# Train Control Uncertainty Treatment and Safety Assurance: Shifting from Manual Driving to Fully Automation

FEI YAN, Chunhai Gao, Ru Niu, Tao Tang

Beijing Jiaotong University

IRSE INSTITUTION OF RAILWAY SIGNAL ENGINEERS

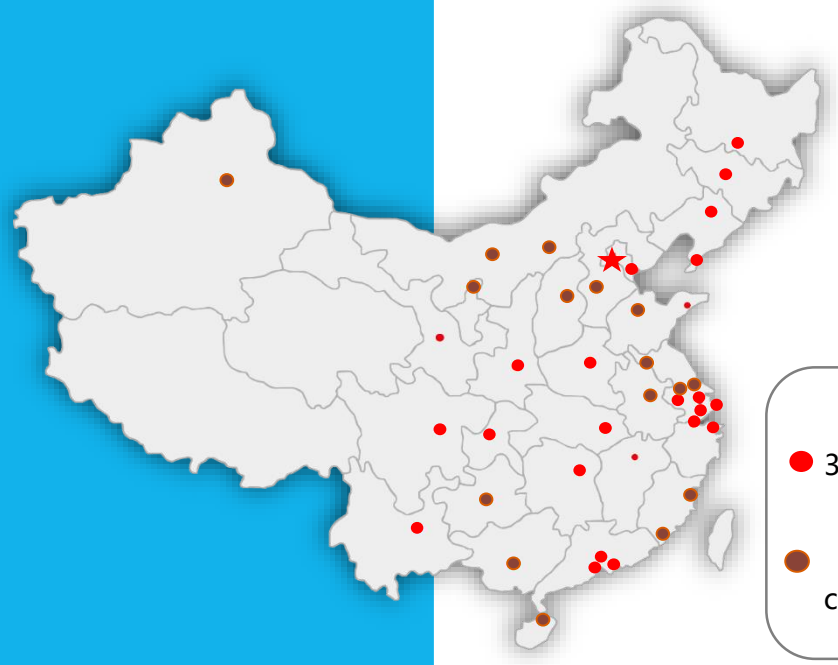
ASPECT2019

北京交通大學 BEIJING JIAOTONG UNIVERSITY

# Contents

# Urban Transit Development In China

- 150 urban transit lines are operating in 39 cities by 2018.
- The total Metro length is 3031 KM long and by 2020, another 3000 KM transit will be built.



Legend

- 39 cities have their own metro
- More than 30 cities are building the metro

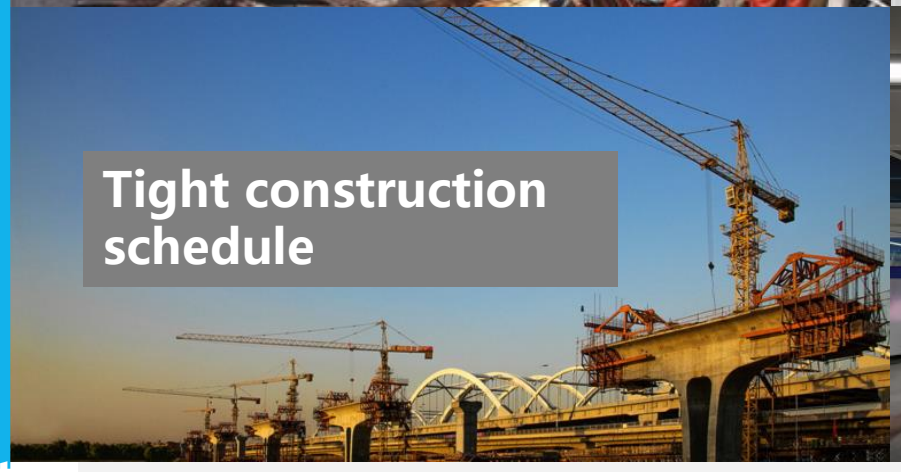
# Industrial background

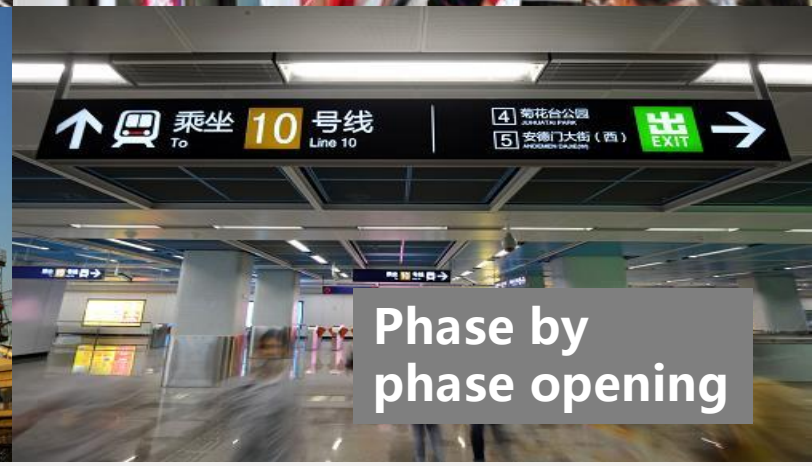
- Chinese urban rail witnessed rapid development since 1990s. New emerging requirements posed big challenges to signaling system

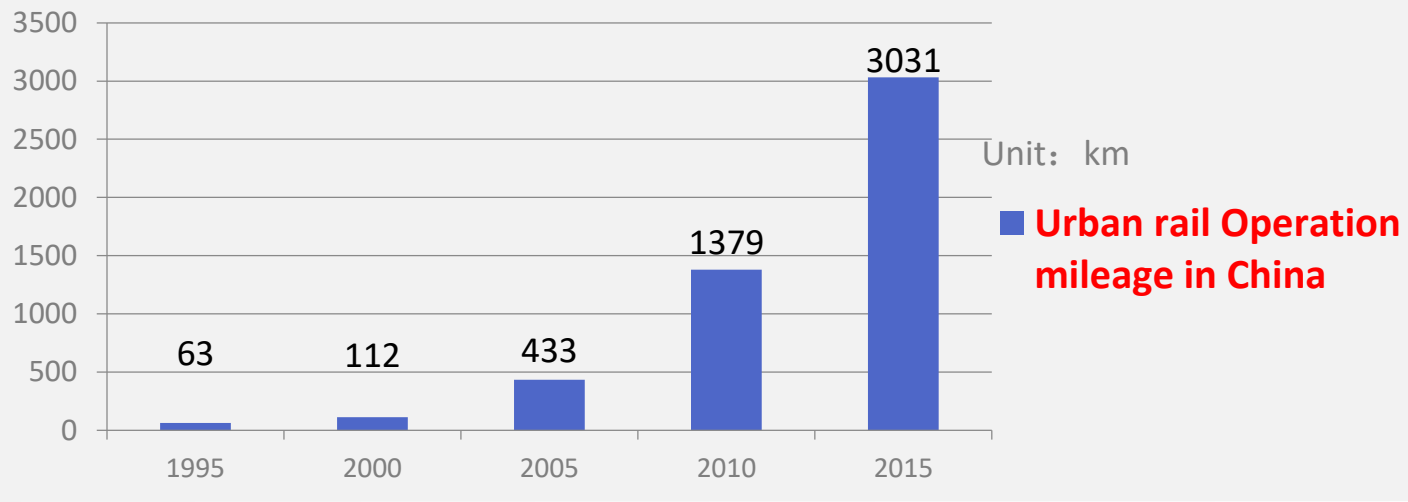
Overseas signaling suppliers cant meet the changing requirements with slow response

» Localized and self-relied signaling system NEEDED





# Establishment of TCT

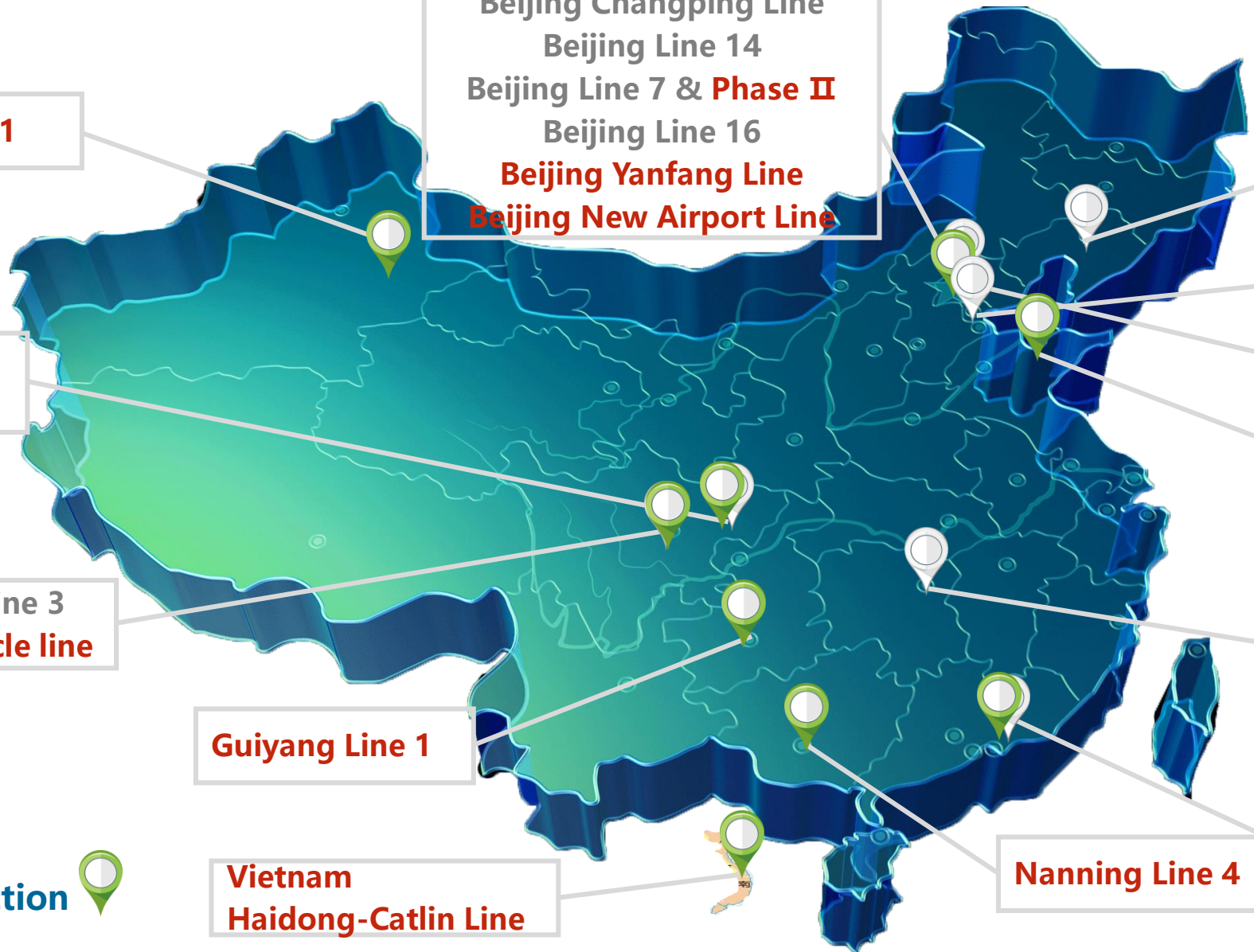
In 2002, according to the need and trend of industry, BJTU started the R&D of CBTC.

