Technische Universität Braunschweig

Institut für Verkehrssicherheit und Automatisierungstechnik iVA
Prof. Dr.-Ing. Dr. h.c. mult. E. Schnieder

Integration of Petri Nets into CAST by the Example of 7.23 Accident

Dipl.-Wirtsch.-Ing. René S. Hosse, Dirk Spiegel M.Sc. M.Sc., Prof. Dr.-Ing. Dr. h.c. mult. Eckehard Schnieder

27. March 2013

Contents

1. Motivation
What do we do?

Institute für Traffic Safety and Automation Engineering

- Ground transportation safety
  - Automotive
    - *Driver assistant systems / automous driving*
    - *E.g. time series analyses*
  - Railway
    - *ERTMS/ETCS development*
    - *Satellite based localisation services*
    - *Safety cases (or: hazard cases)*
- System Safety Engineering, primarily model-based engineering
- Automation Engineering (e.g. SmallCAN)
- Terminology and Requirements Engineering

1. Motivation

Why we do need STAMP + ?

Advantages of STAMP for Railway applications:

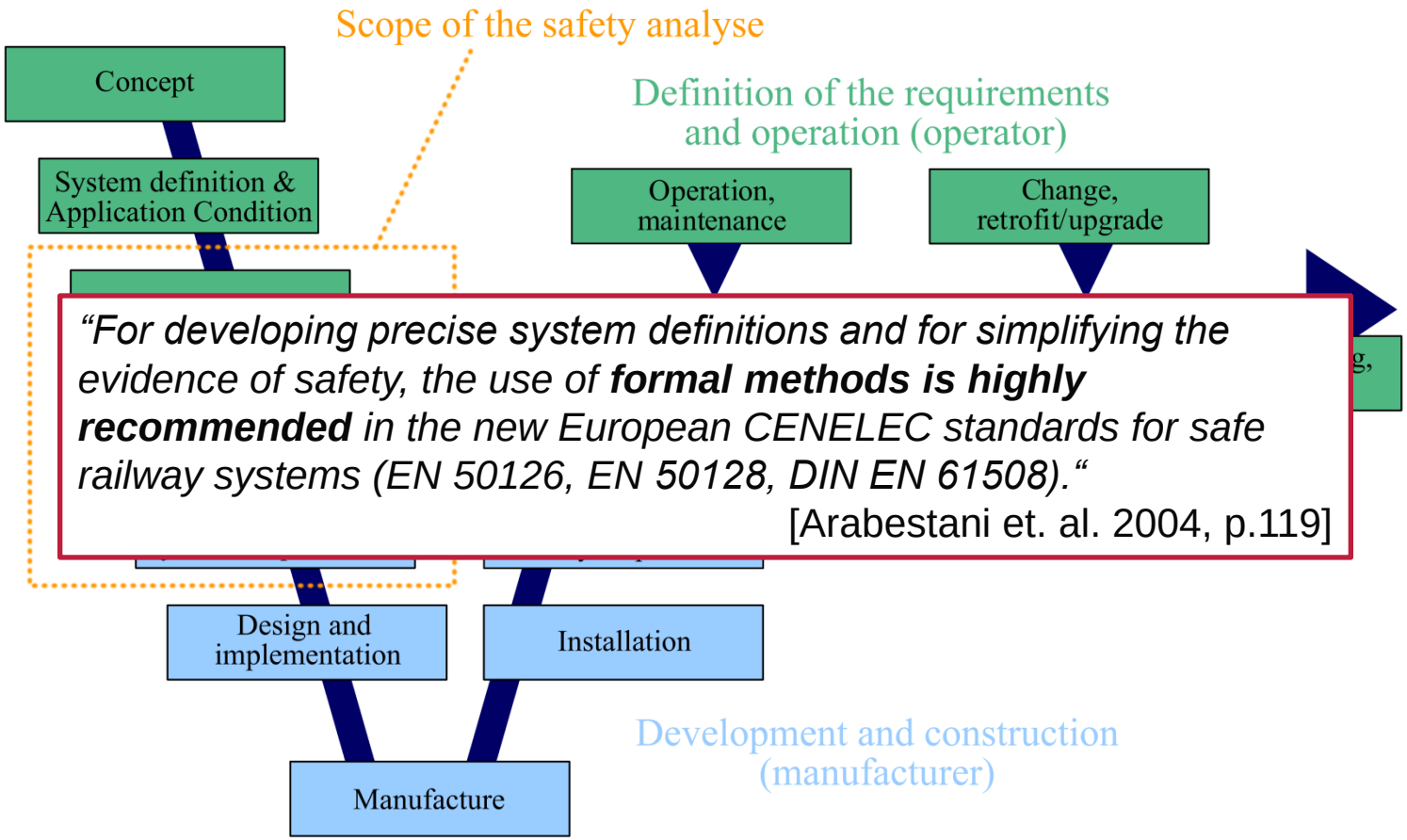
- Understandable for non-engineers (interdisciplinary application) and relatively easy to use
- High amount of detection of control lacks
- Involving complex human decision making, software error, systemic accidents and organizational risk
- Performing STAMP analysis improves significantly system understanding

Why we need *STAMP + ?*

- **But:**
  - Little normative background
  - Partly conflicting with RAMS standards (reliability, availability, maintainability, safety)
  - Little distribution throughout ground transportation industry in Europe, only few application known
  - No accepted formal methods included, except System Dynamics

1. Motivation

System Development in Europe Railway Standards: V-Model

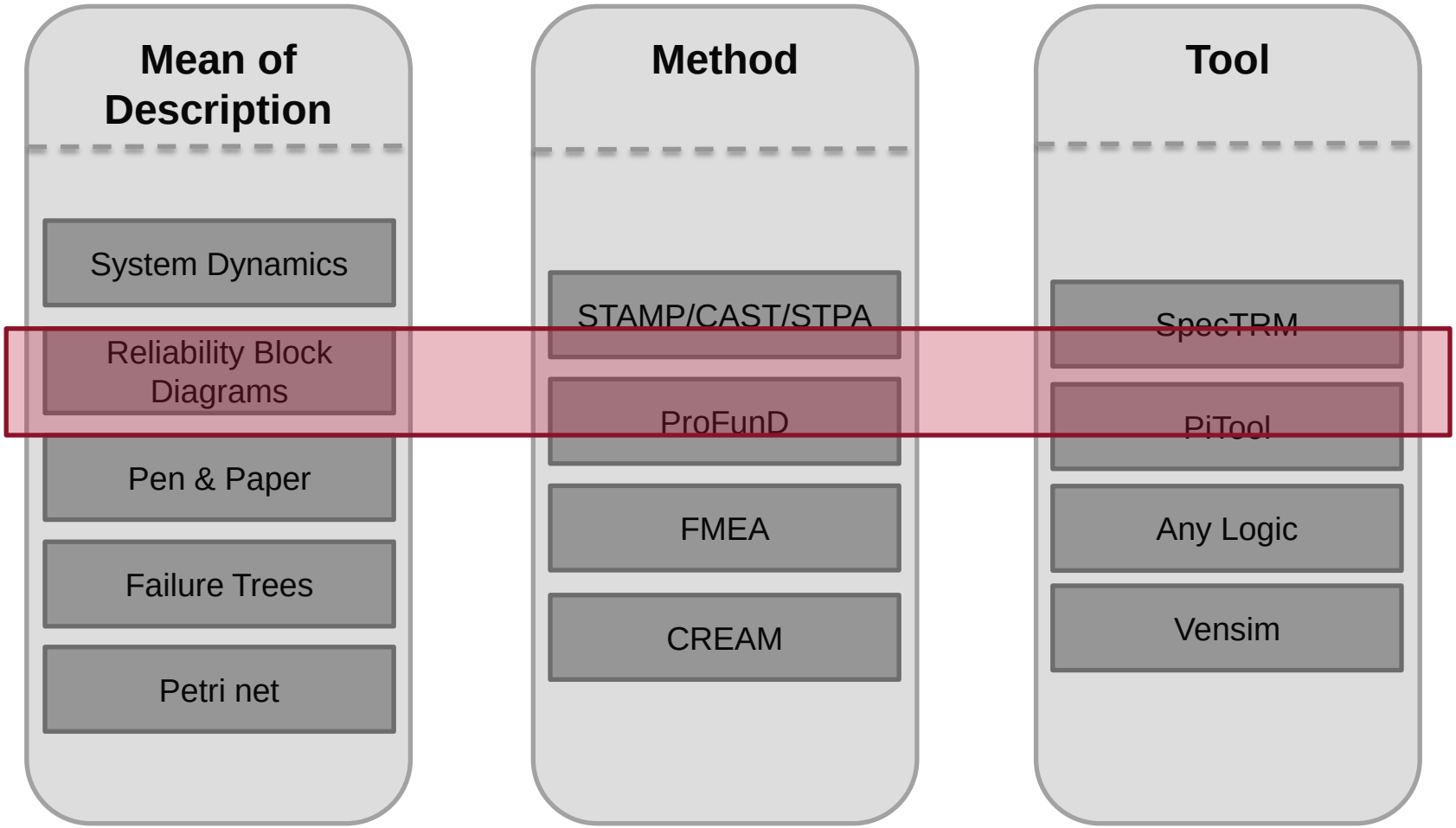


*"For developing precise system definitions and for simplifying the evidence of safety, the use of **formal methods is highly recommended** in the new European CENELEC standards for safe railway systems (EN 50126, EN 50128, DIN EN 61508)."*

