北京交通大學
BEIJING JIAOTONG UNIVERSITY

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

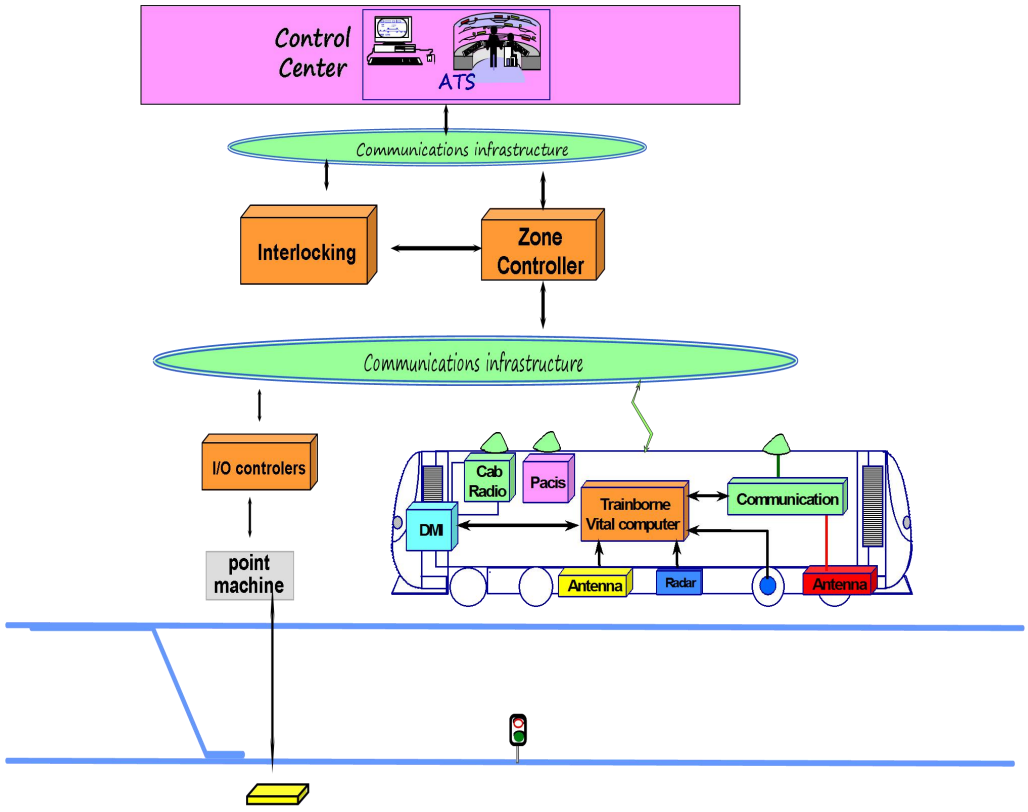
Mo Li, Fei Yan, Nannan Xiang, Ru Niu, Tao Tang, Jidong Lv

OUTLINE

- Introduction
- Leading indicator in metro operation
  - sources
  - characteristics
  - steps of identification
- Application of STPA and leading indicator
- Conclusions

