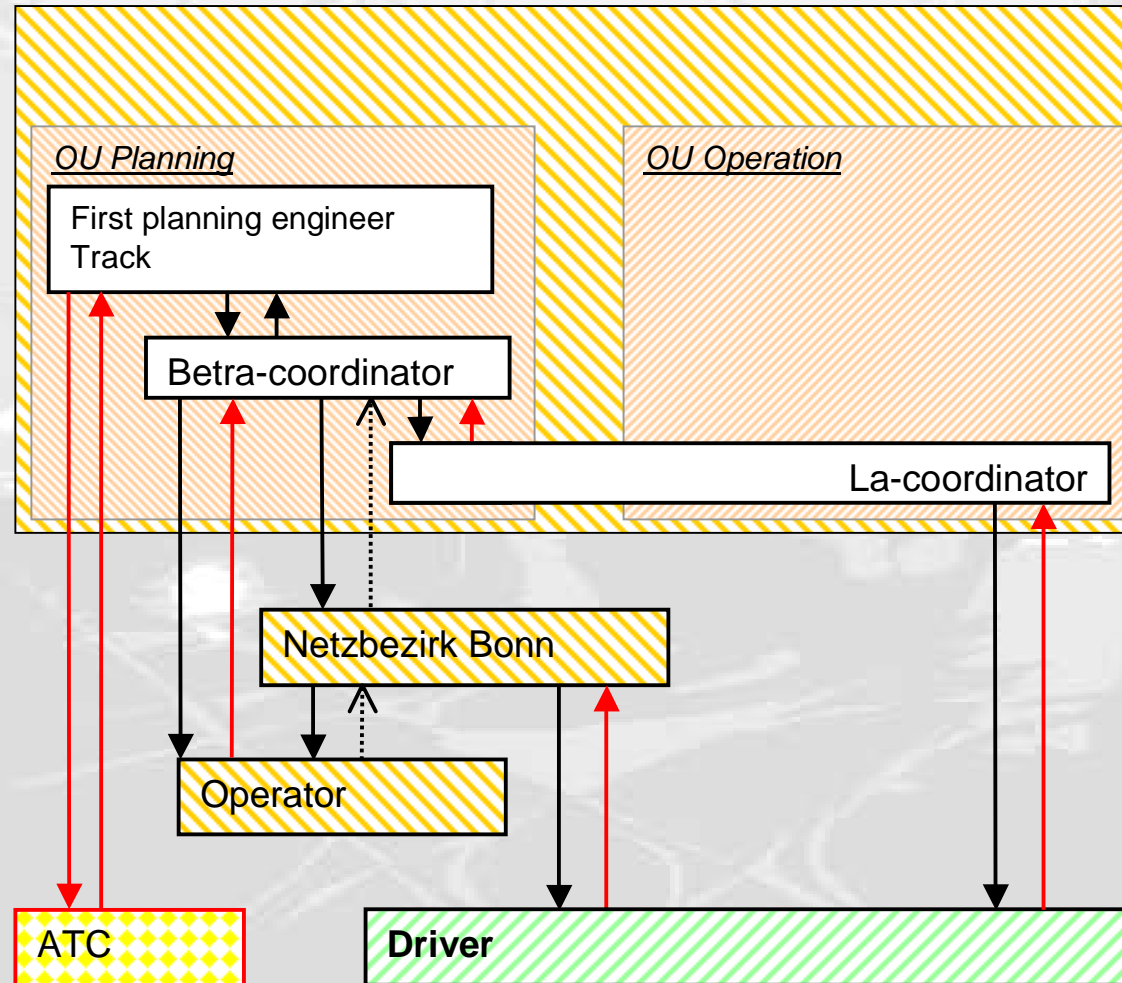
Zooming in on a detail

Betriebsstandort Cologne



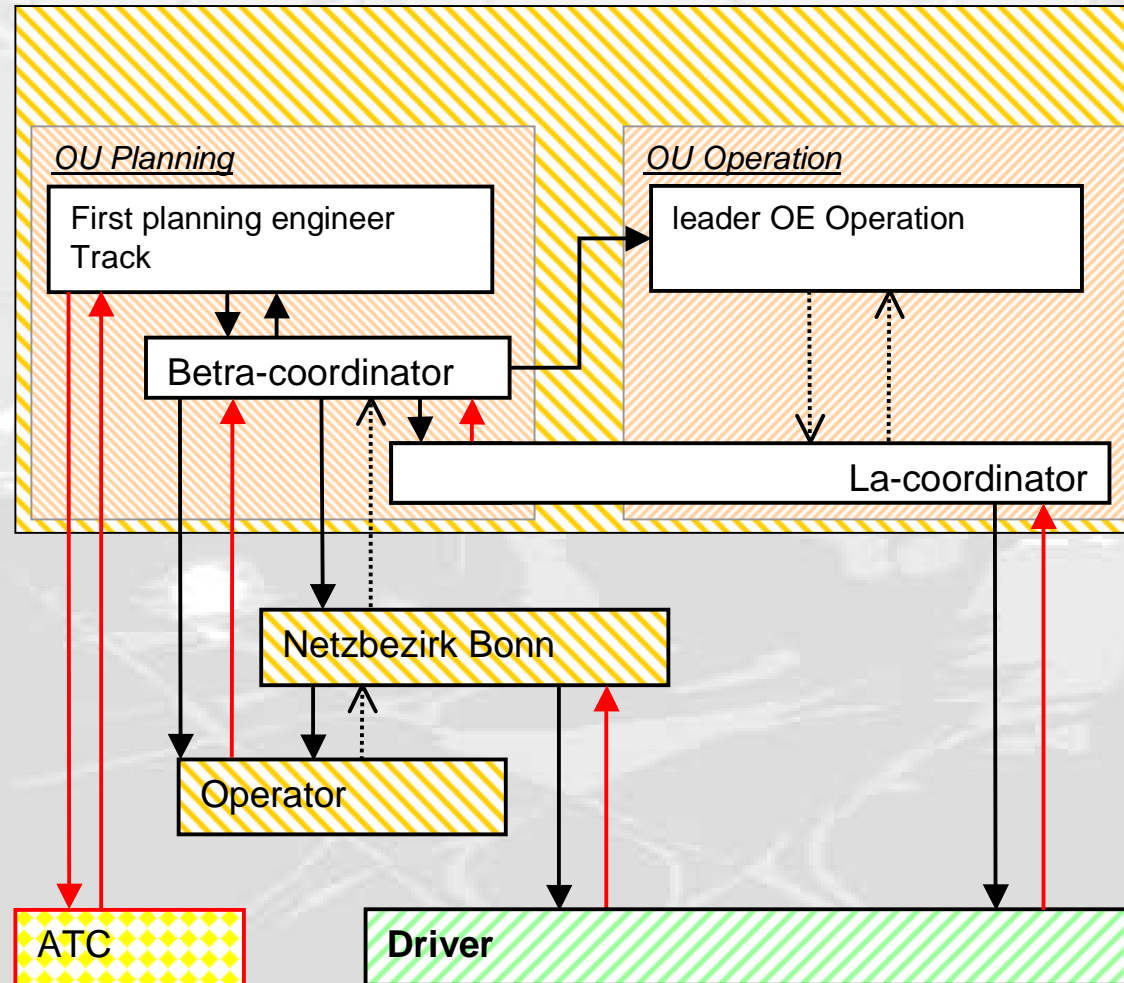
Zooming in on a detail

Betriebsstandort Cologne



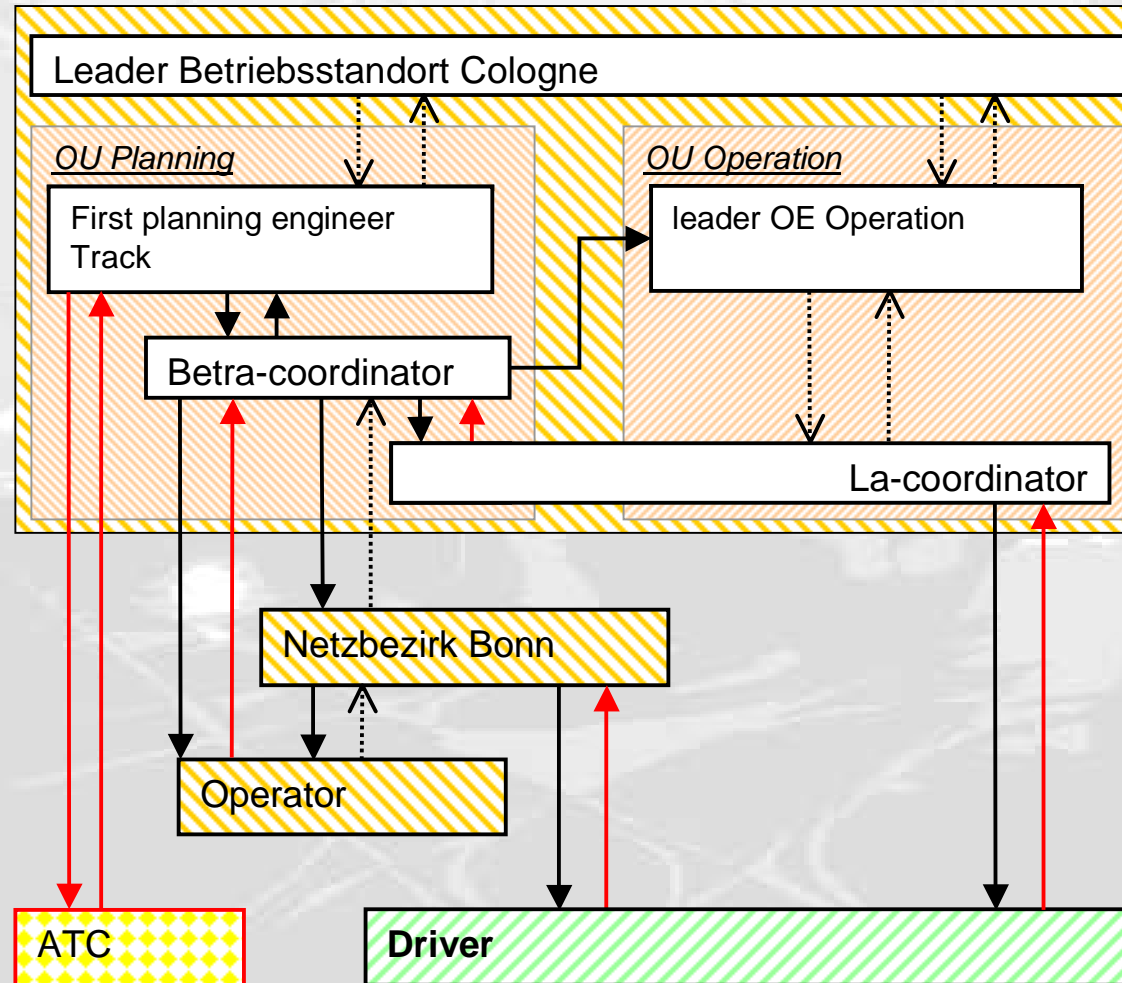
Zooming in on a detail

Betriebsstandort Cologne



Zooming in on a detail

Betriebsstandort Cologne



1. An introduction to STAMP
2. An analysis of Brühl using STAMP
3. Results and experiences



- post-hoc analysis will not bring really new results



- post-hoc analysis will not bring really new results
- STAMP was able to include all facts given by the existing reports into it's analysis-structure

- post-hoc analysis will not bring really new results
- STAMP was able to include all facts given by the existing reports into it's analysis-structure
- STAMP prompted to ask questions, that the existing reports could not answer

- post-hoc analysis will not bring really new results
- STAMP was able to include all facts given by the existing reports into it's analysis-structure
- STAMP prompted to ask questions, that the existing reports could not answer
- STAMP focused on organizational aspects

- post-hoc analysis will not bring really new results
- STAMP was able to include all facts given by the existing reports into it's analysis-structure
- STAMP prompted to ask questions, that the existing reports could not answer
- STAMP focused on organizational aspects