- **Beijing Jiaotong University**
- **National Key Lab of Rail Traffic Control & Safety**
- **National Engineering Research Center of Rail Traffic Control**

In 2009, TCT was established through technology transfer to promote the product engineering application & operation.

TCT
交控科技
Traffic Control Technology

# The CBTC Projects covered 24 Metro Lines, approximately 500 miles in 13 major cities (now 13 Metro Lines already in service)



Beijing Yizhuang Line
Beijing Changping Line
Beijing Line 14
Beijing Line 7 & Phase Ⅱ
Beijing Line 16
Beijing Yanfang Line
Beijing New Airport Line

Urumqi Line 1

Dalian Line 3
Dalian Line 202

Tianjin Line 6

Shijiazhuang Line 3

Qingdao Line 13

Chengdu Line 3
Chengdu Line 5

Chongqing Line 3
Chongqing Circle line

Changsha Line 1

Guiyang Line 1

Shenzhen Line 7
Shenzhen BYD Cloud line
Shenzhen Line 10

Nanning Line 4

Vietnam
Haidong-Catlin Line

In operation

Under construction

# Historical overview of AUGT system

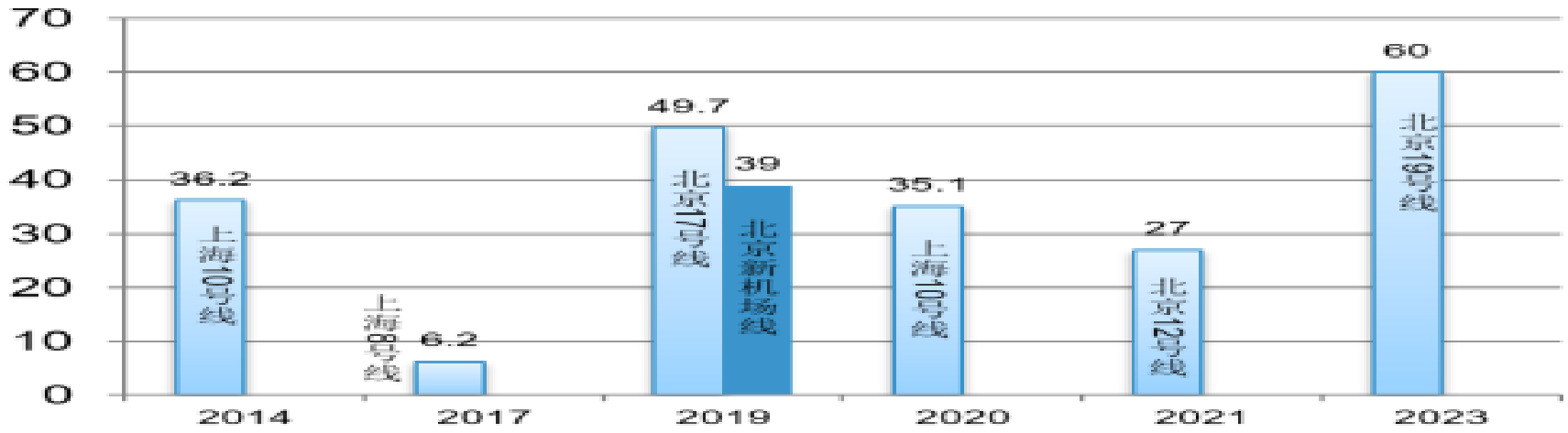
- 60s :
- development of ATO, prototypes
- 70s :
- implementation of ATOs
- Small-sized UTO systems
- 80s
- fully UTO « metros »
- 90s
- deployment of « proven » UTO metros of higher capacity
- 2000s
- continuity : Rennes, Copenhagen, Torino
- upgrading of conventional lines into UTO
- 2010s
- AUGT system has been applied for mass transit system, like Paris Line 1 , Shanghai Line 10, etc.

# Background



## Development opportunity of fully automatic operation


The fully automatic operation technique is developed in due course in order to solve the existing problems, and nowadays, our country has developed multiple urban planning applications. Yanfang Line is the first fully automatic operation system developed by our country independently



# Background

Compared with the existing rail transit system, the fully automatic operation is significantly improved in aspects of passenger transport, maintenance, repair and driving control, therefore, high availability, high reliability and high safety are achieved.

The burden of drivers can be relieved due to the fully automatic operation



Dedicated service posts are set for helping the passengers in all aspects

The system faults can be positioned automatically to achieve preventative maintenance



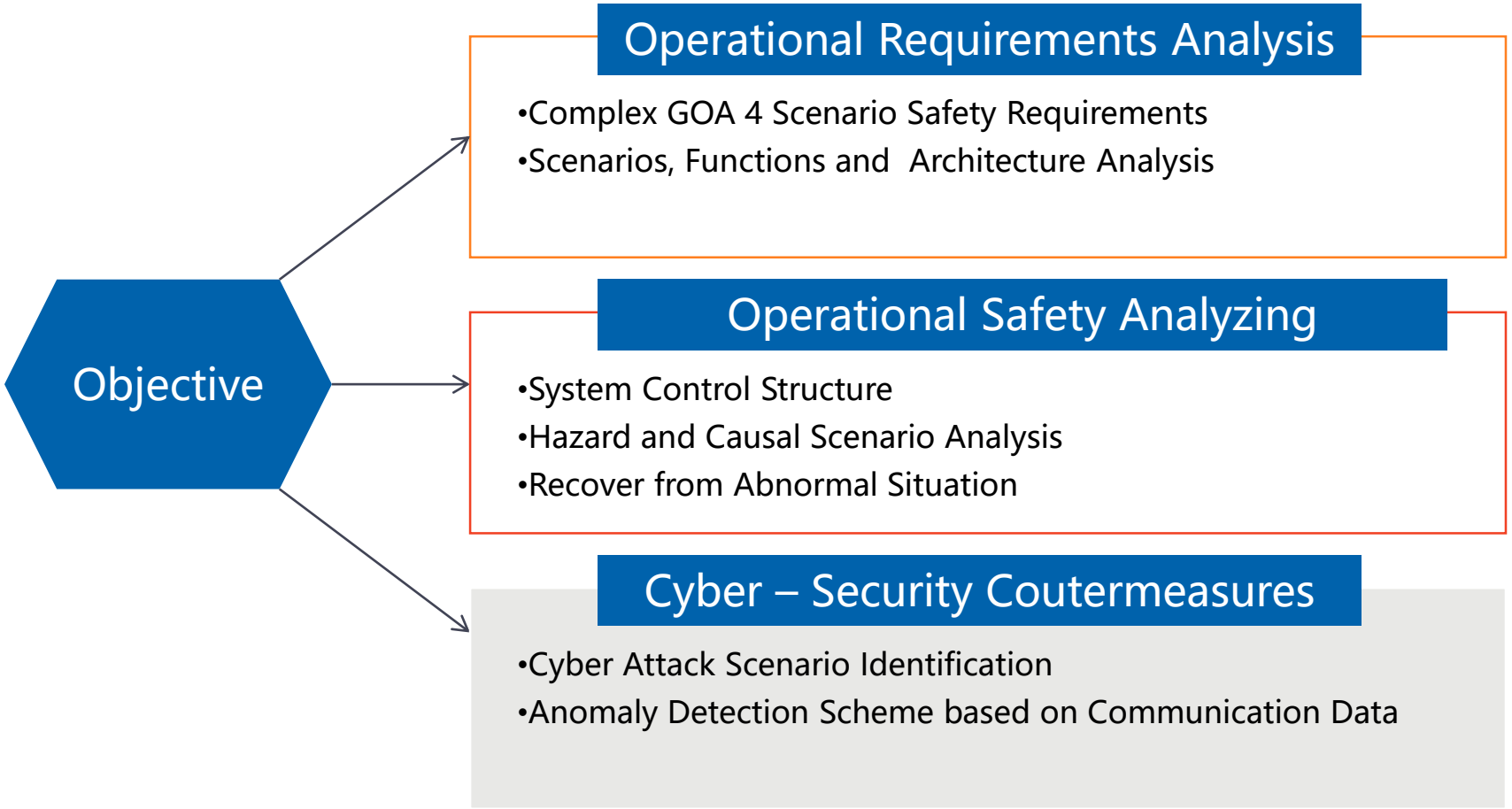
Human caused errors can be reduced, and real-time accurate monitoring can be achieved

# Background

The biggest problem has been found in the phase of integration testing is the mismatching between newly defined functions for driverless operation and traditional CBTC system, especially in abnormal or rarely used emergency scenarios. To solve this problem, ordinary operational scenarios are analyzed with a new systematic safety analysis method, like STPA.