[Arabestani et. al. 2004, p.119]

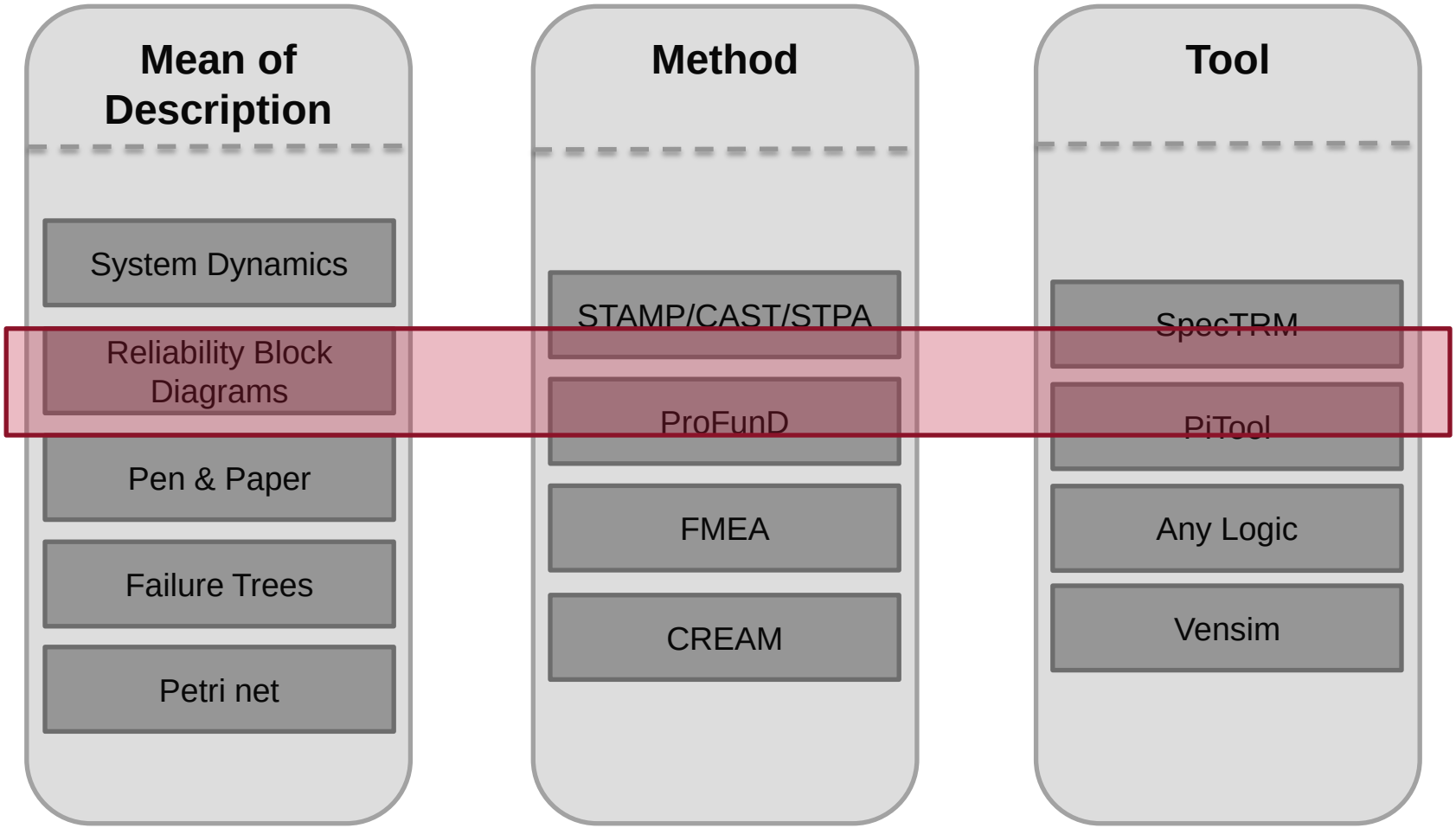
1. Motivation

Orthogonality: Thinking in Means of Description, Methods and Tools (1/3)



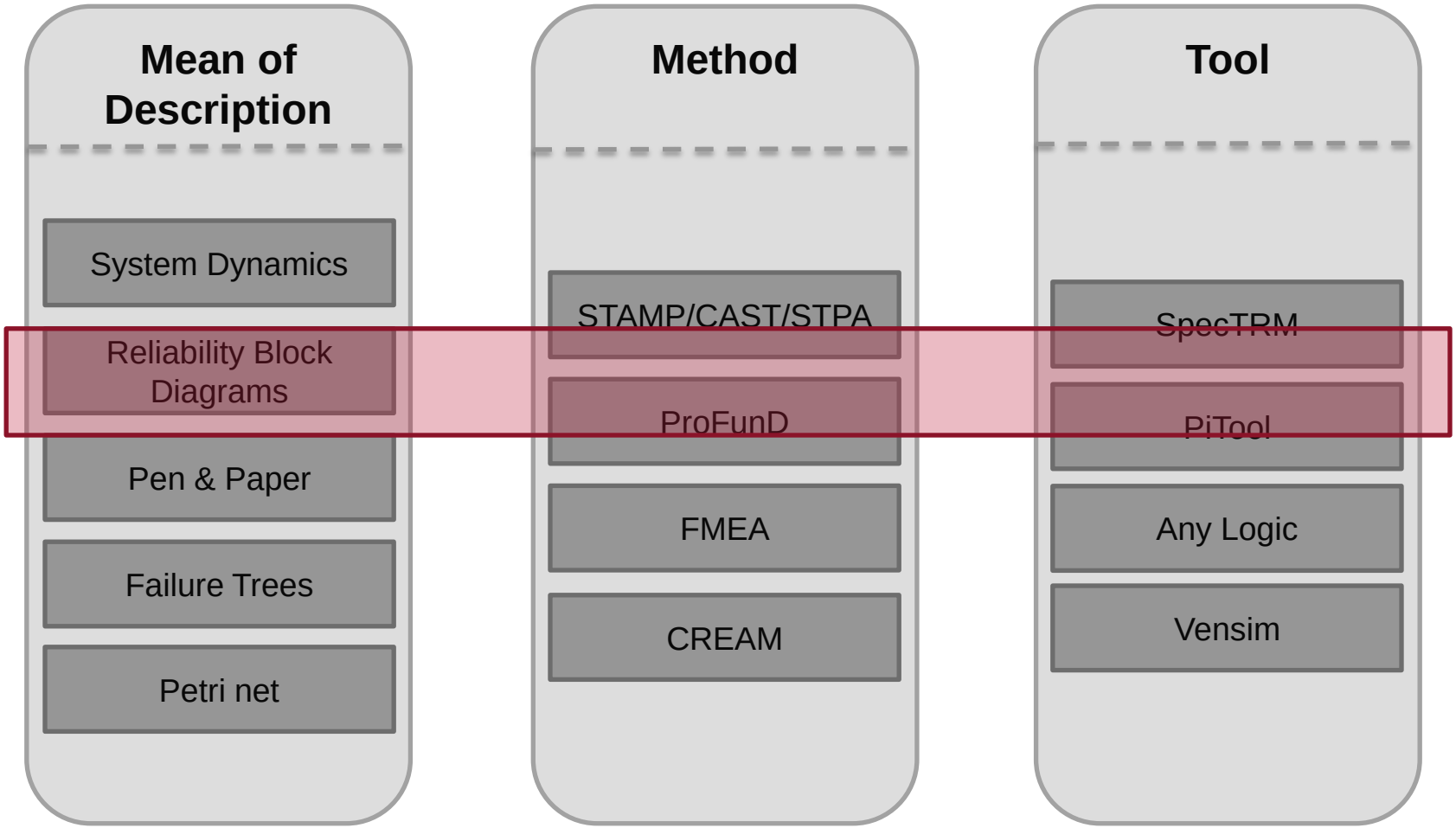
1. Motivation

Orthogonality: Thinking in Means of Description, Methods and Tools (2/3)



