Identification of causal scenarios and application of leading indicators in the interconnection mode of urban rail transit based on STPA

Mo Li, Fei Yan, Nannan Xiang, Ru Niu, Tao Tang, Jidong Lv
Introduction

Leading indicator in metro operation
  • sources
  • characteristics
  • steps of identification

Application of STPA and leading indicator

Conclusions
INTRODUCTION

urban rail transit

- hybrid control
  - human (driver, dispatcher)
  - machine (train control system)
- interaction & cooperation
- multiple factors
  - environment
  - human
  - machine
  - management
INTRODUCTION

- **Interconnection**: Trains on one line can run across other lines without decelerating or degrading.
- **Cross-line**: the train is controlled by two controllers of two lines.
• same equipment
• different control structure
• different function
• new hazards
INTRODUCTION

How to find risks?
- STPA

How to monitor risks?
- Leading indicator

- Normal and abnormal operation scenarios
- Stopping at station; jumping; fire;
- Daily operation

- Detailed abnormal scenarios
- Passenger falling off the platform without Platform Screen Door
- Detailed safety constraints

- Signs of abnormal scenarios
- PSD broken
- Monitor during operation
**Sources of leading indicators in urban rail transit operation:**

- **two levels:** train operation process, and daily management

---

## Leading Indicator in Metro Operation

(part of) leading indicators for metro operation

<table>
<thead>
<tr>
<th></th>
<th>Leading indicators in operation (L1)</th>
<th>Leading indicators in management (L2)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Machine</strong></td>
<td>in abnormal working state;</td>
<td>weariness;</td>
</tr>
<tr>
<td></td>
<td>error beyond allowable range;</td>
<td>maintenance record;</td>
</tr>
<tr>
<td><strong>Personnel</strong></td>
<td>absence without leave;</td>
<td>examination result;</td>
</tr>
<tr>
<td></td>
<td>donzing and chatting;</td>
<td>error records;</td>
</tr>
<tr>
<td><strong>Environment</strong></td>
<td>bad weather;</td>
<td>construction around the line or machine;</td>
</tr>
<tr>
<td></td>
<td>temperature and humidity, etc.</td>
<td>application of new technologies;</td>
</tr>
<tr>
<td></td>
<td>passenger flow, etc.</td>
<td></td>
</tr>
<tr>
<td><strong>Organization and</strong></td>
<td>senior management of emergency</td>
<td>no safety inspection plan;</td>
</tr>
<tr>
<td><strong>management</strong></td>
<td>treatment absence without leave;</td>
<td>lack of personnel;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>lack of training and learning;</td>
</tr>
</tbody>
</table>
Steps for identifying leading indicators:

1) define purpose of the analysis
2) model the control structure
3) identify unsafe control actions
4) identify loss scenarios

- Determine the object and user of the indicators
- Identify specific leading indicators based on unsafe control actions
- Identify safety assumptions
- Add more leading indicators according to casual scenarios and safety assumptions
APPLICATION IN CROSS-LINE SCENARIO

simplified layout of Chongqing Metro Line

BEIJING JIAOTONG UNIVERSITY
### STPA Step 1: System level accidents and hazards

<table>
<thead>
<tr>
<th>No.</th>
<th>Accident</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>The train derails</td>
</tr>
<tr>
<td>A2</td>
<td>The train squeezes at switch</td>
</tr>
<tr>
<td>A3</td>
<td>The train hits obstacles that violated the limit</td>
</tr>
<tr>
<td>A4</td>
<td>The train hits personnel</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>No.</th>
<th>Hazard</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1</td>
<td>The train exceeds speed limit on tie line</td>
</tr>
<tr>
<td>H2</td>
<td>The train exceeds speed limit of switch P2602</td>
</tr>
<tr>
<td>H3</td>
<td>The train exceeds speed limit of switch P10</td>
</tr>
</tbody>
</table>
APPLICATION IN CROSS-LINE SCENARIO