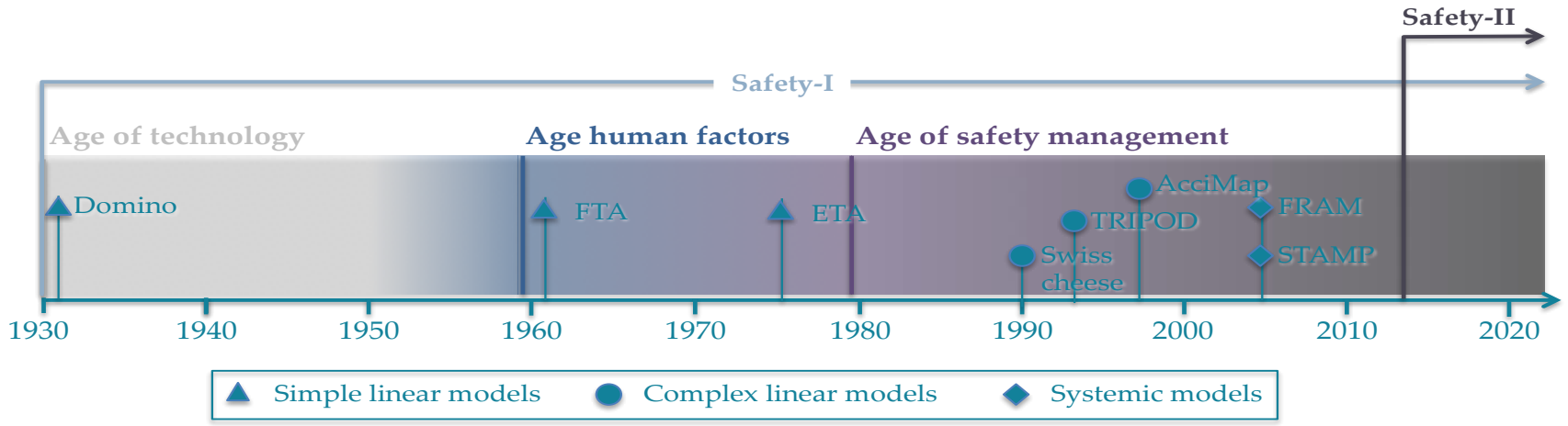
STPA outputs-causal scenarios can be used to capture safety requirements and help system designers to deep understand safety requirements. Abnormal operational scenarios can be also identified from causal scenarios, which can be used to improve emergency response ability by system design and is meaningful for the safe operation of Yanfang Line.

# Background



# Contents

# Methodology




Traditional approaches are designed for electrical and mechanical systems. It's hard to deal with highly complex systems with complex structure and interactions, such as fully automatic operation CBTC systems. Therefore, a newly safety analysis method is badly needed to identify the causes of dysfunctional system interactions and abnormal operation sceneries

# Methodology

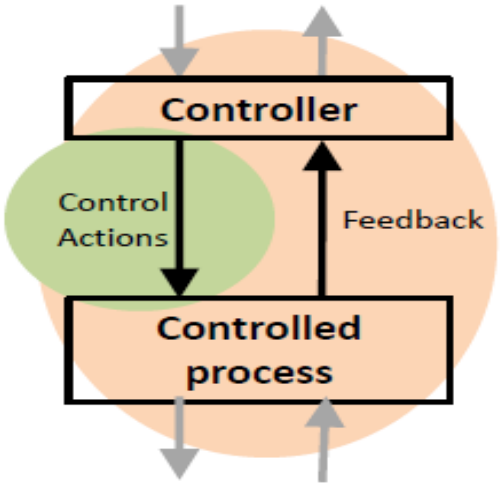
STPA

## STPA
## (System-Theoretic Process Analysis)

**STPA Hazard Analysis**

**STAMP Model**

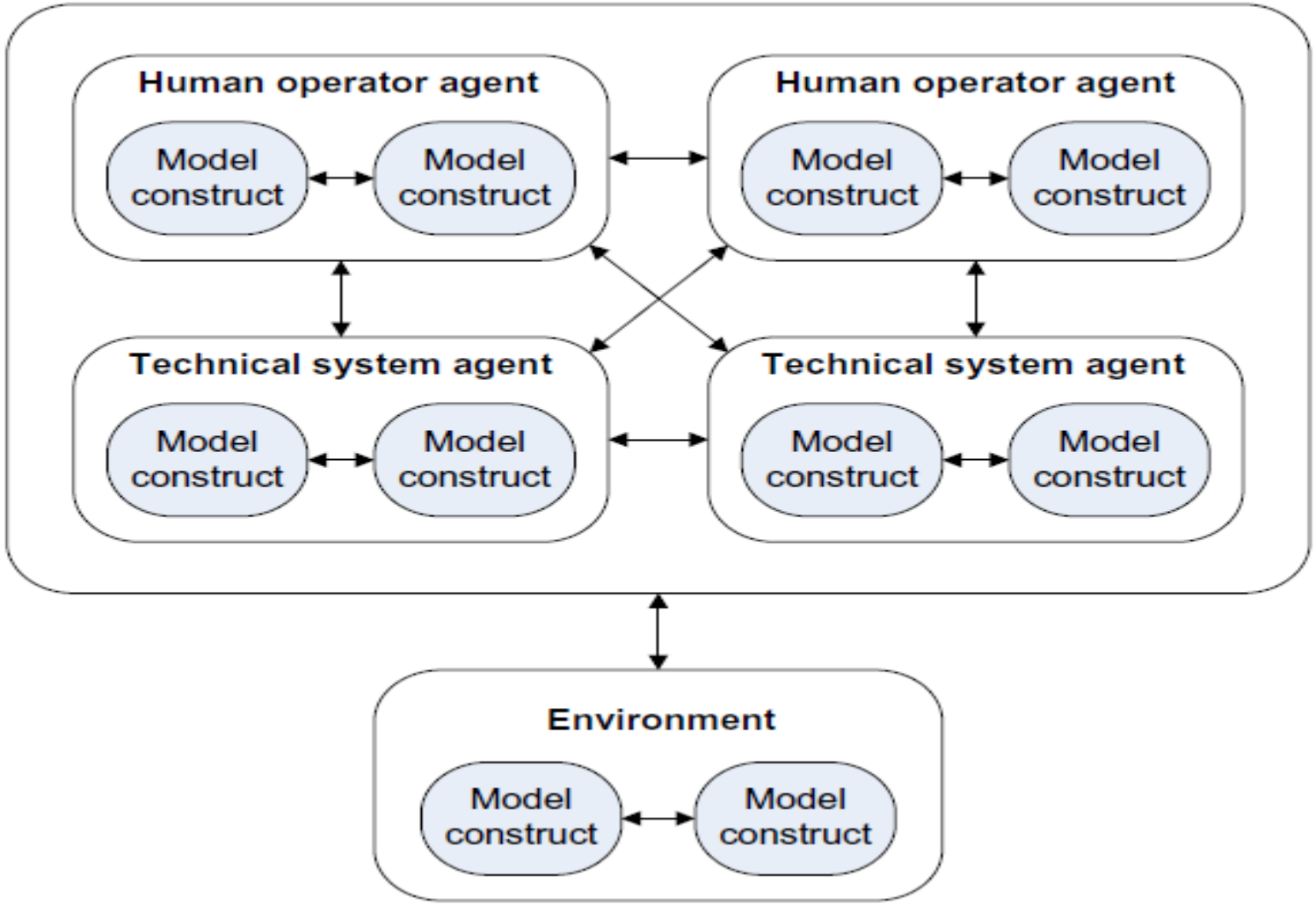
- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and create scenarios