1. Motivation

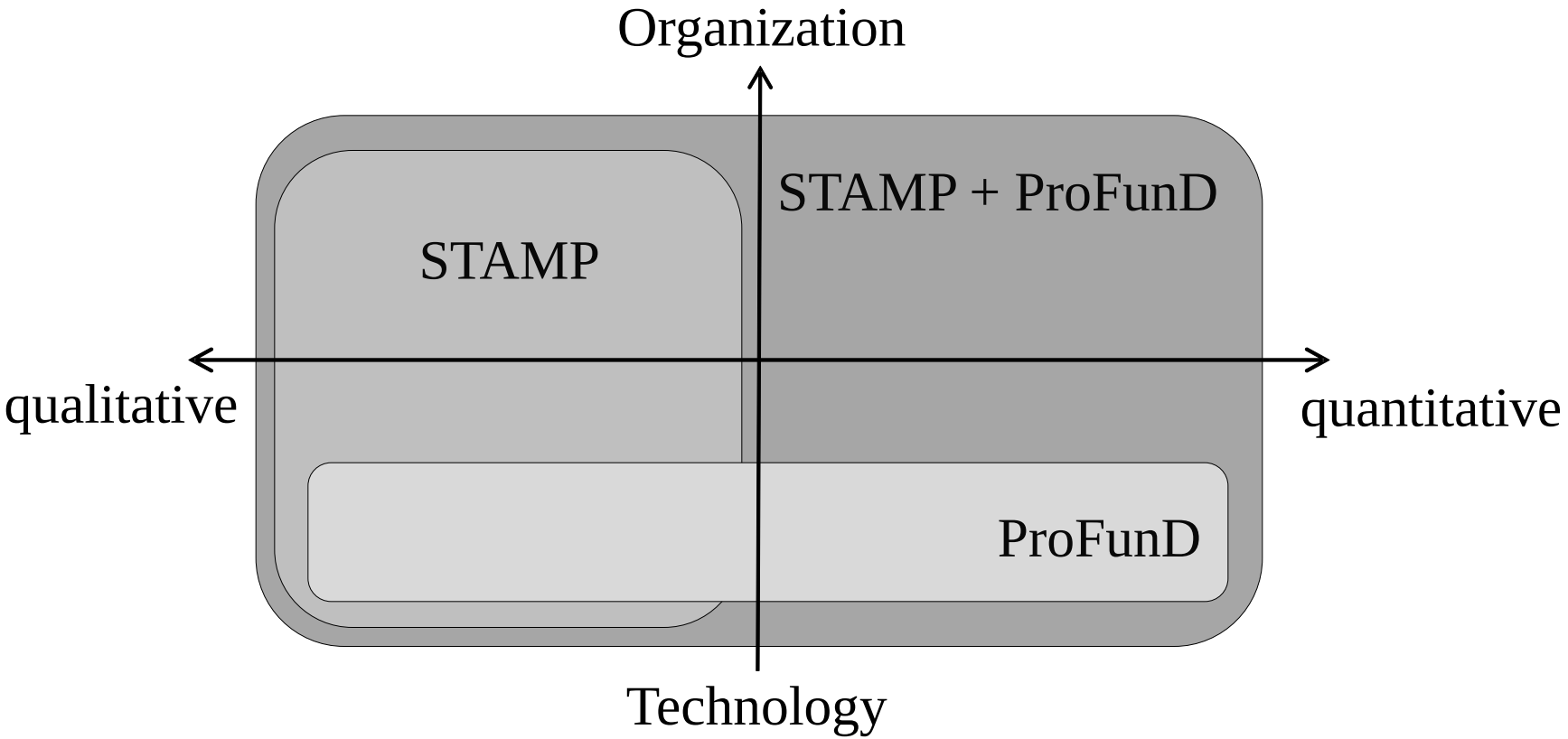
Orthogonality: Thinking in Means of Description, Methods and Tools (3/3)



Contents

2. Goal of Hybrid Approach

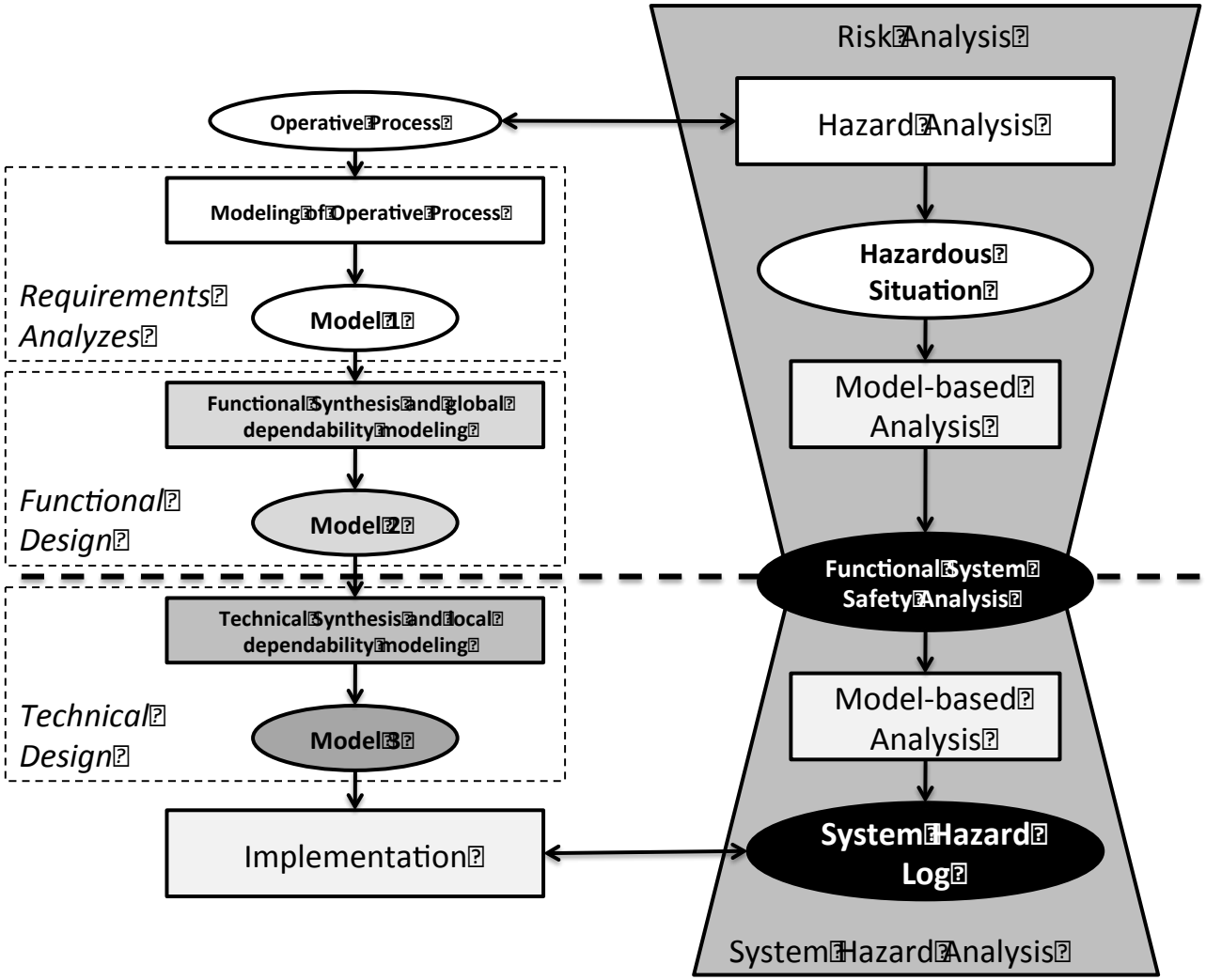
Hybridization of qualitative approach and quantitative approach