INTRODUCTION

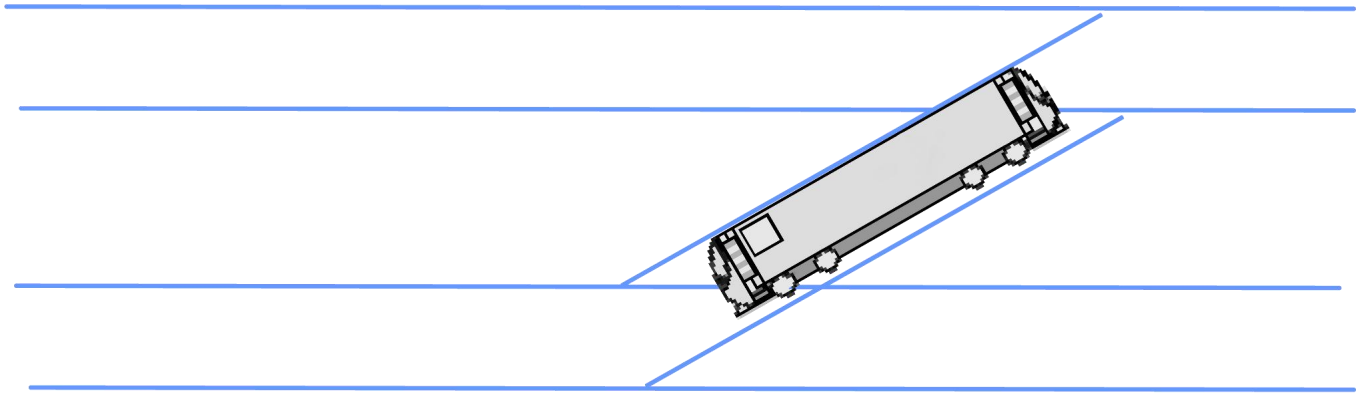
urban rail transit



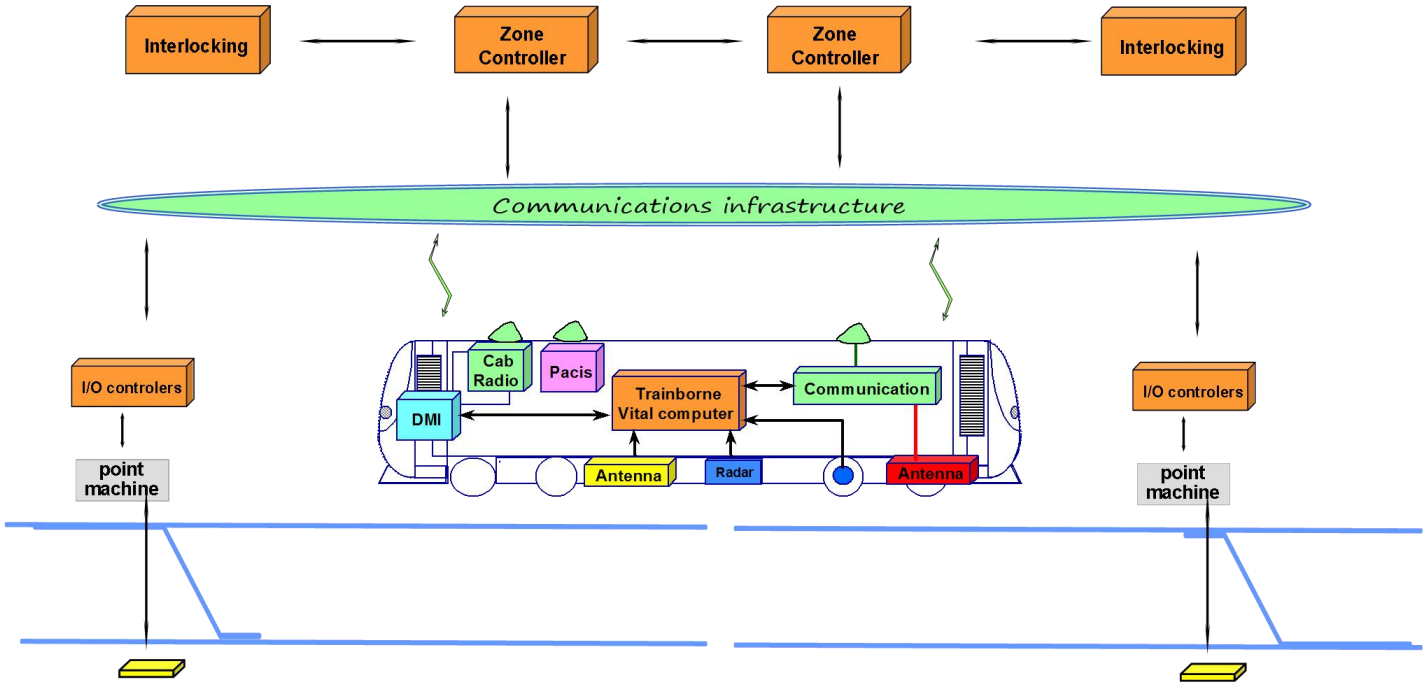
- hybrid control
  - human (driver, dispatcher)
  - machine (train control system)
- interaction & cooperation
- multiple factors
  - environment
  - human
  - machine
  - management