STPA Step 2: Control structure

Process model

**Variables:**
1. current location L_C
2. operation direction D
3. MA2
4. switch information S_SWITCH
5. route rules R

**Control rules:**
1. end of MA ≤ min\{R, S_SWITCH, MA2\}[D]

Loop Line CI

Switch information S_SWITCH Route state R

Loop Line ZC

Process model

**Variables:**
1. current location L_C
2. operation direction D
3. switch information S_SWITCH
4. route rules R

**Control rules:**
1. end of MA ≤ min\{R, S_SWITCH[D\}

Line 10 CI

Switch information S_SWITCH Route state R

Line 10 ZC

Process model

**Variables:**
1. current speed S_c
2. current location L_C
3. operation direction D
4. speed limit of tie line S_limit
5. speed limit of P2502 S_limit
6. spliced MA1
7. spliced MA2

**Control rules:**
1. \(S_c \leq S_{limit}\) \land \(S_c \leq S_{limit}\)
2. \(L_C \in\{\text{spliced MA1}\} \land L_C \leq L_{boundary~point}\)

Trackside server

Speed limit of tie line

Speed limit of switch P10

Spliced MA1

Spliced MA2

Current location L_C

operation direction D

Brake

Braking system

A TP

Train

Current location

Current speed

Speed sensor

BTM

Current location

BEIJING JIAOTONG UNIVERSITY
APPLICATION IN CROSS-LINE SCENARIO

Leading indicator Step 1: Determine the object and user of the indicators

- objects of leading indicators:
  - Loop Line ZC and CI
  - Line 10 ZC and CI
  - ATP
  - Braking system
  - BTM
  - Balise
  - Speed sensor
  - Communication system
- users of leading indicators:
  - Driver
  - Dispatchers
### STPA Step 3: Unsafe Control Action

<table>
<thead>
<tr>
<th>System level accident</th>
<th>Control action</th>
<th>Not providing</th>
<th>Providing</th>
<th>Out of order</th>
<th>Stopped too soon or applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1: The train derailed due to overspeed in the axle counting section JZ2604-JZ2608 during the cross-line turnaround phase</td>
<td>Spliced MA1</td>
<td>UCA1: MA1 sent to ATP by Loop line ZC includes dangerous point</td>
<td>UCA2: Loop line ZC sent MA too late</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Braking</td>
<td>UCA3: The braking system did not provide sufficient braking force</td>
<td>N/A</td>
<td></td>
<td>UCA4: The braking system provided braking too late</td>
<td>UCA5: The braking system stopped applying brakes prematurely</td>
</tr>
<tr>
<td>Traction</td>
<td>N/A</td>
<td>UCA6: The traction system applied traction when parking</td>
<td>N/A</td>
<td></td>
<td>UCA7: The traction system applied traction for too long</td>
</tr>
</tbody>
</table>
APPLICATION IN CROSS-LINE SCENARIO

Leading indicator Step 2: (part of) leading indicators according to Unsafe Control Action

<table>
<thead>
<tr>
<th>UCA</th>
<th>Leading Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCA1</td>
<td>LI01: Improper selection of ZC (L2)</td>
</tr>
<tr>
<td></td>
<td>LI02: ZC once calculated MA wrong (L2)</td>
</tr>
</tbody>
</table>
STPA Step 4: causal scenarios

1. Incorrect CA2

2. Incorrect switch information S_{\text{S.WITCH}}
3. Incorrect route state R

6. Control algorithm does not follow control rules

Loop line CI

Loop line ZC

19. The status of the dangerous points on the track surface obtained by the driver is inconsistent with the actual situation

Trackside server

Splicing MA1

7. Incorrect speed limit of the tie line or turnout P2602

18. Error in transmission of current location from BTM to ATP

17. Error in transmission of current speed from the speed sensor to the ATP

15. Speed sensor hardware failure

16. BTM hardware failure

8. Error in transmission of brake from ATP to brake system

9. Brake system hardware failure

10. Error in transmission from brake system to vehicle

11. Error in transmission from the balise to the vehicle BTM antenna

12. The acquisition path of the speed sensor fails

14. Transmission from Vehicle BTM antenna to BTM transmission fails

20. The status of the dangerous points on the track surface obtained by the driver is inconsistent with the actual situation
### APPLICATION IN CROSS-LINE SCENARIO