Contents

3. Methodology

(2) ProFunD – Fundamental Concepts



Component Dependability

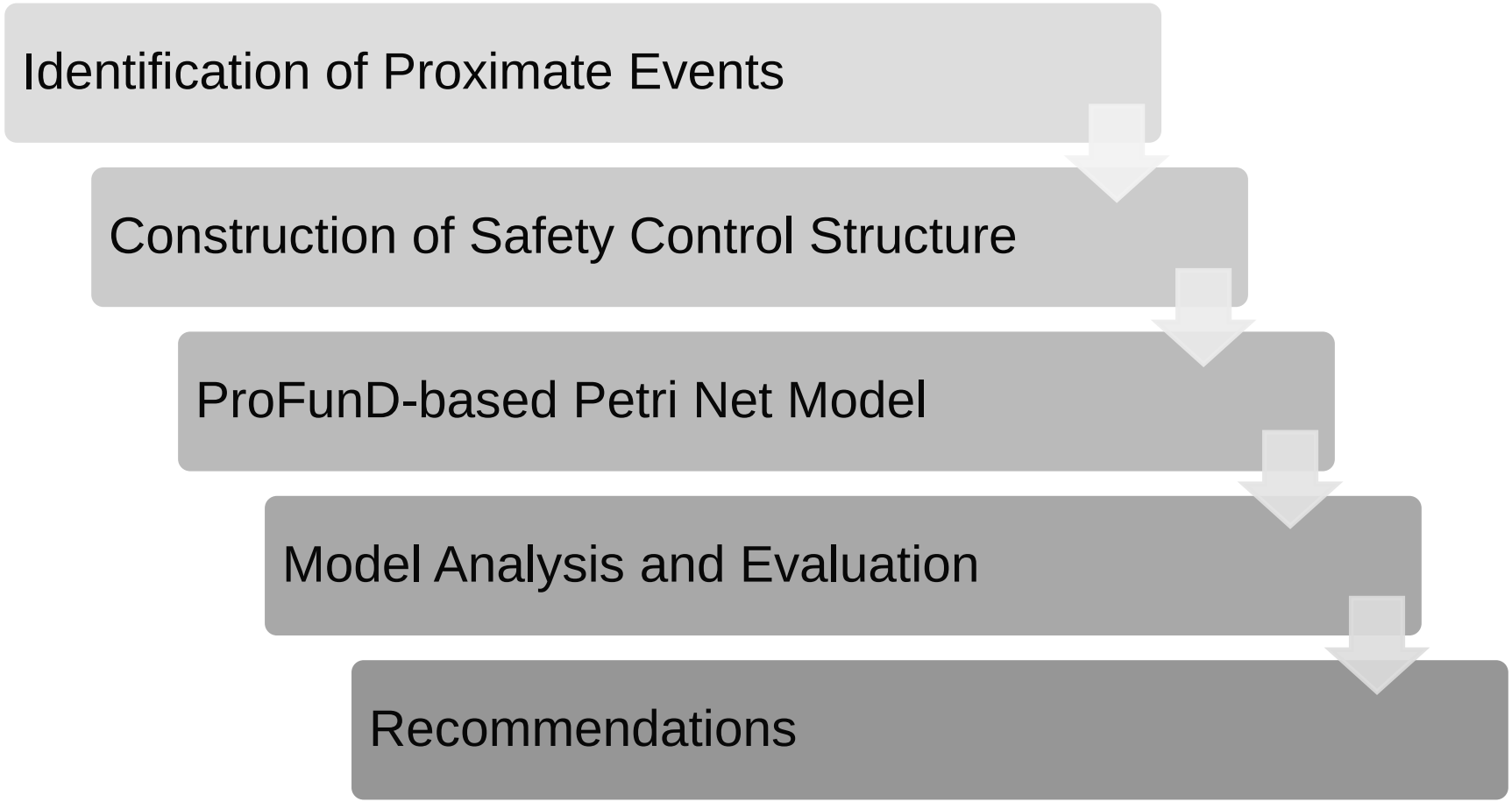
Functional Layer (Human, Soft- and Hardware)

Physical Processes

[Slovák 2006]

3. Methodology

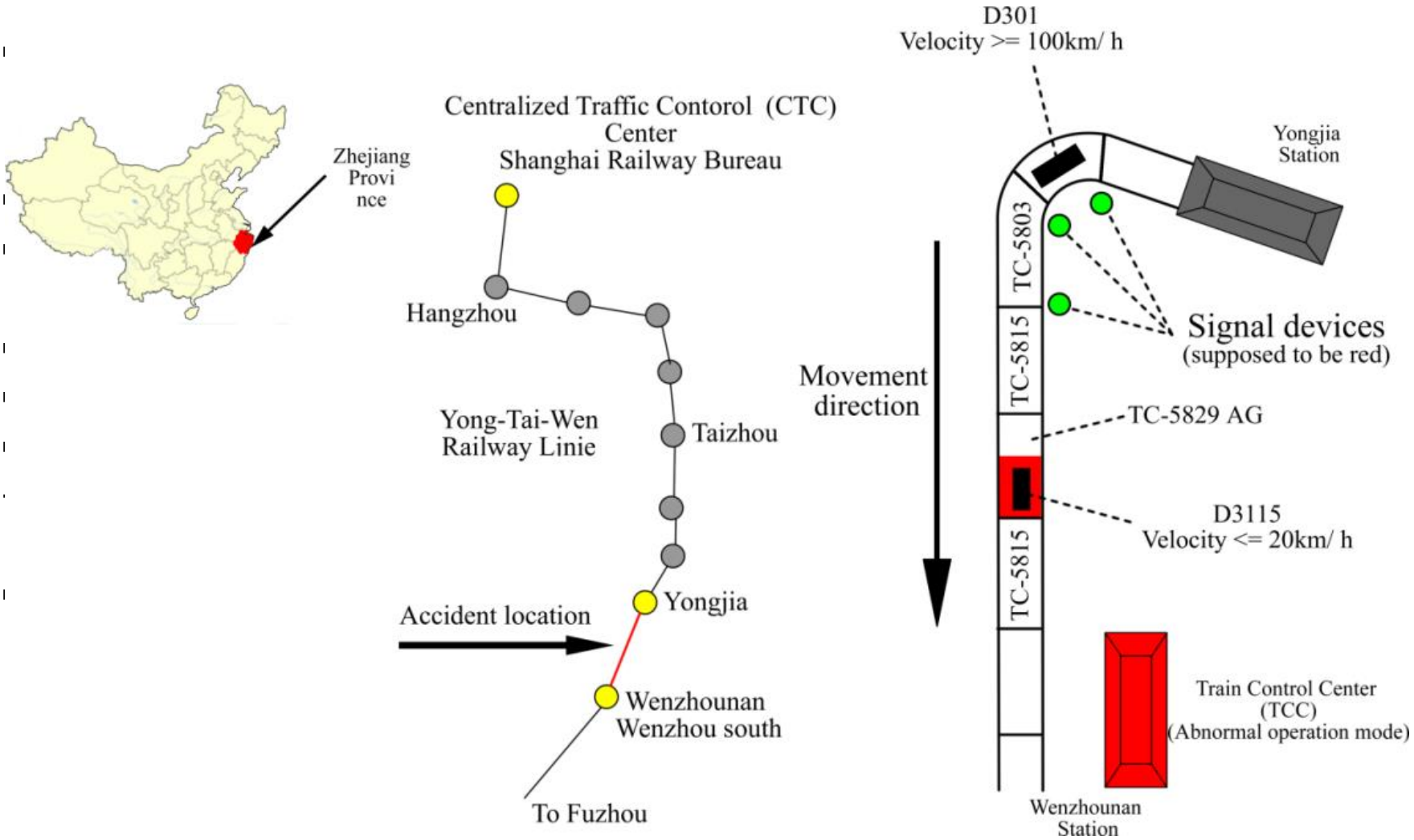
(3) Hybrid Approach – Analysis Process on the example of CAST