**Can capture requirements flaws, software errors, human errors**

# Methodology

Agent-based modeling and mental simulation



# Contents

# Application



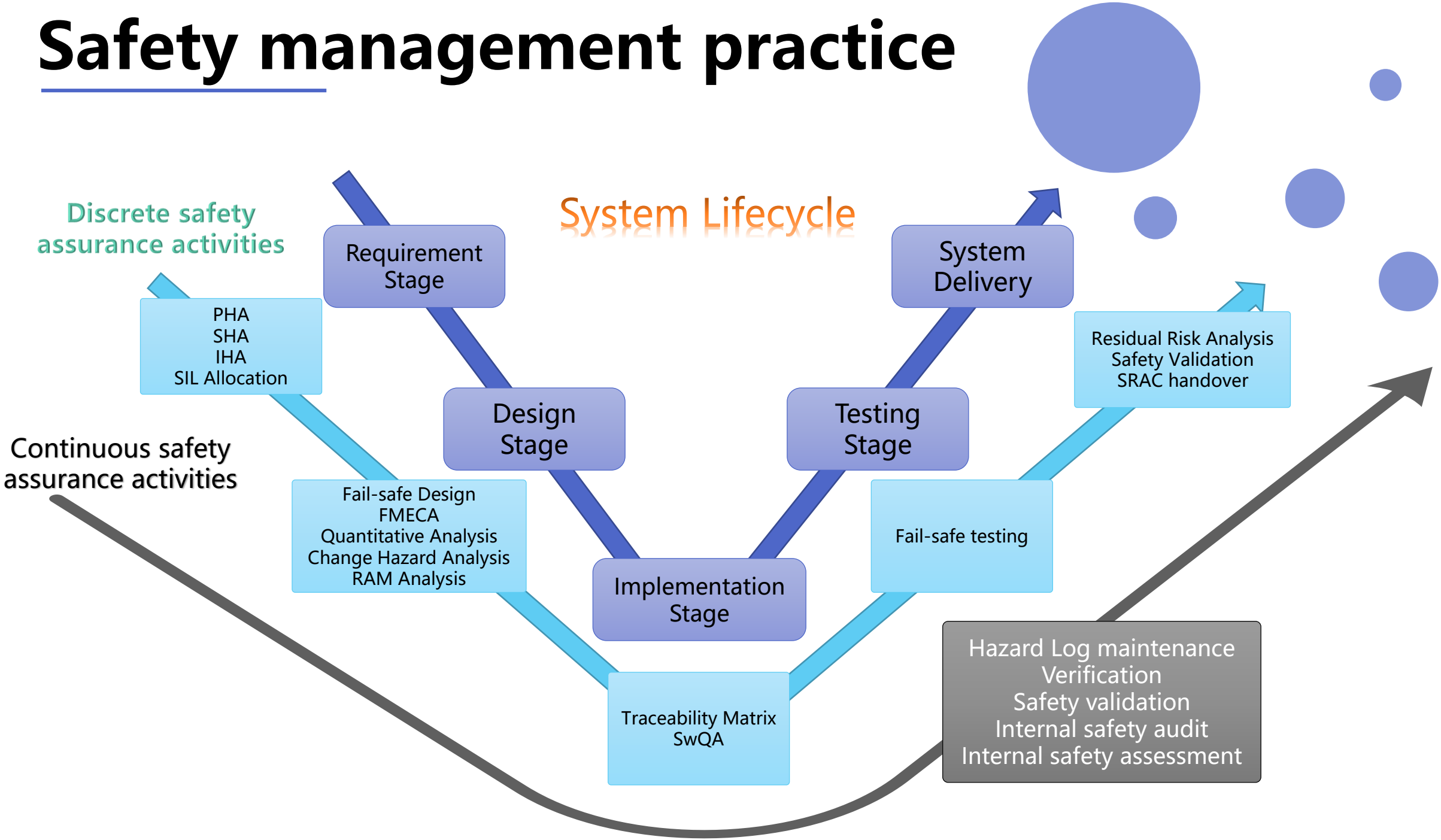
Central TIAS equipment

Train-ground communication equipment

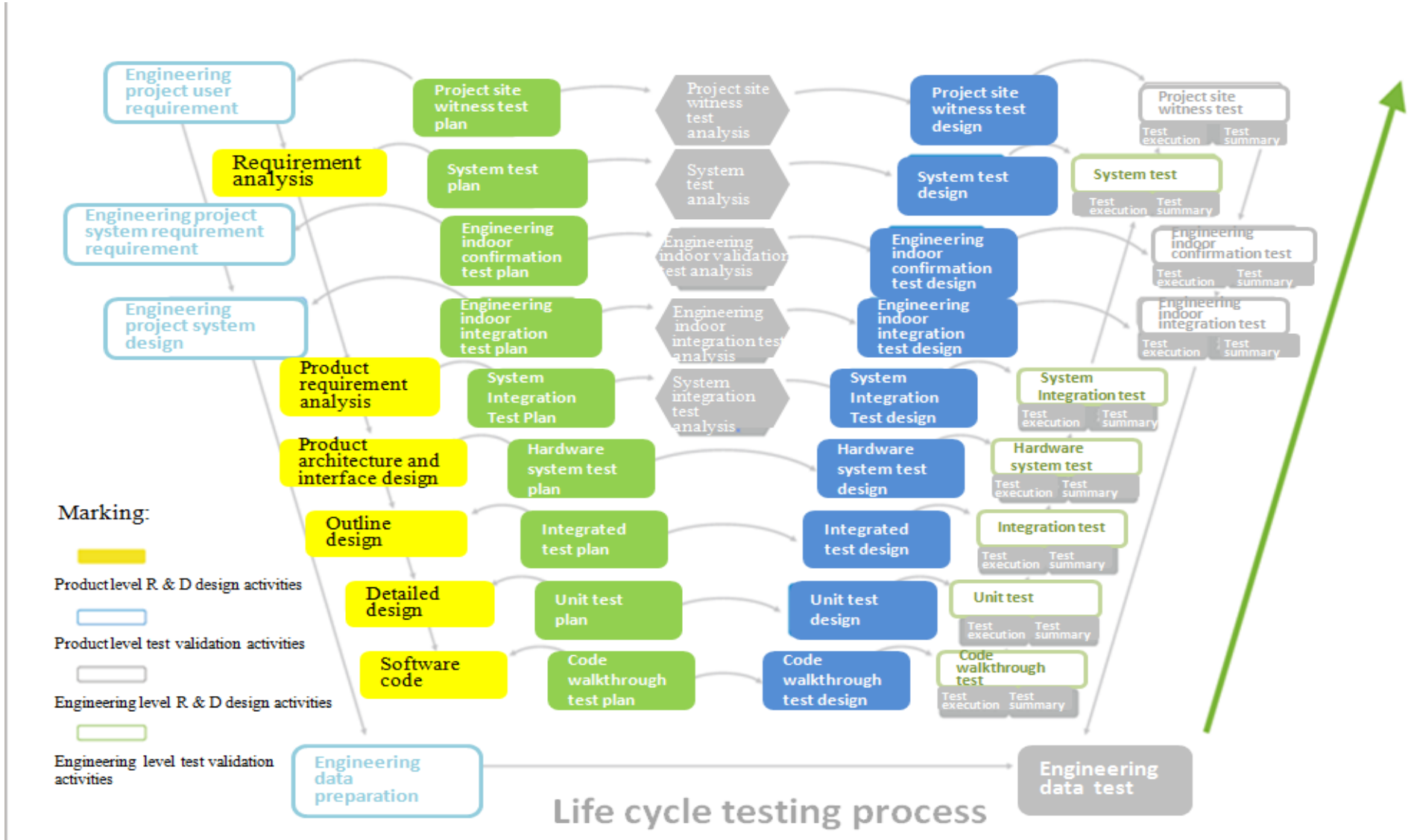
Station interlocking machine

On-board controller

# Safety management practice



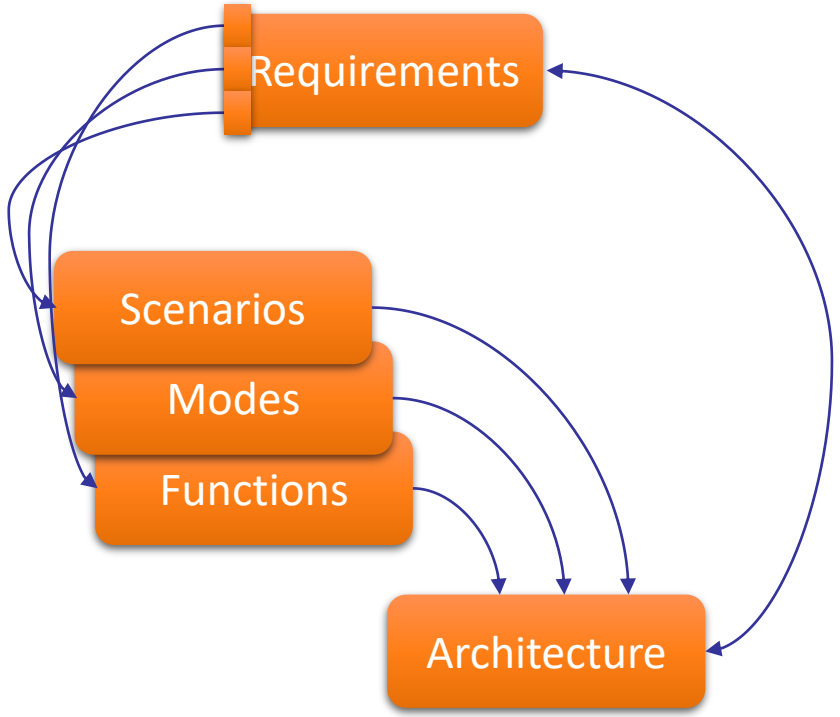
# Requirements of the life cycle test process



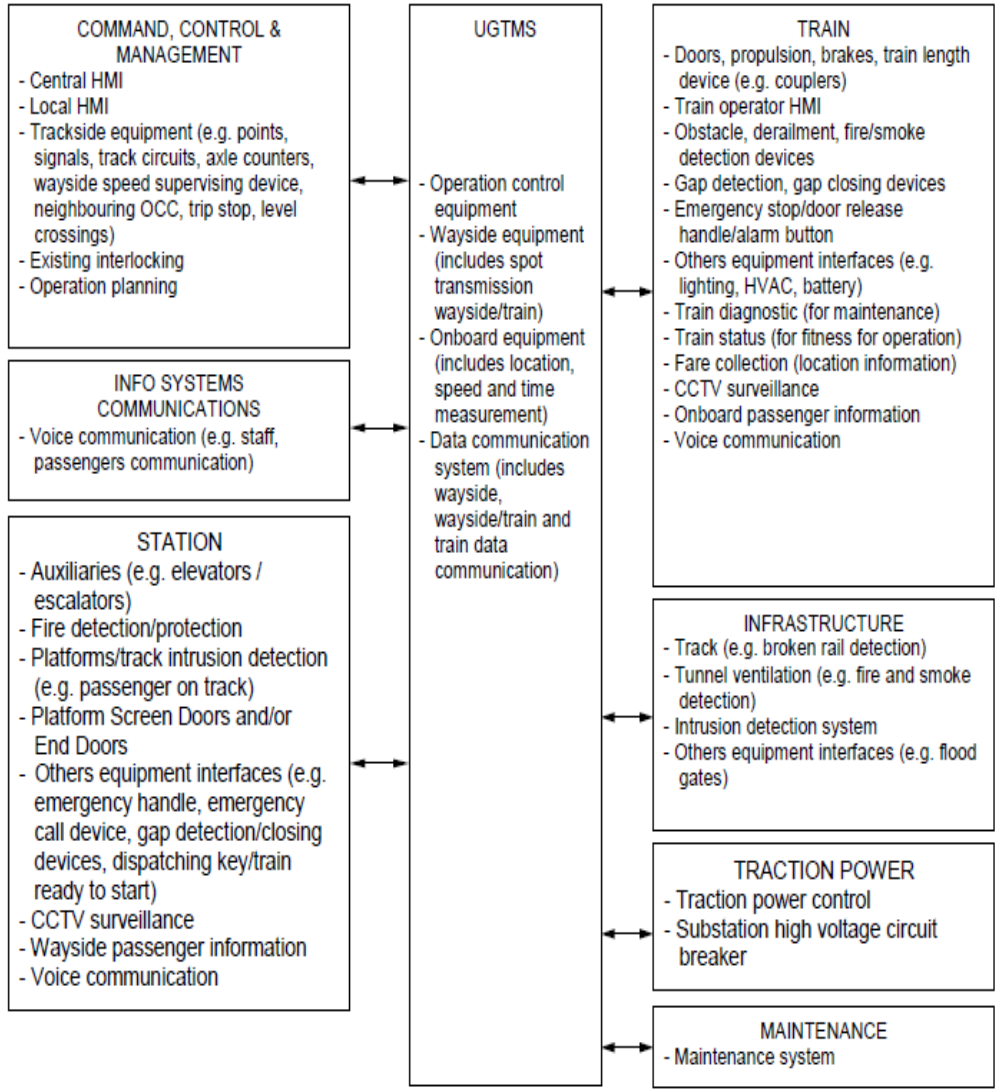
# Grades of automation ( IEC62267/62290 )

| Grade of Automation | Type of train operation | Setting train in motion | Stopping train | Door closure | Operation in event of Disruption |
|---|---|---|---|---|---|
| GoA 1  | ATP with driver | Driver | Driver | Driver | Driver |
| GoA 2  | ATP and ATO with driver | Automatic | Automatic | Driver | Driver |
| GoA 3  | Driverless | Automatic | Automatic | Train attendant | Train attendant |
| GoA 4  | Driverless, unattended | Automatic | Automatic | Automatic | Automatic |