- STAMP questioned processes that are common practice in the German railway operation

- post-hoc analysis will not bring really new results
- STAMP was able to include all facts given by the existing reports into it's analysis-structure
- STAMP prompted to ask questions, that the existing reports could not answer
- STAMP focused on organizational aspects
- STAMP questioned processes that are common practice in the German railway operation
- In post hoc application STAMP delivered new questions not new answers

Experiences - difficulties



- No established procedure (two different examples by Prof. Leveson)

- No established procedure (two different examples by Prof. Leveson)
- Several possible ways to visualize the control structure

- No established procedure (two different examples by Prof. Leveson)
- Several possible ways to visualize the control structure
- It's not always clear, what to define as a separate process and what to include in an existing loop

- No established procedure (two different examples by Prof. Leveson)
- Several possible ways to visualize the control structure
- It's not always clear, what to define as a separate process and what to include in an existing loop
- No 1 on 1 assignment of control loop and control flaws (see also Prof. Johnson's paper)

- No established procedure (two different examples by Prof. Leveson)
- Several possible ways to visualize the control structure
- It's not always clear, what to define as a separate process and what to include in an existing loop
- No 1 on 1 assignment of control loop and control flaws (see also Prof. Johnson's paper)
- No obvious direct usage of classification (how do classified flaws help?)

Experiences - strengths



- The control structure helps to get a very complete and structured analysis
 - Forces to consider every single loop
 - Revealed blind spots in the existing report

- The control structure helps to get a very complete and structured analysis
 - Forces to consider every single loop
 - Revealed blind spots in the existing report
- STAMP delivers a flaw-list for every considered process

- The control structure helps to get a very complete and structured analysis
 - Forces to consider every single loop
 - Revealed blind spots in the existing report
- STAMP delivers a flaw-list for every considered process
- By applying the classification scheme STAMP finds inadequate actions as well as actions that have not been taken

- The control structure helps to get a very complete and structured analysis
 - Forces to consider every single loop
 - Revealed blind spots in the existing report
- STAMP delivers a flaw-list for every considered process
- By applying the classification scheme STAMP finds inadequate actions as well as actions that have not been taken
- Applying the concept of the control loop to every part of the control structure questions fundamental processes



Thank you for your attention