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



INTRODUCTION

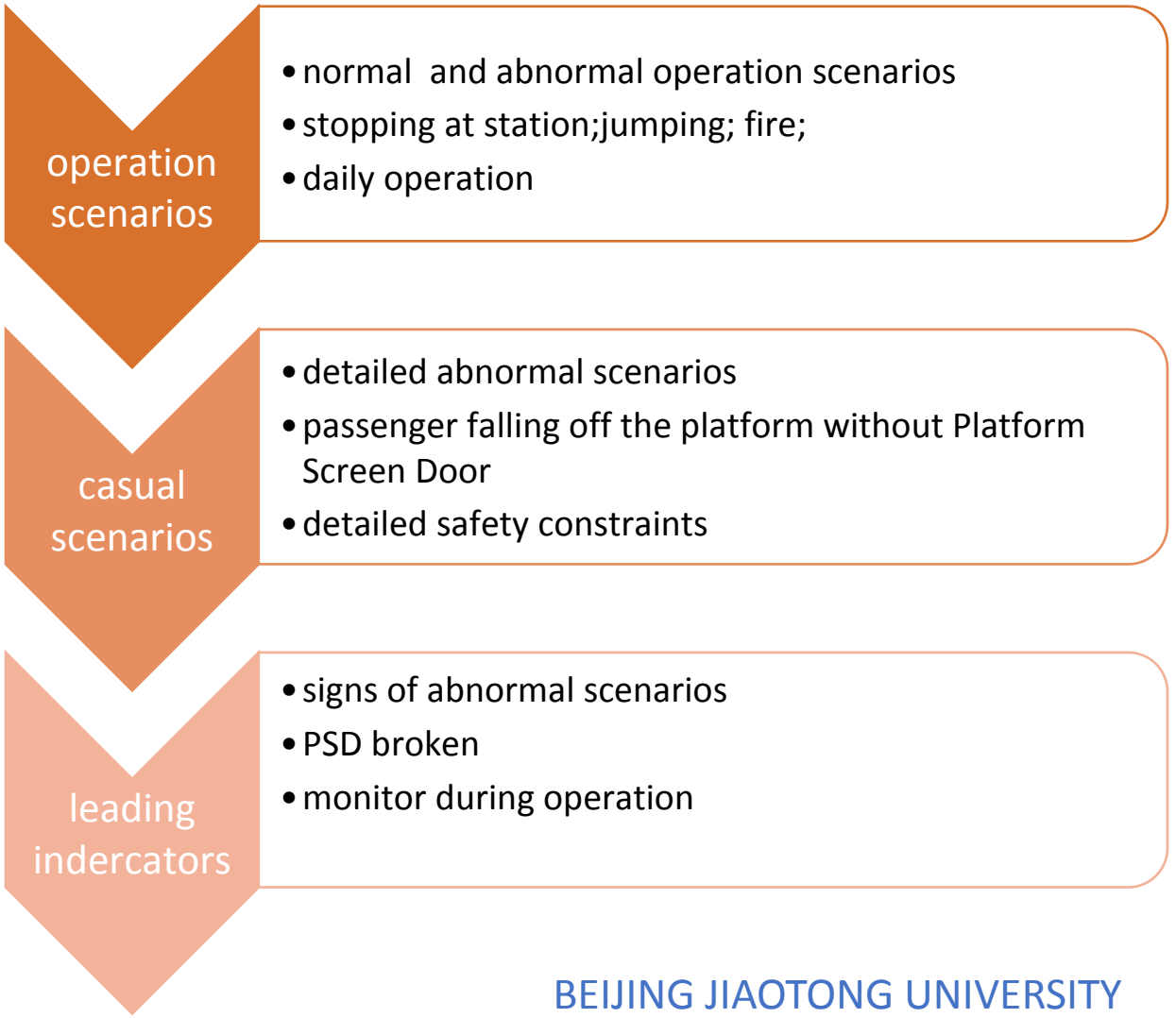


- same euipment
- different conntrol structure
- different function
- new hazards

STPA

INTRODUCTION

- How to find risks?
  - ✓ STPA
- How to monitor risks?
  - ✓ Leading indicator



LEADING INDICATOR IN METRO OPERATION

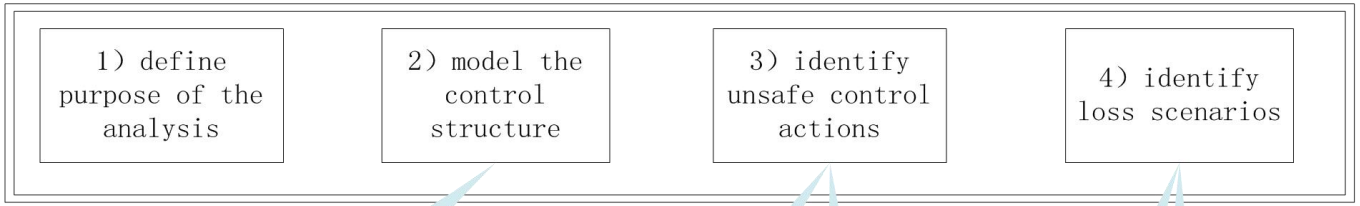
- Sources of leading indicators in urban rail transit operation:
  - two levels: train operation process, and daily management