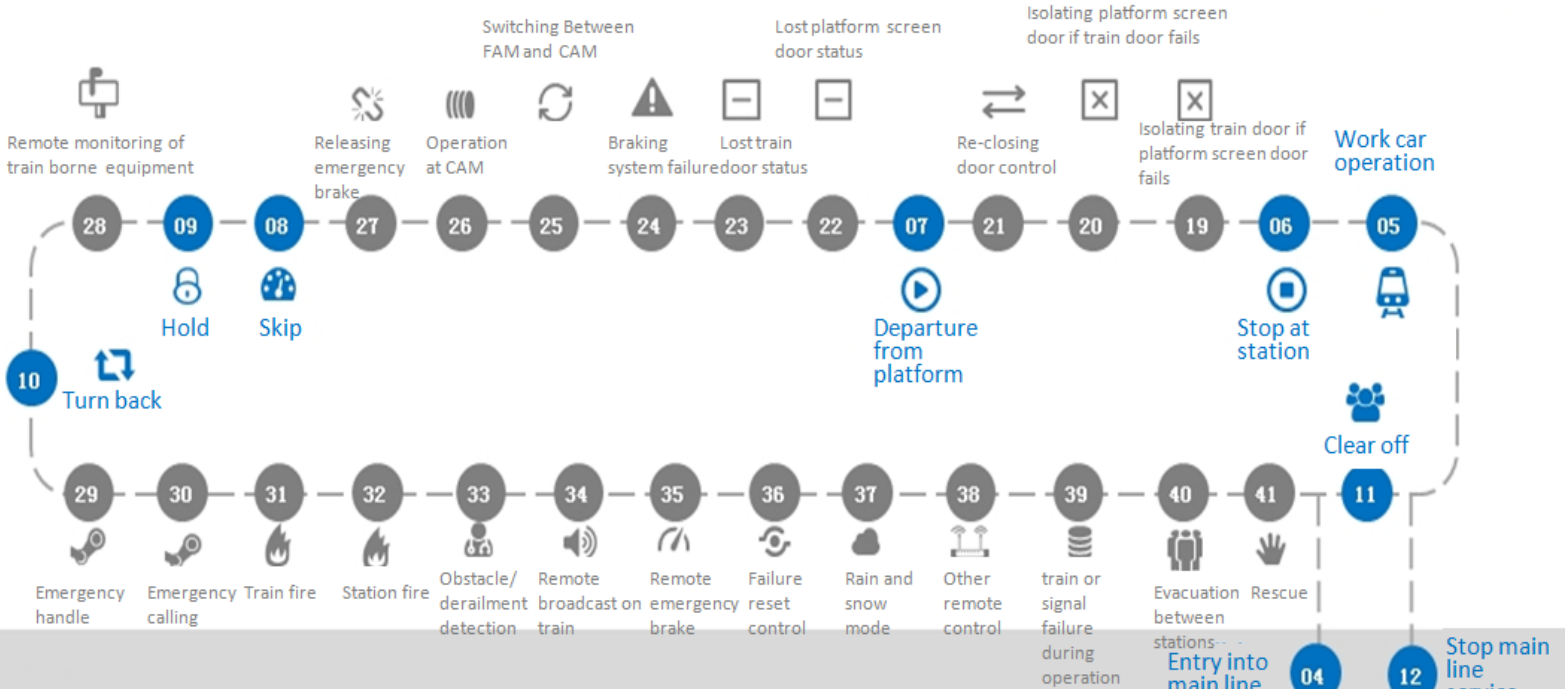
# Application




Requirements according to UGTMS



# Beijing Yanfang Line - Normal Operation Scenario Aspect




Pose the scenarios and operating rules as the main line

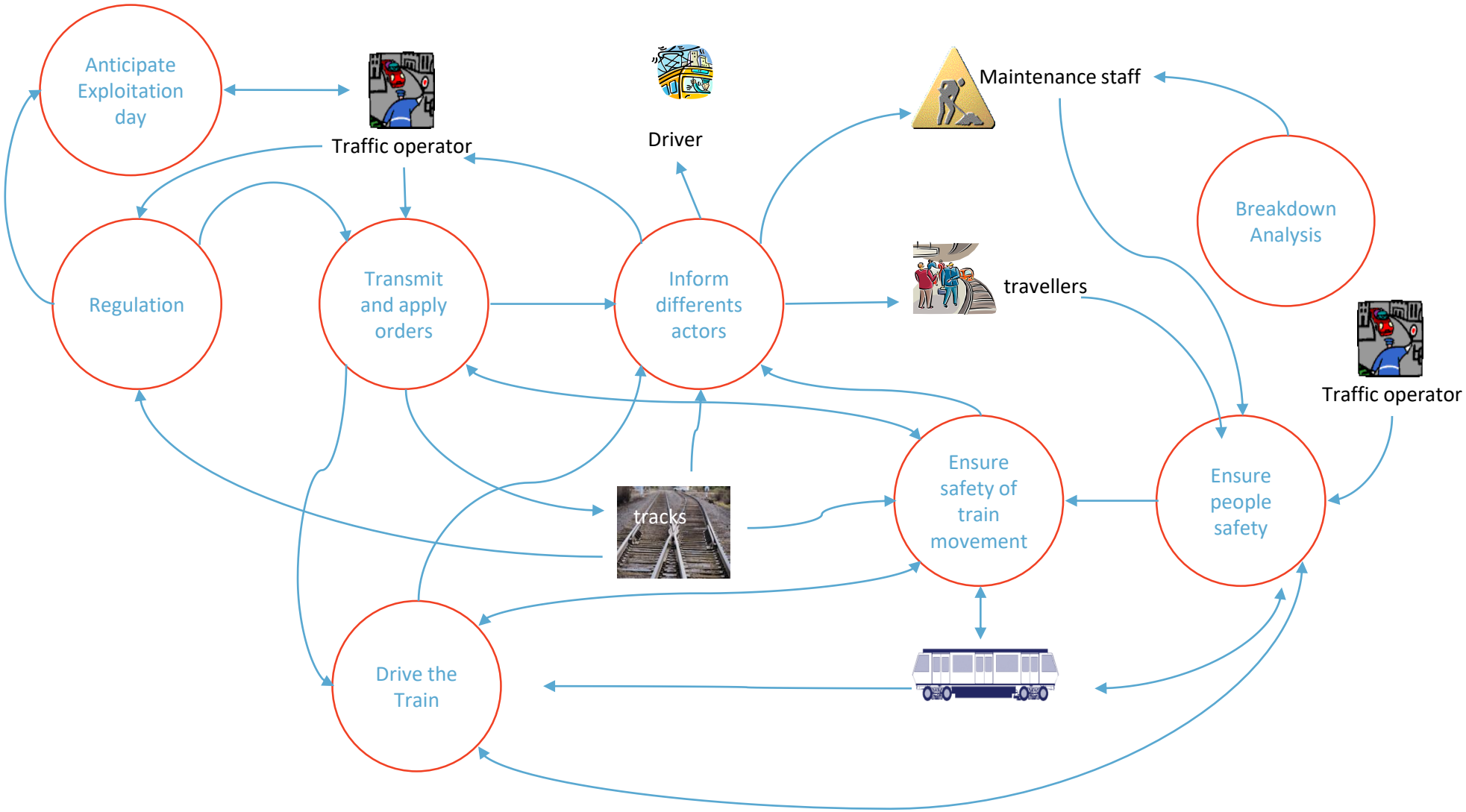
There are 41 scenarios

**Normal Scenarios: 18**

**Fault or Abnormal Scenarios: 23**

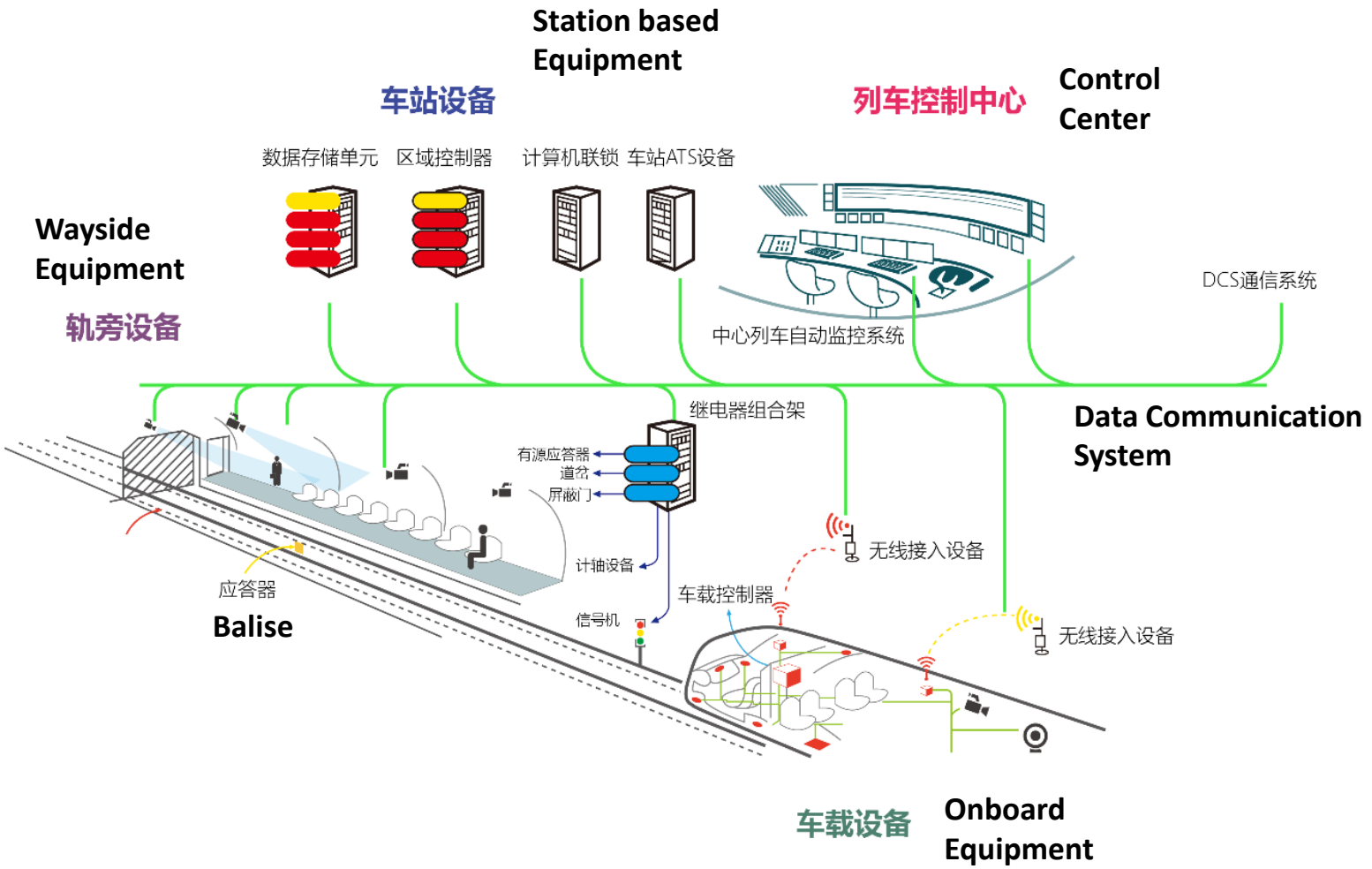
# Application

## Functional Interaction from Operation View



# Application

## Physical Architecture



# Train Operational Scenarios


无线接入设备 无线接入设备