#### STPA Step 4: (part of) causal scenarios and safety constraints

<table>
<thead>
<tr>
<th>No</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Causal Scenario</strong></td>
<td></td>
</tr>
<tr>
<td>S01</td>
<td>When MA2 of ZC line 10 is 0 and P10 is not locked in the reverse position, Loop line ZC spliced MA1 over the boundary point, causing the train to split and derail at P10.</td>
</tr>
<tr>
<td><strong>Safety Constraint</strong></td>
<td></td>
</tr>
<tr>
<td>SC01</td>
<td>The Loop line ZC should use the newly received MA2 for the calculation of spliced MA1.</td>
</tr>
<tr>
<td>SC02</td>
<td>The communication cycle between the Loop Line ZC and Line 10 ZC should be no more than Xs.</td>
</tr>
<tr>
<td><strong>Causal Scenario</strong></td>
<td></td>
</tr>
<tr>
<td>S02</td>
<td>When the switch P2602 is not locked in the reverse position, the Loop Line ZC uses the wrong MA1 in the calculation of the splicing MA1, causing the train to derail at the switch P2602.</td>
</tr>
<tr>
<td><strong>Safety Constraint</strong></td>
<td></td>
</tr>
<tr>
<td>SC03</td>
<td>The loop line ZC should use the latest MA1 for the calculation of splicing MA1.</td>
</tr>
</tbody>
</table>
### APPLICATION IN CROSS-LINE SCENARIO

#### Leading indicator Step 3: (part of) safety assumption

<table>
<thead>
<tr>
<th>System level accident</th>
<th>Control action</th>
<th>Not providing</th>
<th>Providing</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1: The train derailed ...</td>
<td>Spliced MA1</td>
<td></td>
<td>UCA1: MA1 sent to ATP by Loop line ZC includes dangerous point</td>
</tr>
</tbody>
</table>

- **Safety assumption**
  - usually implied in the requirements analysis and design phases, basic conditions for the normal operation of the system
<table>
<thead>
<tr>
<th>Causal Scenario</th>
<th>Safety Assumption</th>
</tr>
</thead>
<tbody>
<tr>
<td>S01</td>
<td>SA01: Spliced MA under the worst condition including communication cycle, communication delay and so on is sufficient to ensure safety</td>
</tr>
<tr>
<td></td>
<td>SA02: When the train does not receive MA within the specified time, braking will be implemented</td>
</tr>
<tr>
<td></td>
<td>SA03: When the status of the route changes, ZC will immediately update the MA</td>
</tr>
<tr>
<td></td>
<td>SA04: When the MA calculated by ZC changes, it will immediately send a new MA to ATP and overwrite the previous MA.</td>
</tr>
</tbody>
</table>
### APPLICATION IN CROSS-LINE SCENARIO

**Leading indicator Step 4: (part of) leading indicator**

<table>
<thead>
<tr>
<th>Causal Scenario</th>
<th>Safety Constraint and Safety Assumption</th>
<th>Leading Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>S01</td>
<td>SC01: Improper selection of Loop Line ZC (L2)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SC02</td>
<td>LI04: The communication delay between Loop Line ZC and CI is too large (L1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✅</td>
</tr>
<tr>
<td></td>
<td>SA01: Construction in the line or surrounding (L2)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SA02: Improper selection of ATP (L2)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LI07: The brake system calls for maintenance more frequently (L2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LI08: The service life of the braking system is too long (L2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LI09: The vehicle made an abnormal noise (L1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✅</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LI10: Alarm by braking system (L1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✅</td>
</tr>
<tr>
<td></td>
<td>SA02/03/04</td>
<td>LI11: Improper selection of braking system (L2)</td>
</tr>
</tbody>
</table>
CONCLUSION

- STPA provides more detailed scenario for the train operation process
- a new approach for monitoring: leading indicators
- more comprehensive than experience
- not only individual, but also the system

- future work
  how much does it help
  how to use the indicators
Thank you!