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

2) Goal of Hybrid Approach

3) Methodology
   (1) STAMP/CAST (to be known)
   (2) ProFunD
   (3) Hybrid Approach

4) Sample Application on Accident 7.23

5) Results and Discussions

6) Conclusions
1. Motivation
What do we do?

- Ground transportation safety
  - Automotive
    - Driver assistant systems / autonomous 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)

- **Mean of Description**
  - System Dynamics
  - Reliability Block Diagrams
  - Pen & Paper
  - Failure Trees
  - Petri net

- **Method**
  - STAMP/CAST/STPA
  - ProFunD
  - FMEA
  - CREAM

- **Tool**
  - SpecTRM
  - PiTool
  - Any Logic
  - Vensim
1. Motivation
Orthogonality: Thinking in Means of Description, Methods and Tools (3/3)
Contents

1) Motivation

2) Goal of Hybrid Approach

3) Methodology
   (1) STAMP/CAST (to be known)
   (2) ProFunD
   (3) Hybrid Approach

4) Sample Application on Accident 7.23

5) Results and Discussions

6) Conclusions
2. Goal of Hybrid Approach
Hybridization of qualitative approach and quantitative approach

Diagram:
- STAMP
- ProFunD
- STAMP + ProFunD
- Organization
- Technology
- Qualitative
- Quantitative

27. March 2013
Hosse, Spiegel, Schnieder | 2nd STAMP Workshop | MIT
Slide 10
Contents

1) Motivation

2) Goal of Hybrid Approach

3) Methodology
   (1) STAMP/CAST (to be known)
   (2) ProFunD
   (3) Hybrid Approach

4) Sample Application on Accident 7.23

5) Results and Discussions

6) Conclusions
3. Methodology
(2) ProFunD – Fundamental Concepts

- **Operative Process**
  - Modeling of Operative Process
- **Requirements Analyzes**
  - Model 1
  - Functional Synthesis and global dependability modeling
  - Model 2
  - Technical Synthesis and local dependability modeling
  - Model 3
- **Functional Design**
- **Technical Design**
- **Component Dependability**
- **Functional Layer**
- **Physical Processes**

---

*Slovak 2006*
3. Methodology
(3) Hybrid Approach – Analysis Process on the example of CAST

Identification of Proximate Events

Construction of Safety Control Structure

ProFunD-based Petri Net Model

Model Analysis and Evaluation

Recommendations
Contents

1) Motivation

2) Goal of Hybrid Approach

3) Methodology
   (1) STAMP/CAST (to be known)
   (2) ProFunD
   (3) Hybrid Approach

4) Sample Application on Accident 7.23

5) Results and Discussion

6) Conclusions
4. Sample Application
Accident introduction of the Wenzhou accident

- Lightning caused track circuit failure
- TC continued transmitting to the TTC the "block free signal"
- Transmitting incorrect signals
- Communication channel of D3115 was damaged
- CTC dispatcher "forgot" to track the train
- 7:30 pm track circuit was damaged
- 7:39 pm failure was detected
- 8:30 pm the accident happened

→ ~ 1 hour to fix and consider the failure

- Most of the accident report was dedicated to assign responsibilities and its punishments

[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)
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

1) Motivation

2) Goal of Hybrid Approach

3) Methodology
   (1) STAMP/CAST (to be known)
   (2) ProFunD
   (3) Hybrid Approach

4) Sample Application on Accident 7.23

5) Results and Discussion

6) Conclusions
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

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

[Airong Dong 2012]
Contents

1) Motivation

2) Goal of Hybrid Approach

3) Methodology
   (1) STAMP/CAST (to be known)
   (2) ProFunD
   (3) Hybrid Approach

4) Sample Application on Accident 7.23

5) Results and Discussion

6) Conclusions
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 contextual 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


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


Contacts

Dipl.-Wirtsch.-Ing. René Sebastian Hosse


Institute for Traffic Safety and Automation Engineering
Technische Universität Braunschweig
Germany

{hosse; spiegel}@iva.ing.tu-bs.de
## 2. Goal of Hybrid Approach
Comparison of STAMP and ProFunD Approach

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