无线接入设备 无线接入设备

计算机联锁 车站ATS设备

**车站设备**

数据存储单元 区域控制器


**车载设备**

**车站设备**

数据存储单元 区域控制器 计算机联锁 车站ATS设备

**列车控制中心**

**FAO Mode**

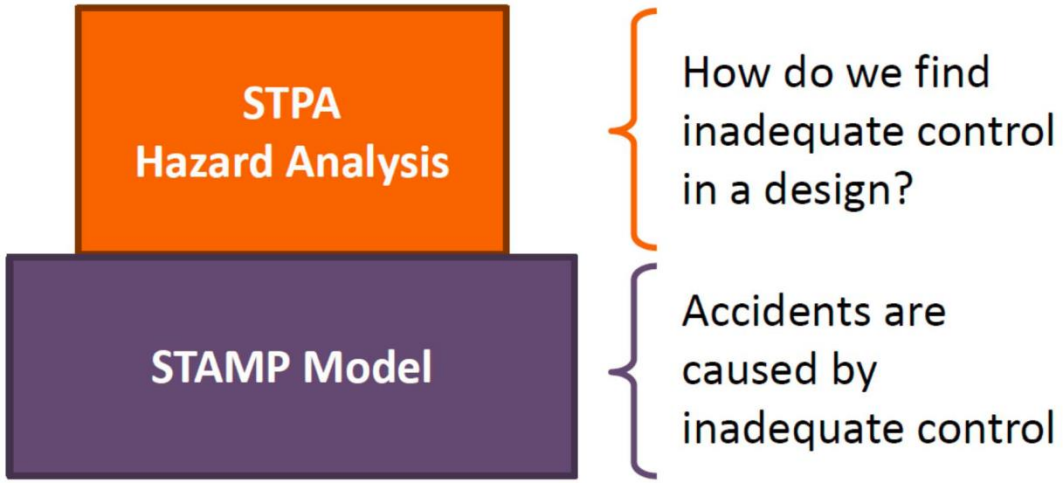
# STPA

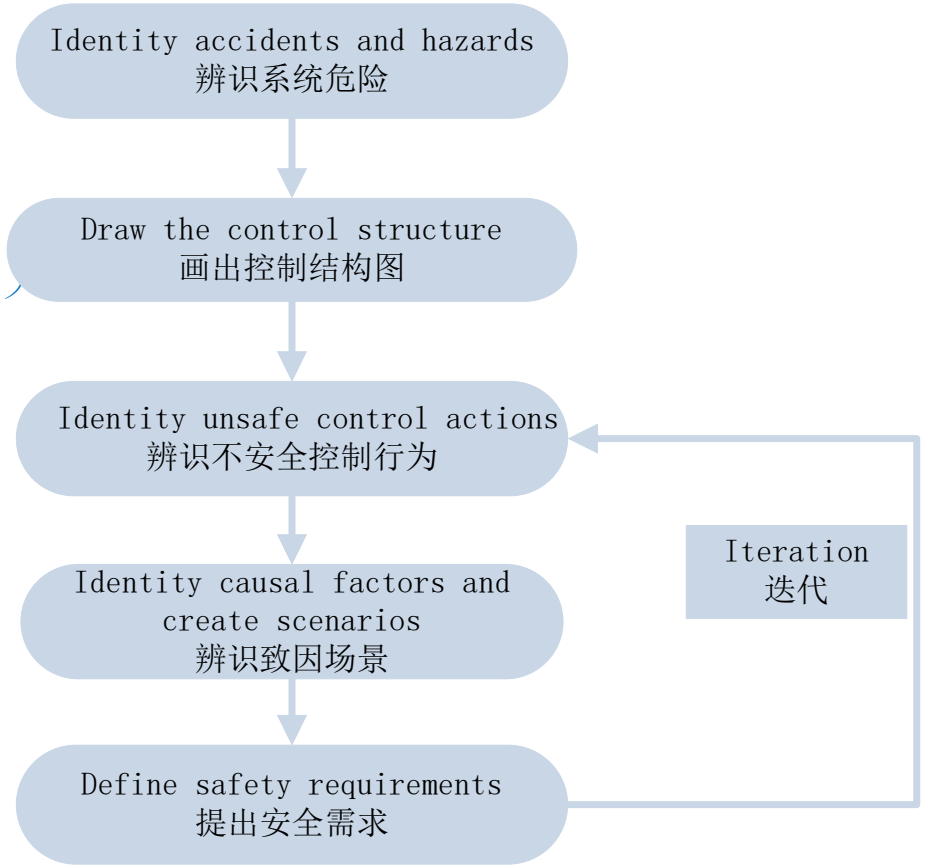
System theoretic process analysis – A hazard identification technique based on STAMP

Prof. Nancy Leveson

- *Accidents occur when interactions violate **safety constrains**.*
- *Goal is to control the behavior of the components and systems as a whole to ensure safety constraints are enforced in the operating system.*

