A System Theoretic Analysis of the “7.23” Yong-Tai-Wen Railway Accident

1st STAMP/STPA Workshop
Lecturer: Dajiang Suo
Tsinghua University
2012-4
Outline

- Background
- Chain of Events
- Safety control structure
- System dynamics of this accident
- Conclusion
Location of the accident

Centralized Traffic Control (CTC) Center
Shanghai Railway Bureau

Zhejiang Province

Yong-Tai-Wen Railway Line

Accident location

Wenzhou

To Fuzhou

Yong-Tai-Wen Station

TC-5829

Velocity <= 20km/h

TC-5845

TC-5815

Velcity >= 100km/h

D301

Signal device (supposed to be red)

Yongjia station

Train Control Center (TCC)

(Abnormal operational mode)

Wenzhou

Wenzhou Station
People involved

- Drivers (D3115&D301)
- Watch keep (Wenzhou Station)
- Electrical Workers
- Dispatcher (Shanghai Railway Bureau)
**Signal & Communication System**

**Centralized Train Control System** – Level 2  
(Designed for speed 200-250 km/h)

**Ground System**
- **Train Control Center - TCC**  
- **Track circuit**

**Train-Mounted system**
- **Automatic Train Protection** - (ATP): Control the train automatically and stop it in case of emergency
Important Definition

“Red Light Strip” - represents the occupancy of the TC by the Train. Sometimes failures in the TC could lead to it;

“Occlusive Section” – Provide protection mechanisms which prevent two trains from travelling at different speed in the same “Occlusive Section”;

“Decentralized autonomous control mode”

“Unconventional station control mode”
Outline

✓ Background

➢ Chain of Events

❖ Safety control structure

❖ System dynamics of this accident

❖ Conclusion
Chain of Events
Outline

✓ Background
✓ Chain of Events
➢ Safety control structure
▫ System dynamics of this accident
▫ Conclusion
## Generic Components - Development

<table>
<thead>
<tr>
<th>Components in hierarchical safety control structure (Development)</th>
<th>The corresponding components in Chinese railway system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governments regulation agencies</td>
<td>Chinese Ministry of Railways</td>
</tr>
<tr>
<td>Governments regulation agencies</td>
<td>Zhejiang Government</td>
</tr>
<tr>
<td>Maintenance and Evolution</td>
<td>Shanghai Railway Bureau</td>
</tr>
<tr>
<td>Company Management</td>
<td>CoastalRailway Zhejiang Co. LTD</td>
</tr>
<tr>
<td>Project Management</td>
<td>China Railway Signal &amp; Communication Corporation (CRSC)</td>
</tr>
<tr>
<td>Design and Implementation</td>
<td>Beijing National Railway Research &amp; Design Institute of Signal &amp; Comm Co. LTD</td>
</tr>
<tr>
<td>Safety Assurance</td>
<td>System Integration Group</td>
</tr>
</tbody>
</table>
## Generic Components - Operation

<table>
<thead>
<tr>
<th>Components in hierarchical safety control structure (Operation)</th>
<th>The corresponding components in Chinese railway system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governments regulation agencies</td>
<td>Chinese Ministry of Railways</td>
</tr>
<tr>
<td>Safety Assurance and Supervision</td>
<td>Shanghai Railway Bureau</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Electrical &amp; Signal Office</td>
</tr>
<tr>
<td>Operation</td>
<td>Transportation Office</td>
</tr>
<tr>
<td>Operation &amp; Maintenance</td>
<td>Wenzhou Station</td>
</tr>
</tbody>
</table>
Safety Control Structure

System Development

- The Ministry of Railways
  - Shanghai Railway Bureau
    - Coastal Railway Zhejiang Co. LTD.
      - System integration group
        - China Railway Signal & Communication Corporation (CRSC)
          - CRSCD
            - Development and testing of TCC - LKD2-T1

- The Ministry of Railways
  - Zhejiang Government
    - System development
      - High-Speed Train System Operation
        - CTCS
          - Track circuit
            - Train Control Center (TCC) (LKD2-T1)
              - CTCS
                - CTC
                  - High-Speed Train
                    - D3115
                      - D301

- The Ministry of Railways
  - Construction office
    - Electrical & Signal office
      - Transportation office
        - Dispatcher
          - Watch keeper
            - Signal Engineer
System Hazard and safety constraints

- **System Hazard:** Two trains are on the same “Occlusive Section” travelling at different speed