(part of) leading indicators for metro operation

	Leading indicators in operation (L1)	**Leading indicators in management (L2)**
Machine	in abnormal working state; error beyond allowable range;	wearness; maintenance record;
Personnel	absence without leave; donzing and chatting;	examination result; error records;
Environment	bad weather; temperature and humidity, etc. passenger flow, etc.	construction around the line or machine; application of new technologies;
Organization and management	senior management of emergency treatment absence without leave;	no safety inspection plan; lack of personnel; lack of training and learning;

LEADING INDICATOR IN METRO OPERATION

Steps for inditifying leading indicators:



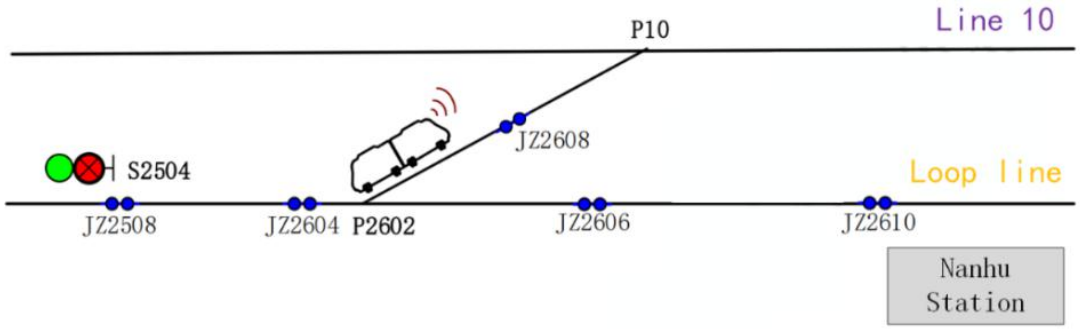
Determine the object and user of the indicators

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

APPLICATION IN CROSS-LINE SCENARIO

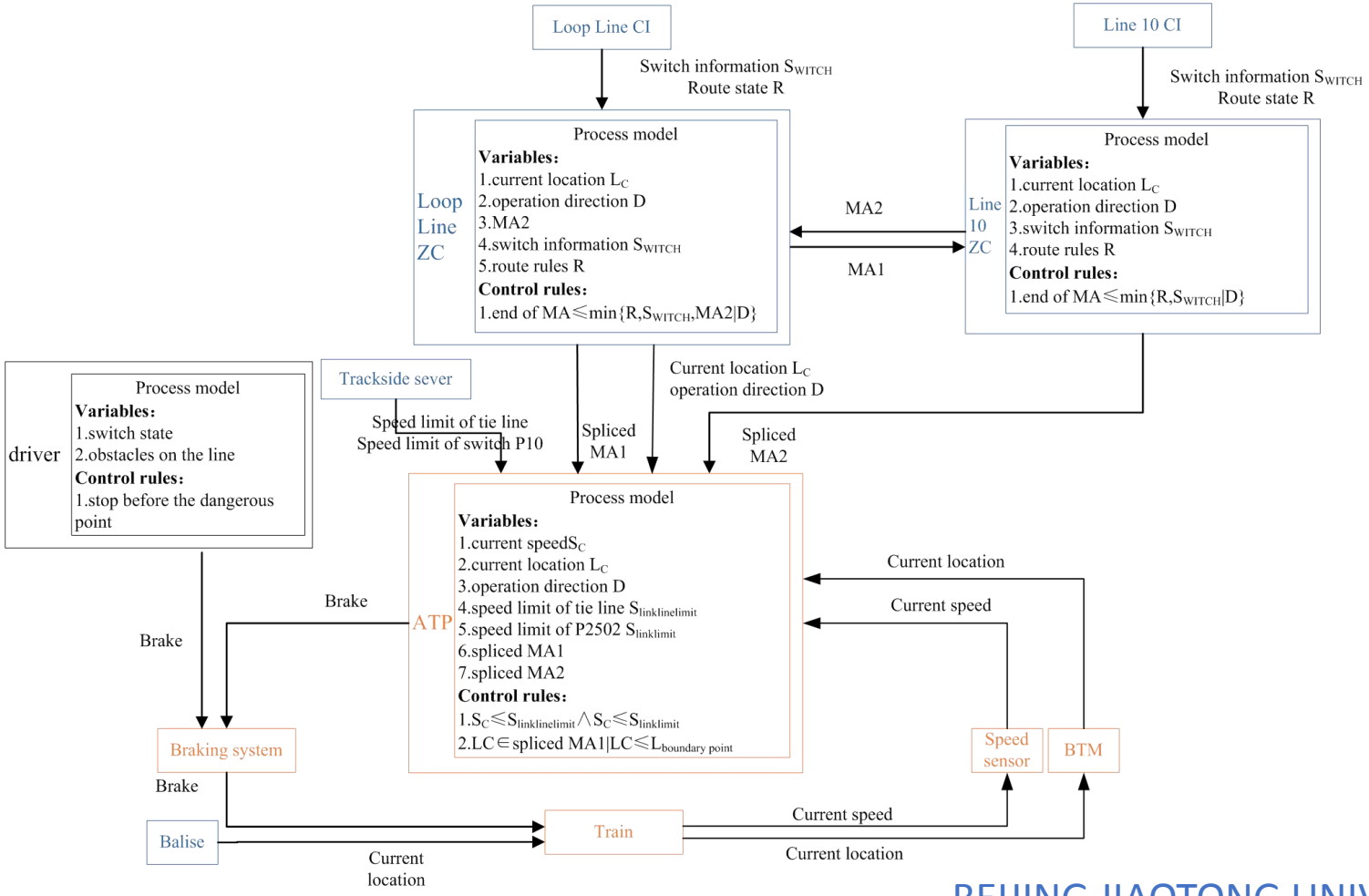
STPA Step 1: System level accidents and hazards