Contents

4. Sample Application

Accident introduction of the Wenzhou accident

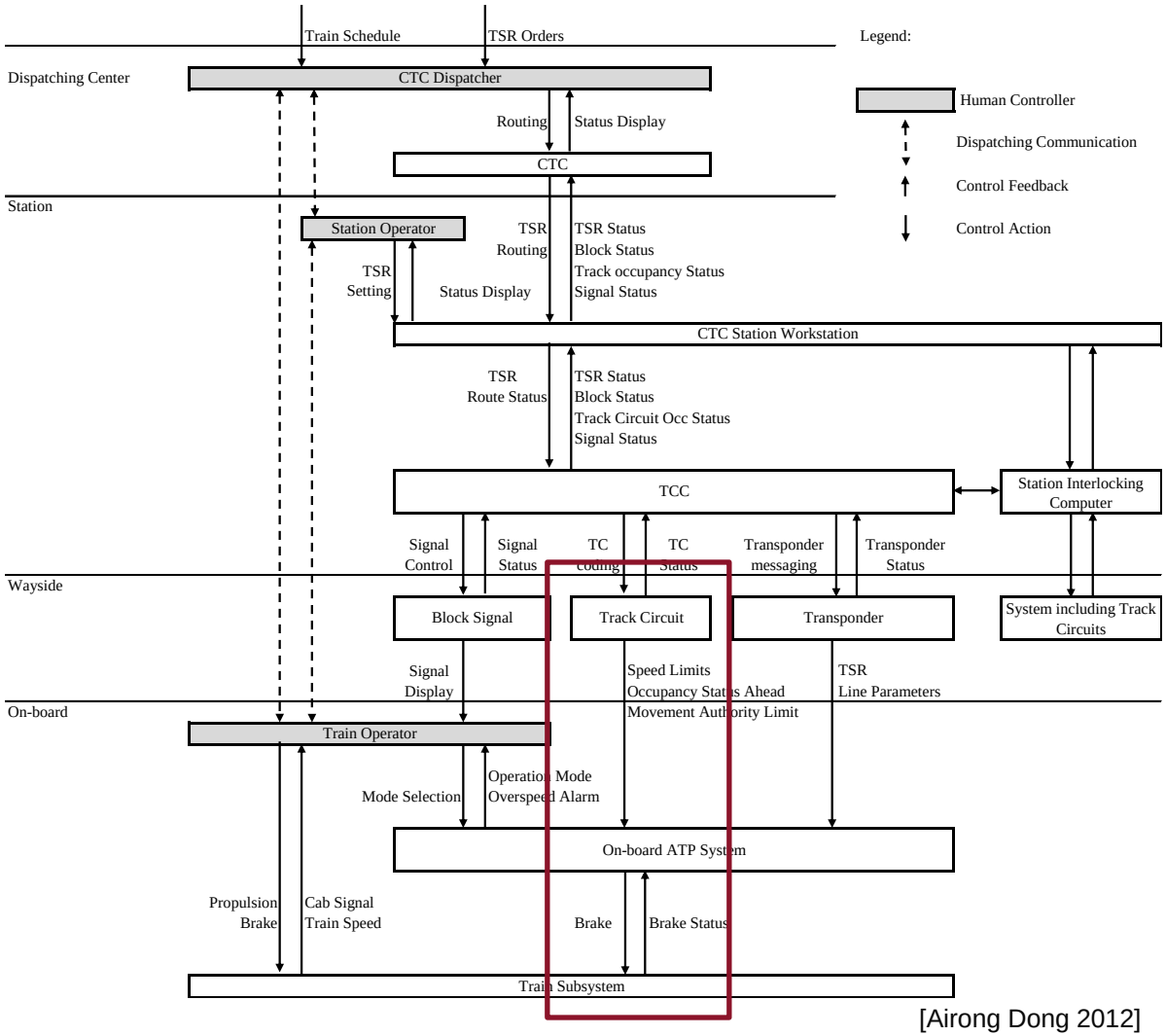


[Dajiang Suo 2012]

4. Sample Application

Control Structure as basis for the Petri net modelling

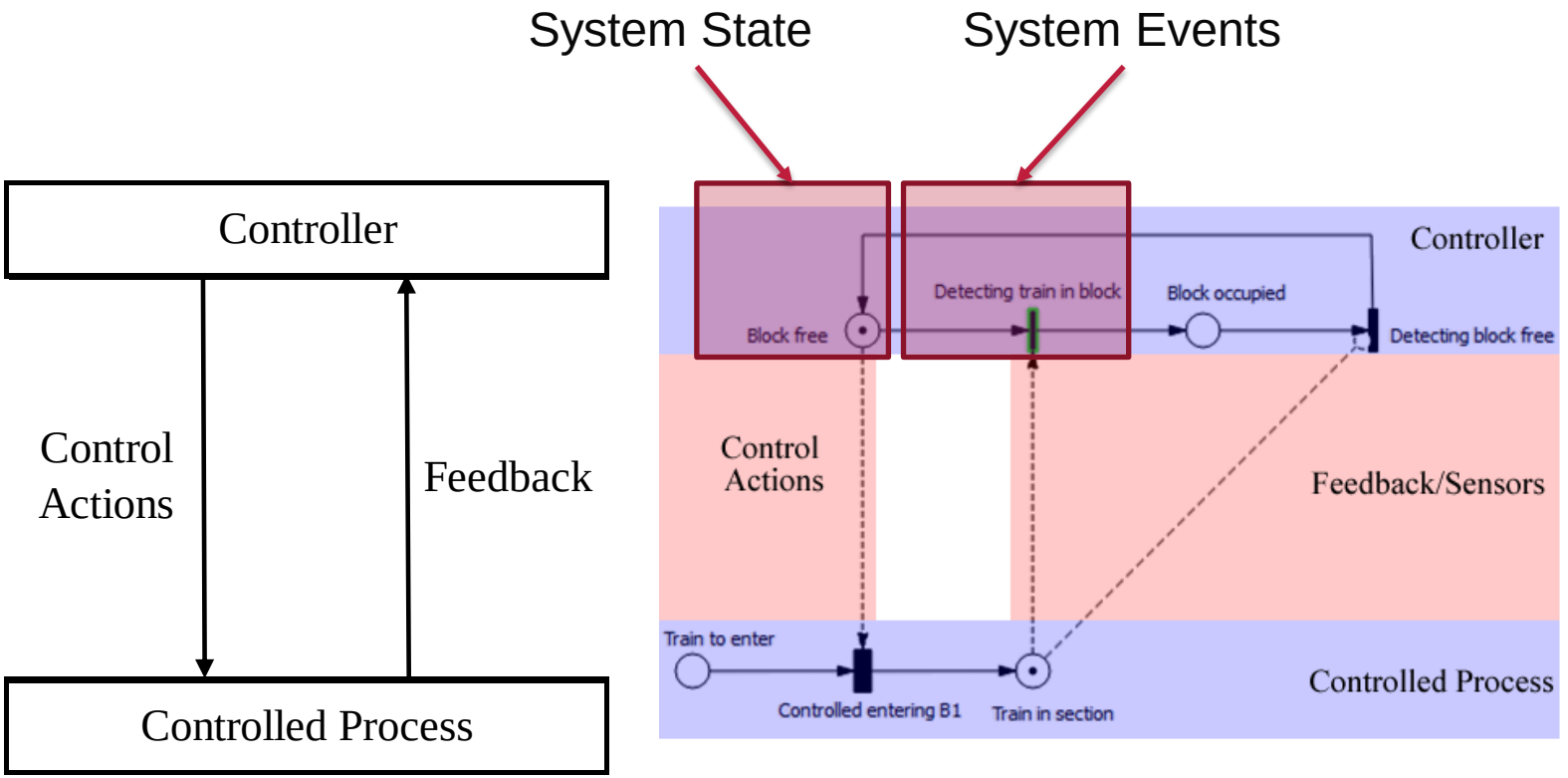
- Application is based on the control structure by Airong Dong
- Multiple simplifications have been made (Signal flows)
- Pi-Tool has been used (Provided by iQST GmbH)



[Airong Dong 2012]