*——System-Theoretic Accident Model and Process（STAMP）*



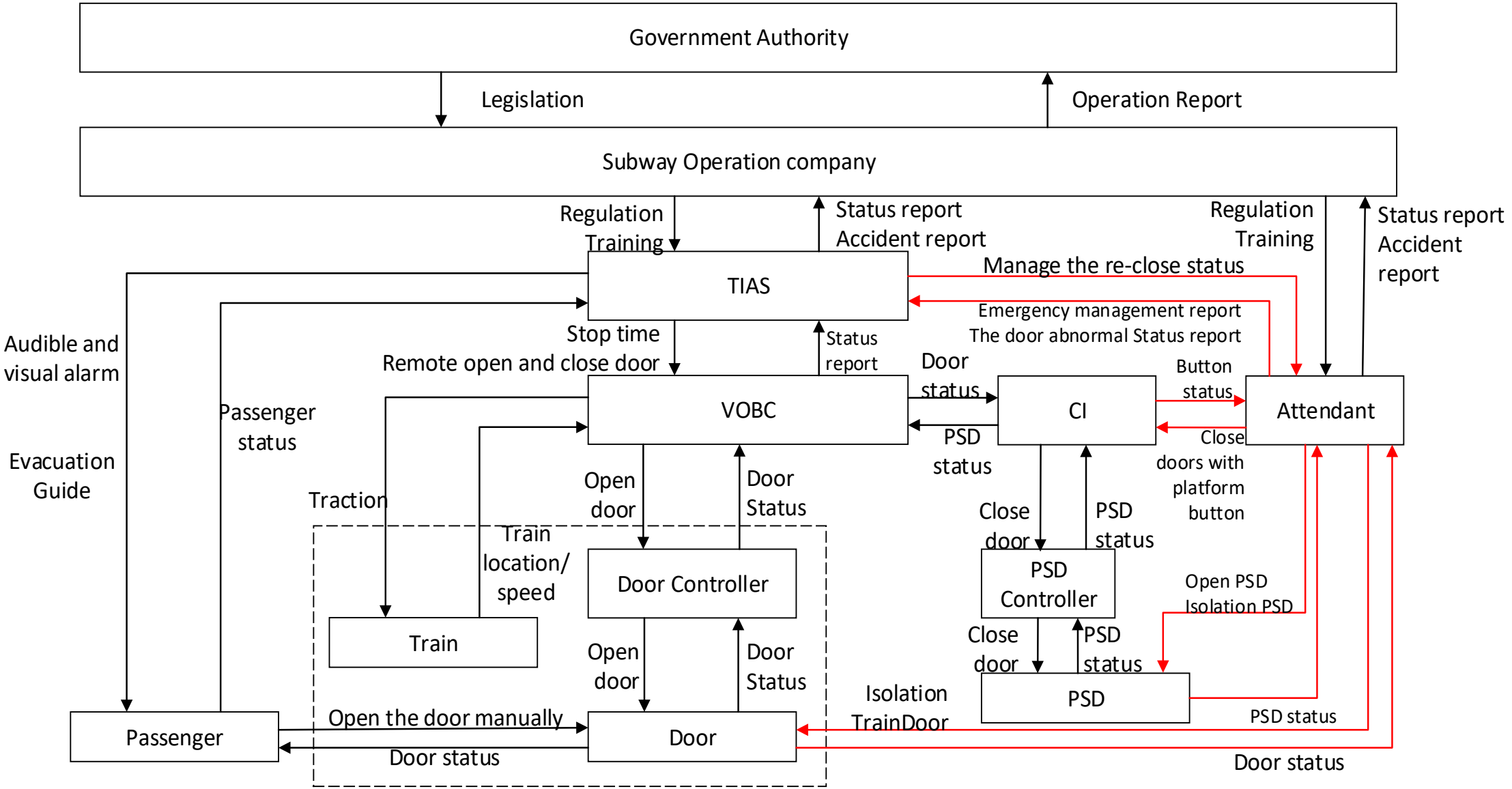

STPA

# Driverless CBTC Accidents and Hazards

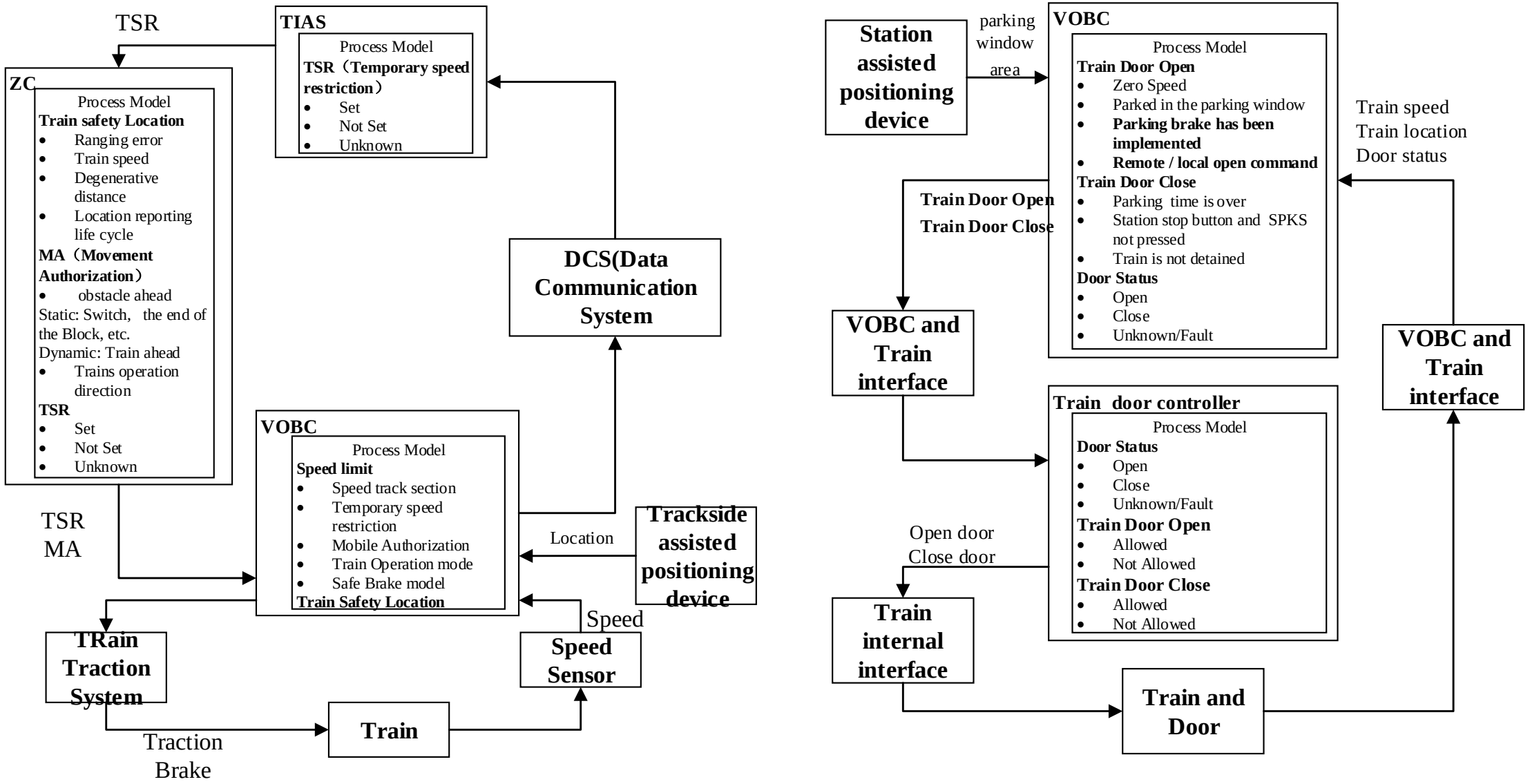
A1. Train and train collision
A2. Trains collide with obstacles within the track clearance (including passengers or operations staff)
A3. Train derailment
A4. Passenger injuries related to doors

H1. Train speeding [A1, A2, A3]
H2. Abnormal opening or closing the door [A4]

# System Control Structure



# Control Process Model

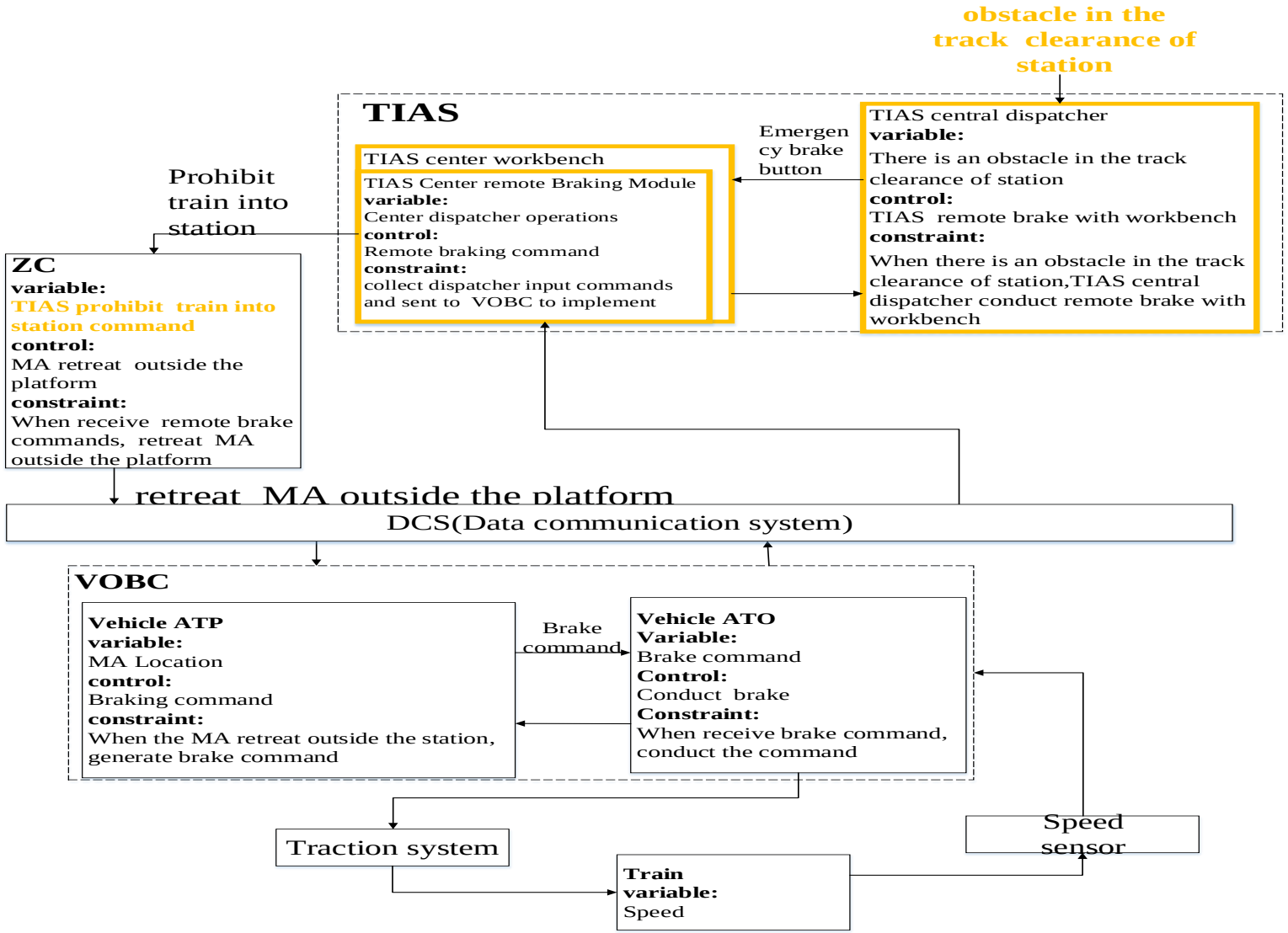


# Unsafe Control Actions

| Hazard | Control Action | Not Providing Caused Hazard | Providing Causes Hazard | Wrong Timing/Order Causes Hazard | Stopped Too Soon or Applied Too Long |
|---|---|---|---|---|---|
| **H1. Train speed control** | TIAS Remote brake（Train braking） | Uca1： When there is an obstacle in the station track gauge, not make the train parking outside the station | / | / | / |
| **H2. Keyless Entry** | VOBC Isolation door （The door does not open） | Uca2： When there is something wrong with the PSD (Platform Safety Door), not isolate the corresponding door. | / | / | / |