No.	Accident
A1	The train derails
A2	The train squeezes at switch
A3	The train hits obstacles that violated the limit
A4	The train hits personnel

No.	Hazard
H1	The train exceeds speed limit on tie line
H2	The train exceeds speed limit of switch P2602
H3	The train exceeds speed limit of switch P10

APPLICATION IN CROSS-LINE SCENARIO

STPA Step 2: Control structure



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
  - Driver
  - Dispatchers
- **users of leading indicators:**
  - Driver
  - Dispatchers

APPLICATION IN CROSS-LINE SCENARIO

STPA Step 3: Unsafe Control Action

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

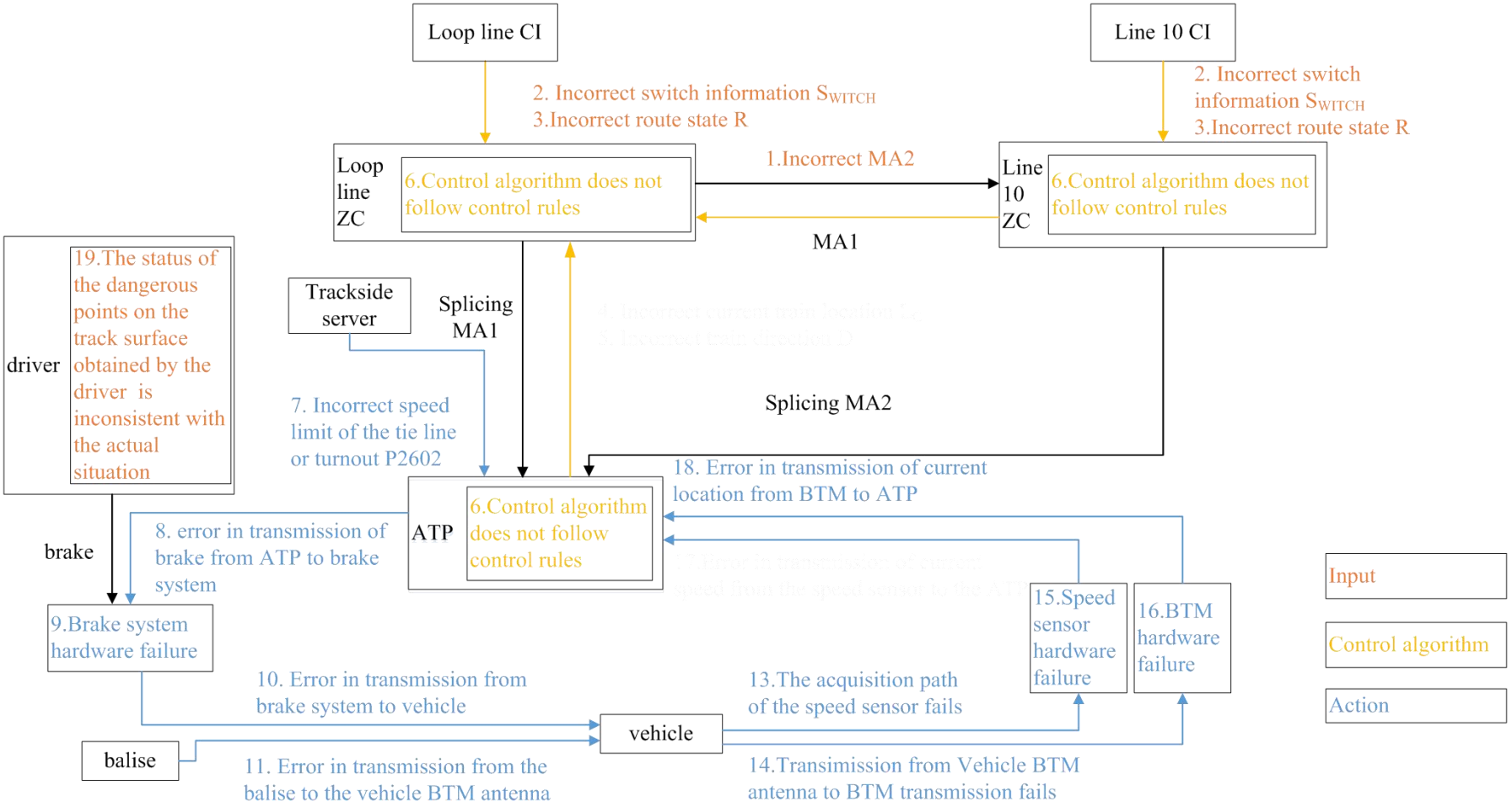
APPLICATION IN CROSS-LINE SCENARIO

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

UCA	Ldading Indicator
UCA1	LI01: Improper selection of ZC (L2)
	LI02: ZC once calculated MA wrong (L2)

APPLICATION IN CROSS-LINE SCENARIO

STPA Step 4: causal scenarios



APPLICATION IN CROSS-LINE SCENARIO

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

	No	Description
Causal Scenario	**S01**	**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.**
Safety Constraint	SC01	The Loop line ZC should use the newly received MA2 for the calculation of spliced MA1.
	SC02	The communication cycle between the Loop Line ZC and Line 10 ZC should be no more than Xs.
Causal Scenario	**S02**	**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.**
Safety Constraint	SC03	The loop line ZC should use the latest MA1 for the calculation of splicing MA1.

APPLICATION IN CROSS-LINE SCENARIO

Leading indicator Step 3: (part of) safety assumption

System level accident	Control action	Not providing	Providing