4. Sample Application

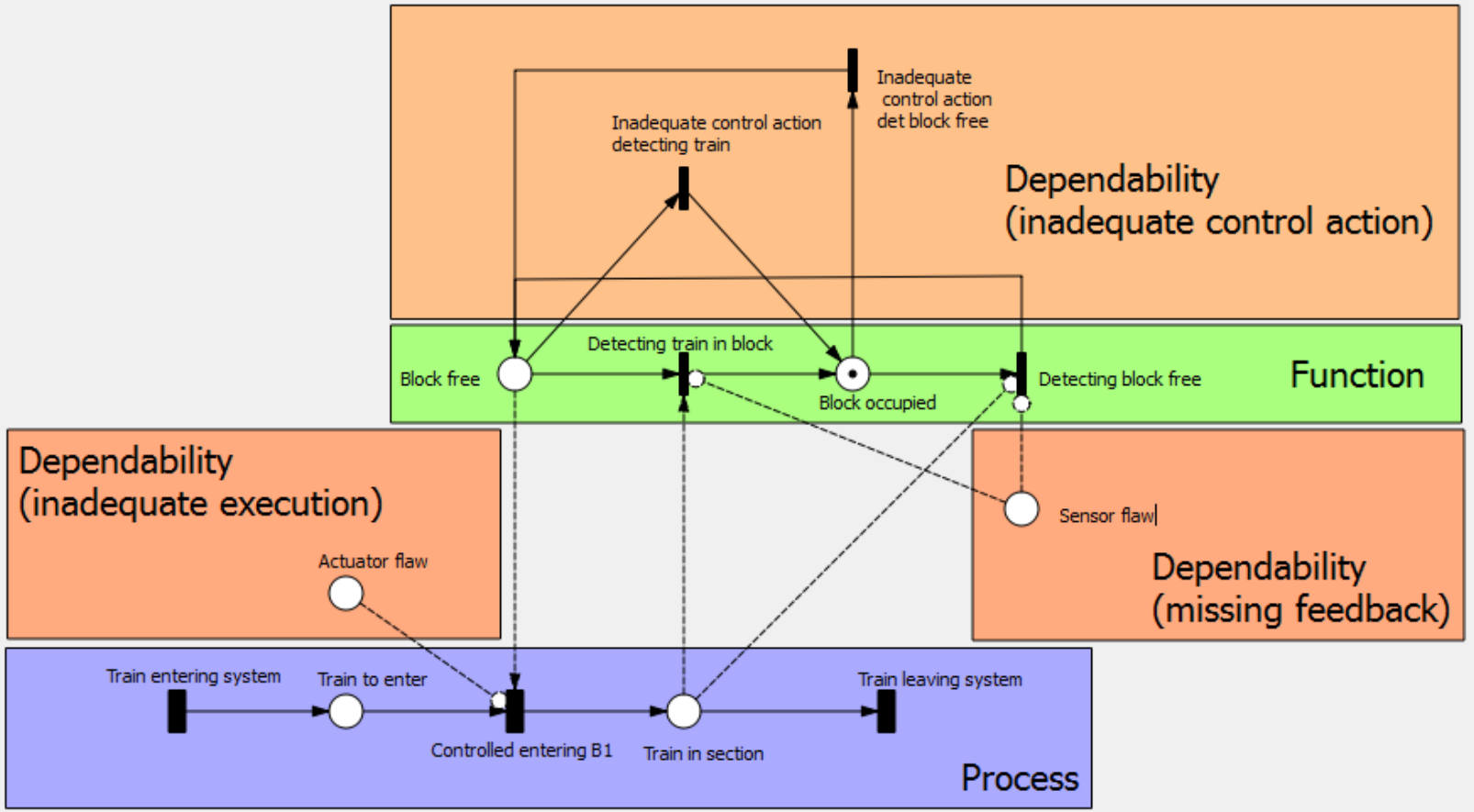
Transforming standard control loop



[Leveson 2011]

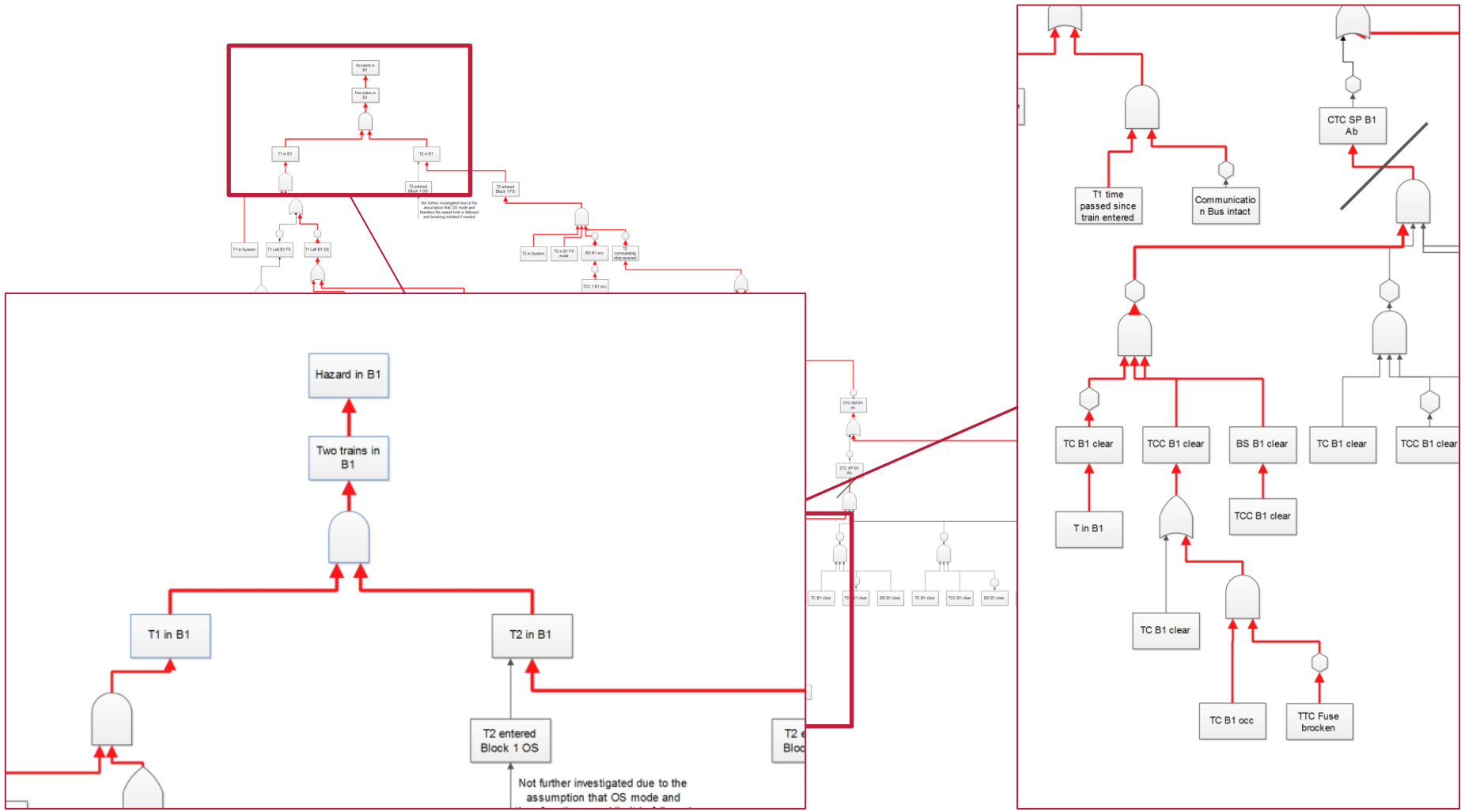
4. Sample Application

System-theory element transformation - simple control loop with control flaws



4. Sample Application

State tree (simplified reachability graph)



Contents

5. Results and Discussions

Comparison with CAST analysis

- Same amount of critical system states as in Airong Dong are detected
- General design rules as the fail-safe principle are detected in either analysis (except the station operator who was neglected during the formal model)
- Grade of detail is much higher within the new method due to the PN which force the analysis for a high precision modelling

CAST Analysis by keywords	New Method
Did not track leading train	Wrong assumptions in mental model (“T1 time passed since train entered” & “communication bus intact”)
Did not track TC 5829 AG failure status	Forgetting of “abnormal condition”
Unable to report train cannot start in OS mode	“T1 FP OS failed to restart” & “Communication bus b1 defect”

[Airong Dong 2012]

Contents

6. Conclusions

The new method:

- enables to detect as many failures as CAST-Analysis
- shows the system states on which basis decisions were made including contextural factors
- enables analysis technique with larger analysis capabilities (qualitative / quantitative)
- Systems are easily too complex to be analyzed with a reachability graph
- has shown STAMP / CAST can be applied orthogonally
- does not help to determine when a system is safe
- **Future Work: Provide Open Source Tools for STAMP / CAST**

Literature

[Airong Dong 2012] Airong Dong: **Application of CAST and STPA to Railroad Safety in China**. Master Thesis, Boston, 2012.

[Dajiang Suo 2012] Dajiang Suo: **System Theoretic Analysis of the "7.23" Yong-Tai-Wen Railway Accident**. Master Thesis, Beijing, 2012.

[DIN EN 50126] Deutsches Institut für Normung:: **Railway application: The specification and demonstration of Reliability, Availability, Maintainability and Safety(RAMS)**.

[Kaiser et al. 2007] Kaiser, B.; Gramlich, C.; Förster, M.: **State/event fault trees—A safety analysis model for software-controlled systems**, in: Reliability Engineering & System Safety, Vol. 92 (2007) No. 11, pp. 1521–1537.

[Leveson 2011] Leveson, N.: **Engineering a safer world**. **Systems thinking applied to safety**, MIT Press, Cambridge Mass, 2011.