- **Safety Constraints:**
  1. When a track section is occupied by a train, the TCC transmits control parameters representing track occupancy to other trains and issues warning signals (red) to the signal device in front of this section.
  2. The failures in the Train Control System must be identified and provided as feedback to the dispatcher of CTC in time.
  3. The dispatcher in the CTC and the watch keeper should identify the potential danger in the railway line and command the train to slow down or stop in emergency situations.
High-Speed Train

Automatic Train Protection (ATP)

Roles and Responsibilities:
1. Perform calculation of the control parameters based on the data provided by Track Circuit and automatically control the train
2. Stop the train when it receives abnormal or no signal from Track Circuit

Roles and Responsibilities:
1. Display Orders from the dispatcher (Through GSM-R)
2. Display Info from the watch keeper (Through GSM-R)
3. Data input from Track circuit

Driver

Roles and Responsibilities:
Manually control the train in on-sight mode and decide the speed according to the dispatching orders from the dispatcher.
Level 2 Structure

Train Control Center (TCC)
(LKD2-T1)
Roles and Responsibilities:
- Encode signal for transmission of the Track Circuit
- Control the signal light of track section
- Give the movement authority to the train in a specified track section

Dispatcher
Roles and Responsibilities:
- Monitor traffic conditions in the sections between railway stations
- Handle emergencies in time to ensure train safety
- Issue dispatching command

Centralized Traffic Control (CTC)
Display status of Track Circuit and Trains
Dispatching commands

Track circuit (ZPW-2000A):
Roles and Responsibilities:
- Testing Track occupation

Track circuit (ZPW-2000A):
Roles and Responsibilities:
- Transmit control signal from the TCC to the train

The operational process of D301 and D3115

Display & Controls

Dispatcher

Electrical Worker

Train Control Center (TCC)
(LKD2-T1)

Track circuit (ZPW-2000A)
Roles and Responsibilities:
- Testing Track occupation

Level 2

Level 1

GSM-R
Communication Channel

Watch Keeper

Sensors

Actuators

Missing Controls or Missing Feedbacks
Level 3 Structure

The Minister of Railways

Transportation Bureau
Department of Science and Technology
Department of Fundamental

Shanghai Railway Bureau
Safety Constraint:
Supervise the implementation of safety regulations;
Train the staff (e.g. dispatcher and watch keeper) to improve their awareness of safety and the ability to respond to emergencies;

Overlapping areas and poor coordination
Outline

✓ Background
✓ Chain of Events
✓ Safety control structure
➢ System dynamics of this accident
★ Conclusion
System development

- Incentives to economic development – Easy access to labors and raw material
# Plan for the high-speed Railways within Zhejiang Province in 2010

<table>
<thead>
<tr>
<th>Railway lines</th>
<th>Start</th>
<th>Finish</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yong-Tai-Wen</td>
<td></td>
<td>Finished</td>
</tr>
<tr>
<td>Shanghai-Hangzhou</td>
<td></td>
<td>Finished</td>
</tr>
<tr>
<td>Hangzhou-Ningbo</td>
<td>2008.12</td>
<td>2011</td>
</tr>
<tr>
<td>Hangzhou-Nanjing</td>
<td>2008.12</td>
<td>2011</td>
</tr>
<tr>
<td>Hangzhou-Changsha</td>
<td>2009</td>
<td>2013</td>
</tr>
<tr>
<td>Hangzhou-Huangshan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shangqiu-Hangzhou</td>
<td>Plan-2011</td>
<td></td>
</tr>
<tr>
<td>Nantong-Jiaxing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Huzhou-Shanghai</td>
<td>Plan-2012</td>
<td></td>
</tr>
</tbody>
</table>
Goal – The first province in China to realize modernization of high-speed Railways
System Operation

"Performance priority over safety"

"Problems fixation"

- Extent of competition from civil aviation/highway transportation
- Critics from the public and the media
- Performance pressure
- Effect and strictness of supervision
- Safety priority
- Risk behaviors
- Incidents and Accidents
- Arrivals behind schedule
- External unsafe conditions
- Confidence in the current safety structure
Experimental Analysis

"Performance priority over safety"

"Problem fixation by management and supervision"

"Problem fixation by staff"
Simulation results

Safety priority: Current
System safety: Current

Incidents and Accidents rate: Current
Conclusion - See the “7.23” accident from a system perspective based on STAMP

- Safety regulations must be established to ensure the enforcement of safety constraints
- Channels for transmitting feedback should be kept open
- Human and organizational factors play a critical role in the accidents
- Safety commitment must be made during the whole process of the system development and operation
Thanks!

Q&A

Email: sdj08@mails.tsinghua.edu.cn