Application of STAMP to Risk Analysis of High-speed Rail Project Management in the US

3/27/14

Soshi Kawakami
SM Candidate
MIT Engineering Systems Division
Systems Engineering Research Lab. (Aero. & Astr.)
Regional Transportation Planning and High-Speed Rail Research Group (CEE)

5/12/14 revision A
Institutional level:

Safety-related interactions among organizations in the industry
Contents

• Motivation
  – Issue in the northeast corridor
  – Rail safety in the US
  – Institutional structure

• Research objectives

• Proposed Methodology (5 steps)
  – How to integrate CAST, STPA, and System Dynamics

• Conclusion
Contents

• Motivation
  – Issue in the northeast corridor
  – Rail safety in the US
  – Institutional structure

• Research objectives

• Proposed Methodology (5 steps)
  – How to integrate CAST, STPA, and System Dynamics

• Conclusion
2013: High-speed rail (HSR) in operation [>155mph]

2025

Source: UIC
American Recovery and Reinvestment Act of 2009 (ARRA)

- Economic stimulus package. $8B for HSR study and planning.

Proposed corridors by FRA

Source: FRA vision for HSR 2009
Capacity Issue in NEC

Highway Congestion

*volume/capacity > 95%

Source: Amtrak vision for NEC 2012
Capacity Issue in NEC

Acela Express
- Max. 240km/h (150mph)
- Ave. 135km/h (84mph) due to poor condition of infrastructure

Solution → new HSR

Source: Amtrak
Rail Safety in the US
Train Accident Rate per Million Train Miles (US)

However...

Source: FRA

-50% (2004-2012)
...how safe?
Chinese HSR accident (2011)

http://www.democraticunderground.com/1002962288

Spanish HSR accident (2013)


...never happen in the US HSRs?
Key Safety Components for new HSRs in the US

1. Positive Train Control (PTC)
2. International-quality “service proven” trains
3. System Safety Program (SSP)

…but safe as a total system?
Institutional structure
General key parameters

• Vertical structure : separation or integration
• Track : dedicated or shared
• Ownership : private or public
• Market Competition : yes or no

Different institutional structures require different safety constraints in the systems
Current NEC HSR

Source: NEC master plan

One of the most complex structures in the world

New NEC HSR

Many alternatives of institutional structures are currently discussed

However...
Issue in new NEC Design

Timeline of Project Design

Current topics

2015

Next

Route, Service, and Technology

Safety-related regulation for HSRs

“In Neutral standpoint”

Institutional structure

Need to incorporate specific alternatives as safety-related factors?
Research Objectives

1. Develop a system-based safety risk analysis methodology based on lessons learned from past accidents for complex systems such as HSR systems

2. As a case study, the new HSR project in the NEC is analyzed by the proposed method with a specific focus on its institutional structure. The final goal of this research is to provide specific suggestions about safety management and regulation in the NEC HSR for project planners.
Contents

• Motivation
  – Issue in the northeast corridor
  – Rail safety in the US
  – Institutional structure

• Research objectives

• Proposed Methodology (5 steps)
  – How to integrate CAST, STPA, and System Dynamics

• Conclusion
Identified requirements

• Based on system-based lessons, not a single cause, learned from past key accidents

• Analyze a complex sociotechnical system

• Focus on an institutional level

• Deal with many alternatives of institutional structures

Oh Yes! STAMP!
Key research papers

Paper 1:
*Risk Management Approach for CO₂ Capture Project* (Samadi, 2012) *presented in STAMP workshop 2013*

Paper 2:
Proposed Methodology

Step 1: Accident analysis (CAST)

Step 2: Control Model development (generic model and alternatives)

Step 3: Risk analysis (STPA)

Step 4: Risk analysis (System Dynamics)

Step 5: Organize results
Expected Research Output

1. Unsafe controls and their causal factors for each alternative of the NEC HSR. System requirements and safety constraints to prevent them.