[Meyer zu Hörste 2004] Meyer zu Hörste, M.: **Methodische Analyse und generische Modellierung von Eisenbahnleit- und -sicherungssystemen**. Dissertation. 571, VDI-Verl, Düsseldorf, Braunschweig, 2004.

[Ministry of Railway China 2011] Ministry of Railway China: **Investigation Report of "7.23 Yong-Wen Severe Railway Transportatoin Accident"**, 2011.

[Slovák 2006] Slovák, R.: **Methodische Modellierung und Analyse von Sicherungssystemen des Eisenbahnverkehrs**. Dissertation, Braunschweig, 2006.

Contacts

Dipl.-Wirtsch.-Ing. **René Sebastian Hosse**

Dirk Spiegel, M.Sc., M.Sc.

Institute for Traffic Safety and Automation Engineering
Technische Universität Braunschweig
Germany

{hosse; spiegel}@iva.ing.tu-bs.de

Backup

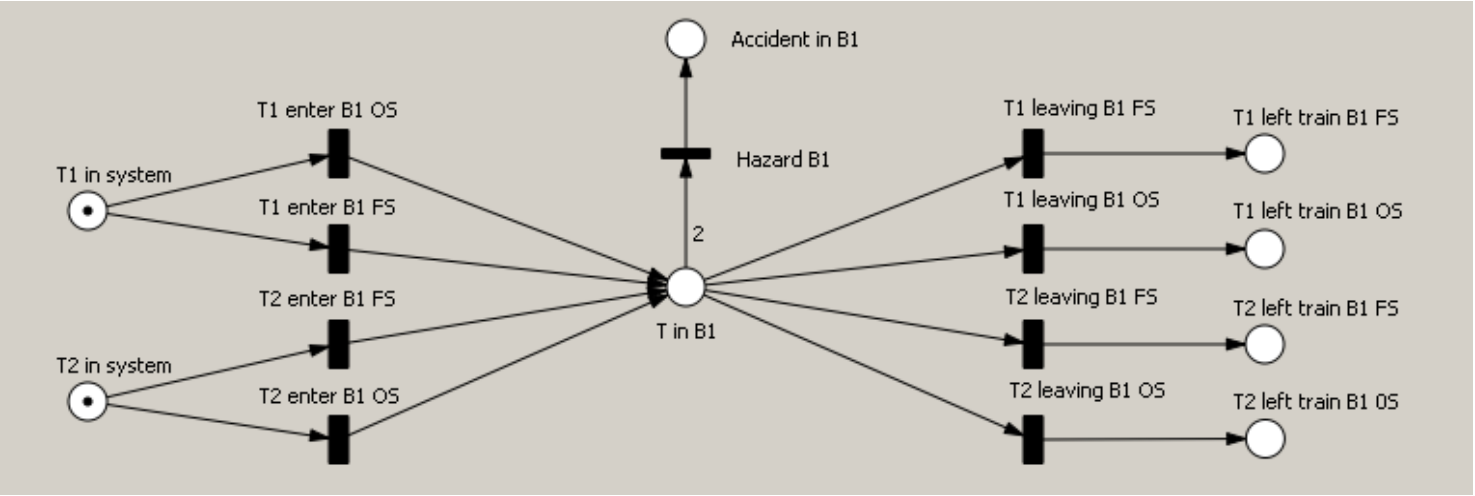
2. Goal of Hybrid Approach

Comparison of STAMP and ProFunD Approach

Technique / Methods / means of description	Suited for complex systems	Suited for new system designs	Qualitative Analysis (State space)	Quantitative Analysis (Probabilities/rates)	Quantitative Analysis (Stochastic distributions)	Simulation	Suited for combination of failures	Suited for order dependencies	Bottom Up or Top Down	Suited for allocation of safety requirements	Expert knowledge required	Acceptance and distribution	Tools needed	Plausibility checks	Availability of Tools	IEC Norm
ETA	-	-	-	○	-	○	-	+	B-U	-	○	○	○	+	○	62502
FMECA	-	-	-	○	-	-	-	-	B-U	-	+	+	○	+	+	60812
FTA	+	+	-	+	-	-	+	-	T-D	+	○	+	○	+	+	61025
HAZOP	-	-	-	-	-	-	-	-	B-U	-	○	○	○	+	○	61882
Markov	○	○	○	-	+	○	+	+	T-D	+	-	○	-	-	○	61165
RBD	+	-	○	+	+	-	+	-	T-D	+	-	○	○	+	○	61078
PN/ProFunD	**+**	**+**	**+**	**+**	**+**	**+**	**+**	**+**	**T-D**	**+**	**-**	**-**	**-**	**+**	**○**	**62551**
SD/STAMP	**+**	**+**	**-**	**-**	**-**	**-**	**+**	**+**	**T-D**	**+**	**+**	**-**	**-**	**○**	**○**	**62740**
SoTeRiA	+	+	-	+	+	+	+	+	T-D	-	-	-	-	○	○	---
CREAM / DREAM	○	○	-	+	-	-	○	+	T-D	-	-	-	○	○	○	---

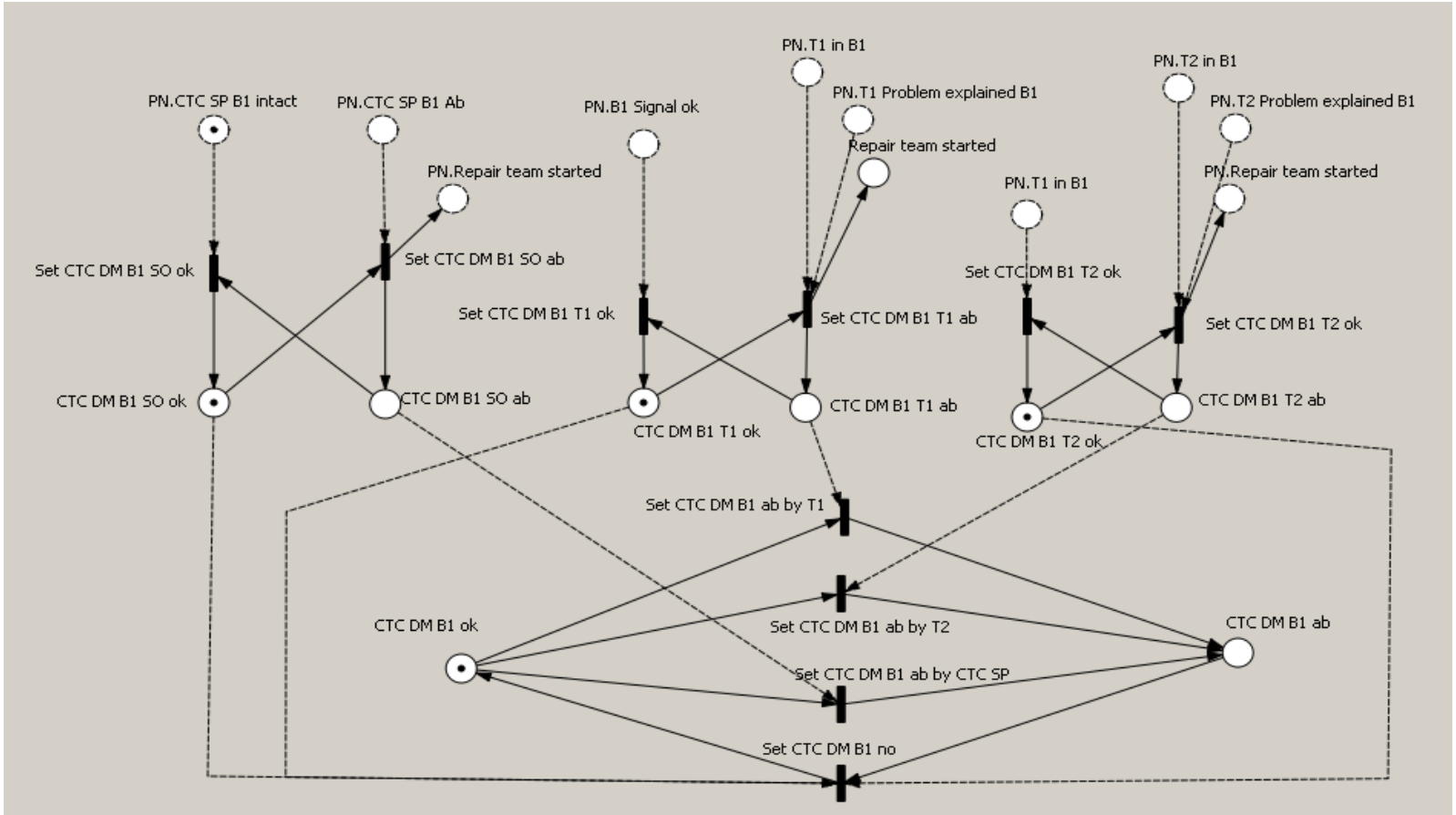
Application of STHAR
Petri net of the process