A1: The train derailed ...	Spliced MA1		UCA1: MA1 sent to ATP by Loop line ZC includes dangerous point

?

- Safety assumption

usually implied in the requirements analysis and design phases, basic conditions for the normal operation of the system

APPLICATION IN CROSS-LINE SCENARIO

Leading indicator Step 3: (part of) safety assumption

Causal Scenario	Safety Assumption
S01	SA01: Spliced MA under the worst condition including communication cycle, communication delay and so on is sufficient to ensure safety
	SA02: When the train does not receive MA within the specified time, braking will be implemented
	SA03: When the status of the route changes, ZC will immediately update the MA
	SA04: When the MA calculated by ZC changes, it will immediately send a new MA to ATP and overwrite the previous MA.

APPLICATION IN CROSS-LINE SCENARIO

Leading indicator Step 4: (part of) leading indicator

Causal Scenario	Safety Constraint and Safety Assumption	Leading Indicator
S01	SC01	LI03: Improper selection of Loop Line ZC (L2)
	SC02	LI04: The communication delay between Loop Line ZC and CI is too large (L1) ✓
	SA01	LI05: Construction in the line or surrounding (L2)
	SA02	LI06: Improper selection of ATP (L2)
		LI07: The brake system calls for maintenance more frequently (L2)
		LI08: The service life of the braking system is too long (L2)
		LI09: The vehicle made an abnormal noise (L1) ✓
		LI10: Alarm by braking system (L1) ✓
	SA02/03/04	LI11: Improper selection of braking system (L2)

supplier qualification
cost reduction. etc

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

- futrue work

how much does it help

how to use the indicators

北京交通大學

BEIJING JIAOTONG UNIVERSITY

Thank you!