2. Weaknesses of key safety regulations applied to the NEC HSR

These outcomes can be valuable for the actual institutional design process as important decision-making criteria.
Proposed Methodology

Step 1:
Accident analysis (CAST)

Step 2:
Control Model development
(generic model and alternatives)

Step 3:
Risk analysis (STPA)

Step 4:
Risk analysis (System Dynamics)

Step 5:
Organize results
Step 1: Accident Analysis (CAST)

1) Choose accidents (Hatfield in UK, Wenzhou in China)
2) Develop their safety control models.
3) Identify inadequate controls, causal factors, and required constraints
4) Identify common safety constraints required at an institutional level

→ System-based lessons learned from past accidents
Proposed Methodology

Step 1: Accident analysis (CAST)

Step 2: Control Model development (generic model and alternatives)

Step 3: Risk analysis (STPA)

Step 4: Risk analysis (System Dynamics)

Step 5: Organize results
Step 2: Model development and gap analysis

1) Develop a generic HSR model.
2) Develop safety control models for three NEC alternatives.
3) Compare 1) with 2), and identify structural differences

System definition (top-down)

Accidents
→ System High level hazards
→ System requirements and constraints
  • ...
  • ...
  • ...
  • ...
  • ...
  • ...

Input from step 1

Generic model

General railway industrial structure (simple)

Alternatives 1-3 (NEC HSR - specific)

Paper, publication reviews
### Preliminary Risk Analysis (Comparative Analysis) [Generic vs. 3 NEC alternatives]

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Safety-related technical and managerial decision-making and its implementation must be</td>
<td>State-of-the-art safety standards and regulations regarding train operation must be independent, programmed, and acquired. The decision-making process during the state-of-the-art safety standards and regulations regarding train operations being independent from programmatic aspects such as cost and schedule of the system development/operation and other stakeholders of other agencies. The decision-making must be critical in safety standards and regulations as outlined.</td>
<td>Vertically separated structure could cause ambiguous decision-making in the decision-making process.</td>
<td>Partially separated structure could cause multiple decision-maker’s acquisition of broad knowledge of the criticality of the decision.</td>
<td>Vertically separated structure could cause multiple decision-maker’s acquisition of broad knowledge of the system’s priority of safety.</td>
<td></td>
</tr>
<tr>
<td>II. Safety considerations must be critical in technical and managerial decision-making and its implementation</td>
<td>Safety-related technical decision-making in train operations should be independent of programmatic considerations, including cost, schedule, and performance. (Lesson 2.1.2)</td>
<td>Having multiple TOCs could cause multiple decision-maker’s acquisition of broad knowledge of the system’s priority of safety.</td>
<td>Nothing.</td>
<td>Having multiple TOCs could cause multiple decision-maker’s acquisition of broad knowledge of the system’s priority of safety.</td>
<td></td>
</tr>
<tr>
<td>III. Safety-related technical and managerial decision-making and its implementation must be</td>
<td>Technical decision-making in train operations must be clear and unambiguous with respect to authority, responsibility, and accountability.</td>
<td>Nothing.</td>
<td>Having multiple TOCs could cause multiple decision-maker’s acquisition of broad knowledge of the system’s priority of safety.</td>
<td>Having multiple TOCs could cause multiple decision-maker’s acquisition of broad knowledge of the system’s priority of safety.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>All safety-related managerial decisions in train operation, before being implemented, must have the approval of the technical decision-maker.</td>
<td>Nothing.</td>
<td>Having multiple TOCs could cause multiple decision-maker’s acquisition of broad knowledge of the system’s priority of safety.</td>
<td>Having multiple TOCs could cause multiple decision-maker’s acquisition of broad knowledge of the system’s priority of safety.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mechanisms and processes must be created that allow and encourage all employees and contractors to communicate effectively to the train operations.</td>
<td>Nothing.</td>
<td>Having multiple TOCs could cause multiple decision-maker’s acquisition of broad knowledge of the system’s priority of safety.</td>
<td>Having multiple TOCs could cause multiple decision-maker’s acquisition of broad knowledge of the system’s priority of safety.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>All operators involved in train operations must be well-trained and certified to identify any system failure and to manage emergent situations (Lesson 2.1.3).</td>
<td>Nothing.</td>
<td>Having multiple TOCs could cause multiple decision-maker’s acquisition of broad knowledge of the system’s priority of safety.</td>
<td>Having multiple TOCs could cause multiple decision-maker’s acquisition of broad knowledge of the system’s priority of safety.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>High-quality, up-to-date analyses of train operation must be created.</td>
<td>Nothing.</td>
<td>Having multiple TOCs could cause multiple decision-maker’s acquisition of broad knowledge of the system’s priority of safety.</td>
<td>Having multiple TOCs could cause multiple decision-maker’s acquisition of broad knowledge of the system’s priority of safety.</td>
<td></td>
</tr>
</tbody>
</table>