- Accidental condition = 2 trains in one block

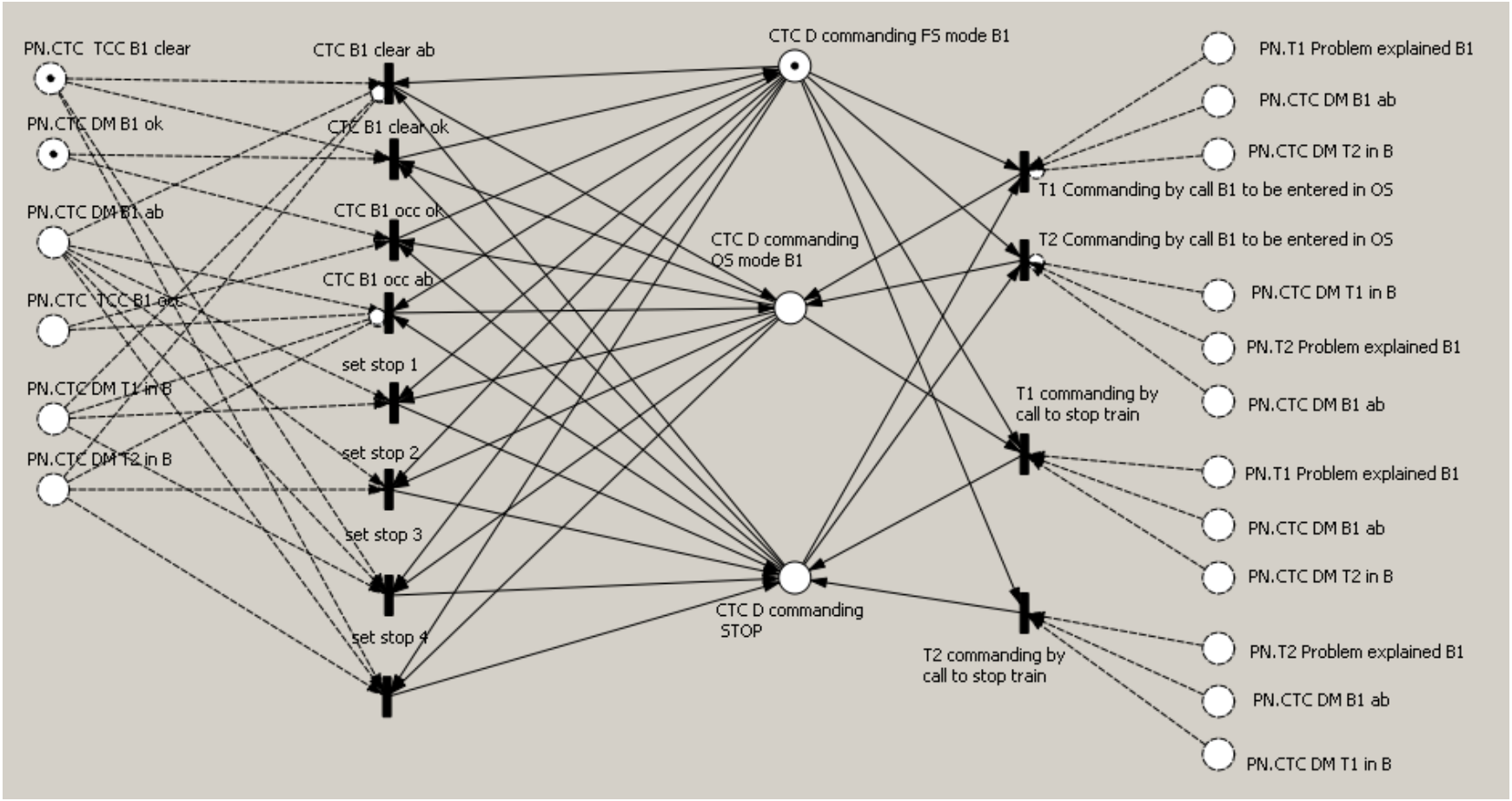


[Slovák 2006]

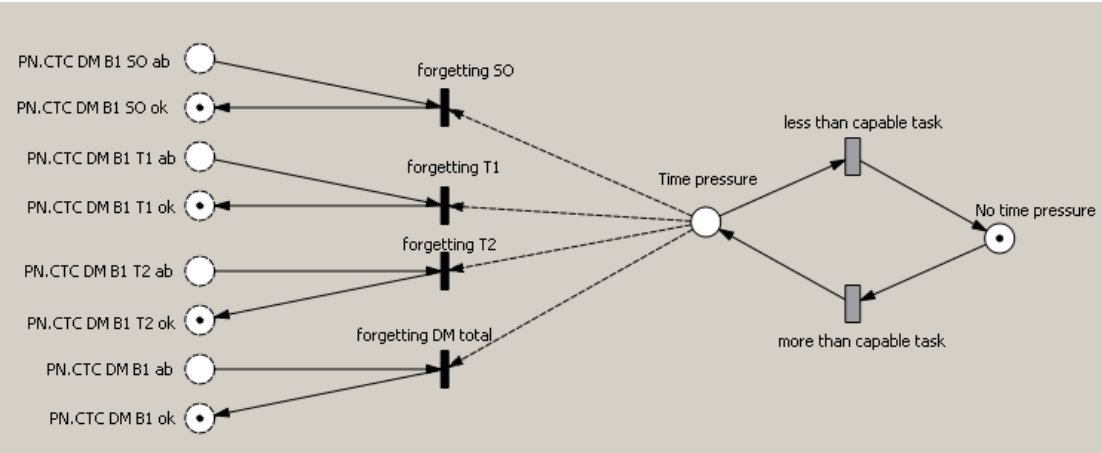
Application of STHAR
Petri Net of CTC dispatcher mental model



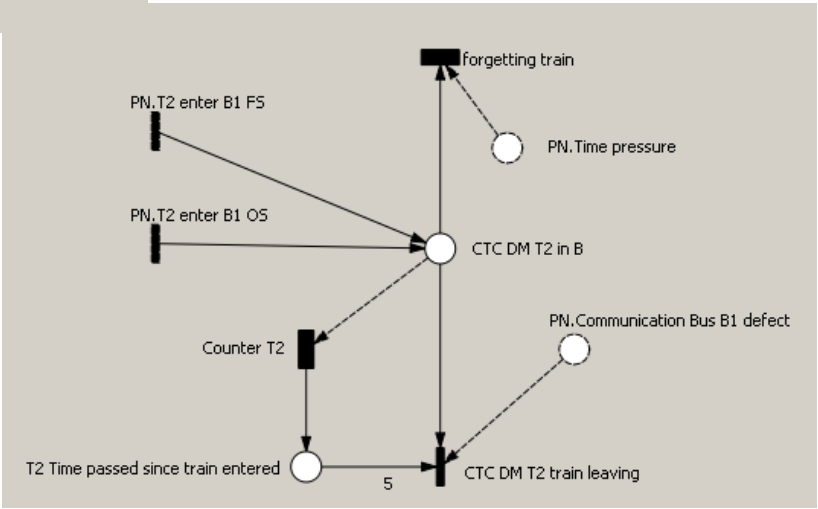
Application of STHAR
Petri net of the CTC Dispatcher functional model



Application of STHAR
Dependability CTC dispatcher



"Forgetting" of abnormal condition



Assumptions of mental tracking

2. Goal of Hybrid Approach

Objectives of the Hybrid Approach

Objectives of STAMP

- To use the *control structure* as a basis for the combination
- To take *socio-technical elements* into consideration
- To retain the *foundations of system theory* (emergence and hierarchy, communication and *control, process model)*
- *To facilitate a* state-based analysis method
- To ensure safety by integrating *safety constraints*

Objectives of ProFunD

- To provide *guidance* for the *model building process*
- To enable *hazard* and *accident analyses*

Objectives of STAMP/ProFunD

- To maintain *nonlinearity*
- To allow investigation into *causal effects*
- To allow *detection* of *states* leading to *hazards*
- To facilitate *qualitative and quantitative analysis*

[Slovák 2006] [Leveson 2011]