Clarity the impact of structural difference (additional complexities), which could provide unsafe controls on safety constraints.
Proposed Methodology

Step 1: Accident analysis (CAST)

Step 2: Control Model development (generic model and alternatives)

Step 3: Risk analysis (STPA)

Step 4: Risk analysis (System Dynamics)

Step 5: Organize results
Step 3: Risk Analysis 1 (STPA of the NEC HSR)

1) Identify causes of hazards.
2) Identify causal factors, in the context of the actual NEC’s approach
## 58 types of NEC-specific risks are Identified

<table>
<thead>
<tr>
<th>Controller</th>
<th>Controlled Entity</th>
<th>Risk</th>
<th>Type of Causal Factor</th>
<th>Type of Risk</th>
<th>Alt. 1</th>
<th>Alt. 2</th>
<th>Alt. 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulation/certification Agency</td>
<td>System Integrators (rolling stock, infrastructure) *Partially applicable to Train Operating Company [Amtrak], Infrastructure Owners/Operators</td>
<td>1</td>
<td>Inadequate process model</td>
<td>General</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>Incorrect process model</td>
<td>General</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>Inadequate decision making algorithm</td>
<td>General</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>Inadequate feedback</td>
<td>Immediate</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>Wrong input</td>
<td>General</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6</td>
<td>Wrong input</td>
<td>General</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7</td>
<td>Inadequate process model</td>
<td>General</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8</td>
<td>Inadequate process model</td>
<td>General</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>System Integrators (rolling stocks or infrastructure)</td>
<td>R&amp;D Company/Suppliers (rolling stocks or infrastructure)</td>
<td>9</td>
<td>Inadequate process model</td>
<td>Immediate</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10</td>
<td>Inadequate input</td>
<td>Immediate</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11</td>
<td>Inadequate process model</td>
<td>Immediate</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12</td>
<td>Inadequate process model</td>
<td>General</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>13</td>
<td>Missing input</td>
<td>Immediate</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>14</td>
<td>Inadequate process model</td>
<td>General</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>Inadequate control algorism</td>
<td>General</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>16</td>
<td>Inadequate control algorism</td>
<td>General</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>17</td>
<td>Missing input</td>
<td>General</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>18</td>
<td>Process failure</td>
<td>Immediate</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>R&amp;D Company/Suppliers (rolling stocks or infrastructure)</td>
<td>Manufacturers (rolling stocks or infrastructure)</td>
<td>19</td>
<td>Inadequate process model</td>
<td>General</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Regulation/certification Agency</td>
<td>Train Operating Company, Infrastructure Owners/Operators (or Infrastructure Owner and Infrastructure Operator)</td>
<td>20-1</td>
<td>Inadequate control algorism</td>
<td>General</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>20-2</td>
<td>Inadequate control algorism</td>
<td>General</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>20-3</td>
<td>Inadequate control algorism</td>
<td>General</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>21</td>
<td>Inadequate process model</td>
<td>General</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Train Operator</td>
<td></td>
<td>22</td>
<td>Inadequate process model</td>
<td>General</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Maintenance Company (rolling stocks)</td>
<td></td>
<td>23</td>
<td>Inadequate feedback</td>
<td>General</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>24</td>
<td>Conflicting control action</td>
<td>General</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>25</td>
<td>Inadequate feedback</td>
<td>Immediate</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>26</td>
<td>Inadequate feedback and inadequate process model</td>
<td>Immediate</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>27</td>
<td>Inadequate process model</td>
<td>Immediate</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>28</td>
<td>Inadequate feedback</td>
<td>Immediate</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>29</td>
<td>Inadequate feedback from other controlled entities</td>
<td>General</td>
<td>x</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Proposed Methodology

Step 1: Accident analysis (CAST)

Step 2: Control Model development (generic model and alternatives)

Step 3: Risk analysis (STPA)

Step 4: Risk analysis (System Dynamics)

Step 5: Organize results
Why System Dynamics model?

• Integrate interrelated causal relations of some risks identified in STPA

• Incorporate indirect causal factors and impact of multiple changes within the entire safety control structure.

• Provide information about positive/negative feedback loops in causal relations (dynamic behavior)

• Help understand causal relation visually
Step 4: Risk Analysis 2 (SD-based analysis of the NEC HSR)

1) Develop a System Dynamics model, integrating the causal relations of the key risks identified in Step 3.
2) Analyze the detailed causal relations.

Risk 23, 24, 33, 34, 37, and 58

Focus 1: Coordination in operation

Focus 2: Market competition

Risk 39, 53, and 54
Proposed Methodology

Step 1: Accident analysis (CAST)

Step 2: Control Model development (generic model and alternatives)

Step 3: Risk analysis (STPA)

Step 4: Risk analysis (System Dynamics)

Step 5: Organize results
Step 5: Organize the results

Discuss weaknesses of regulations applied to the NEC HSR.

- System Safety Program (49 CFR 270, proposed rule in 2012)
- Etc.

E.g., System Safety Program (49 CFR Part 270, proposed rule in 2012)

<table>
<thead>
<tr>
<th>No.</th>
<th>SSP Items</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Purpose and scope of system safety program</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>System safety program goals</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Railroad system description</td>
<td>Risk * could be ...</td>
</tr>
<tr>
<td>4</td>
<td>Railroad management and organizational structure</td>
<td>Risk * and ** are not considered ...</td>
</tr>
<tr>
<td>5</td>
<td>System safety program implementation plan</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Maintenance, inspection and repair program</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Rules compliance and procedures review</td>
<td>Risk * and ** are not considered ...</td>
</tr>
<tr>
<td>8</td>
<td>System safety program employee/contractor training</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Emergency management</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Workplace safety</td>
<td></td>
</tr>
</tbody>
</table>

+ Prioritize risks and design safety constraints (in practice)
Conclusion

• Developed a STAMP-based risk analysis methodology with a specific focus on past accidents’ lessons and institutional structures.

• As a case study, the HSR project in the NEC is analyzed. Three alternatives of the institutional structure are taken into account. As a result,
  – 58 NEC-specific risks are identified in STPA.
  – With SD model, their causal relations are further analyzed.
  – Several weaknesses of regulations for HSR systems are identified.

This research suggests that project planners for the NEC HSR adopt this methodology and analyze risks with experts from diverse organizations involved in the project, thereby harmonizing risk managements performed by these diverse organizations in a consistent way.
Questions?

Soshi Kawakami
soshi@mit.edu
**Terminology**

**Accident**: An undesired and unplanned event that results in loss of human life or human injury.

**Hazard**: A system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss).

**Risk**: Risk is the hazard level combined with the likelihood of hazard leading to an accident (sometimes called danger) and hazard exposure or duration (sometimes called latency). Specifically, this research refers to a system state that has an *unsafe control action(s)* and its *causal factor(s)* identified in the context of the actual NEC HSR’s situation, which could lead to an accident, as a safety risk of the NEC HSR.

**Safety**: The freedom from accidents or losses.
Discussed processes in this thesis as risk analysis, in the context of ISO 60300-3-9
Process discussed in this thesis

Risk Analysis (definition in this thesis)

ISO 31000 (2009)
Key Processes of Railway Projects

Model development: processes focused on

- Project Design
- Project Evaluation

Processes focused on

- R&D, Design
- Manufacturing
- Train Operation
- Maintenance
- Construction (track)
System Development

R&D, Design, Manufacturing

- System Integrator (rolling stock)
  - Regulation/certification Agency
    - R&D, Suppliers (rolling stock)
      - Manufacturer
        - Physical System

Train Operation

- System Integrator (infrastructure)
  - Regulation/certification Agency
    - System Integrator (infrastructure)
      - TOC
        - Dispatcher
          - Train Operator
            - Physical System (Train, Signal System, Rails)

Maintenance

- System Integrator (infrastructure)
  - Regulation/certification Agency
    - System Integrator (infrastructure)
      - IM
        - Maintenance Worker
          - Maintenance Company (rolling stock)
            - Physical System (rolling stock)

- System Integrator (infrastructure)
  - Regulation/certification Agency
    - System Integrator (infrastructure)
      - Maintenance Worker
        - Maintenance Company (Infrastructure)
          - Physical System (Infrastructure)