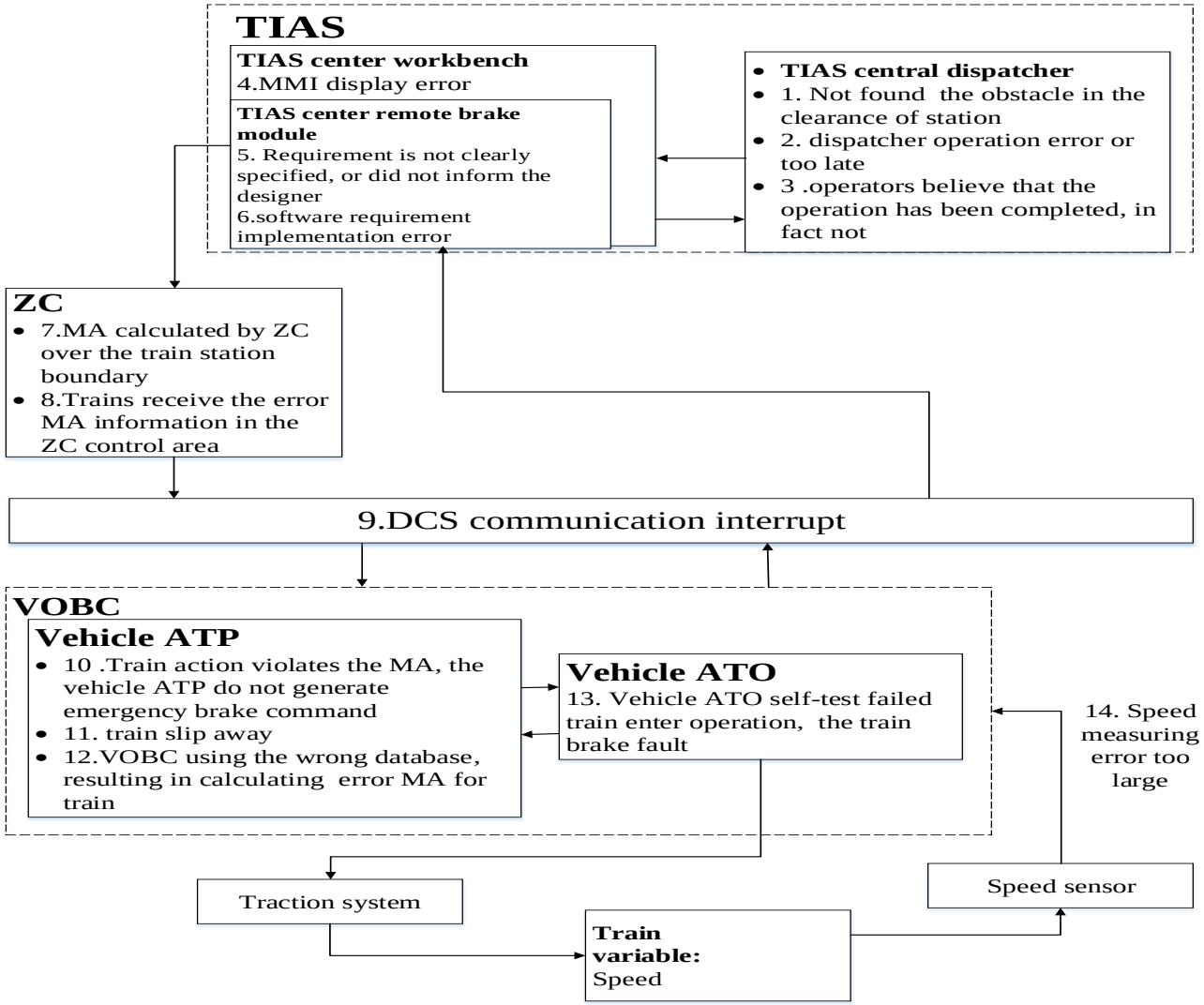
# Scenario based process model for UCA1

## When there is an obstacle in the station track gauge, not make the train parking outside the station



# Causal Factor for UCA1

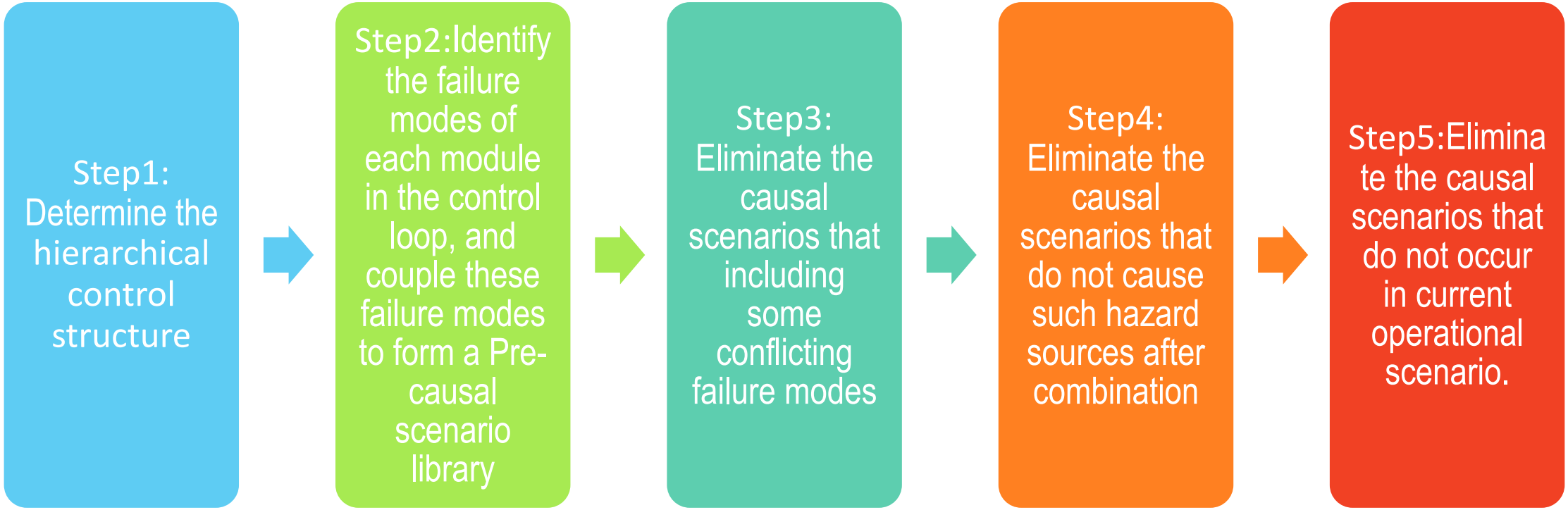
When there is an obstacle in the station track gauge, not make the train parking outside the station



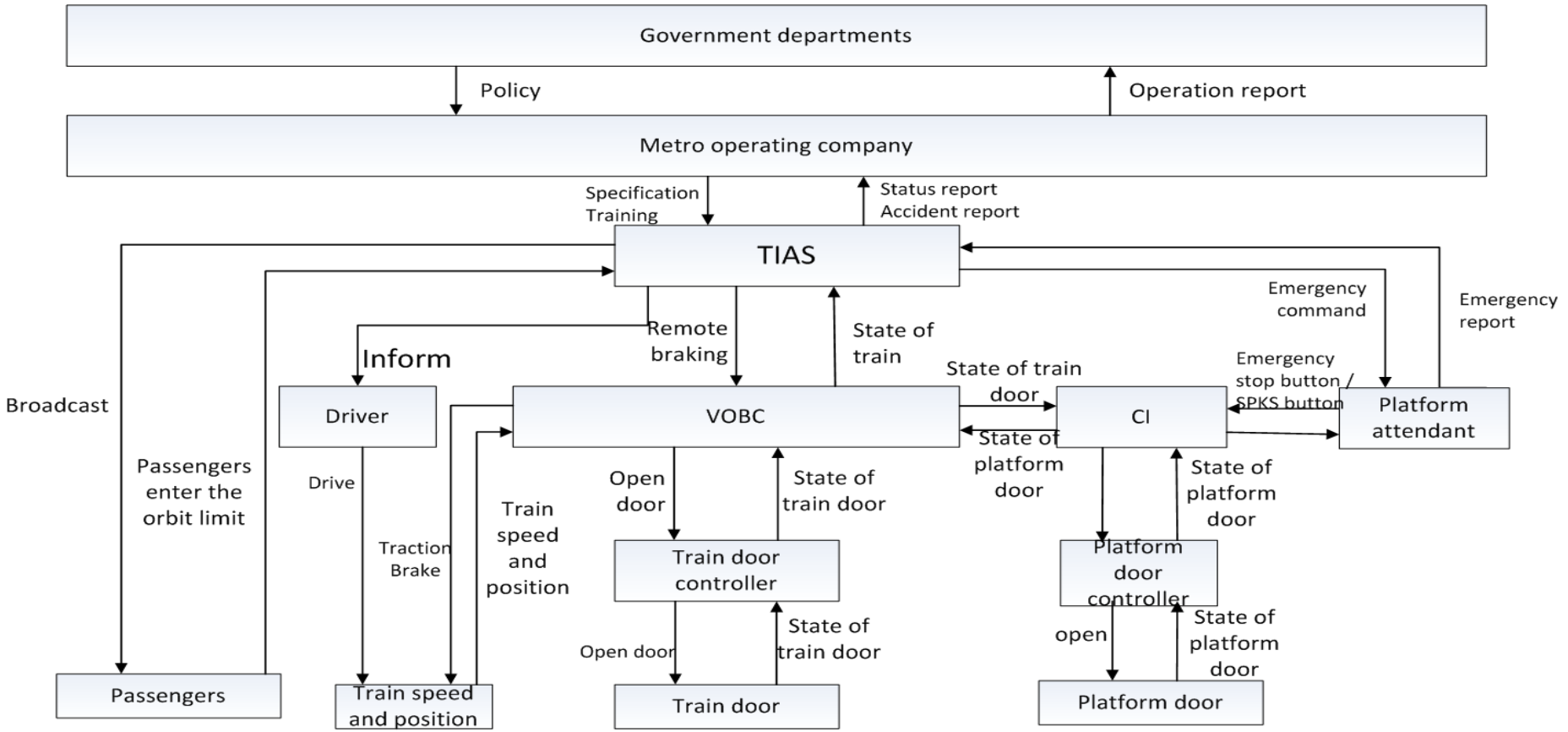
# Hazard List and Hazard Log of Uca1

| Hazard | Unsafety control action | Causal factor number | Causal factor | Safety constraint number | Safety constraint/requirement/mitigation | comment |
|---|---|---|---|---|---|---|
| **H1. Over speed when the train pulled into station** | Uca1: When there are obstructions in the station track clearance，TIAS center dispatcher don't via remote command to make the train stop outside the station. | H1-Uca1-CF1 | Not found obstructions within the station track clearance | H1-Uca1-SC1 | Developed for track clearance inspection requirements, including inspection time check period and inspection processes, etc. | |
| | | | | H1-Uca1-SC2 | Design and installation of wayside obstacle detection devices, such as additional CCTV platform to the station and close to the range of track gauge to monitor | |
| | | | | H1-Uca1-SC3 | Design and installation of automotive obstacle detection device: when the device come into contact with an obstacle, it can detect the obstacle in front of the train, if the obstacle is detected, the train should implement the emergency brake. | |

# The basic steps of the causal scenario search method



# Determine the hierarchical control structure



## Step2: Identify the failure modes of each module in the control loop, and couple these failure modes to form a Pre-causal scenario library

Gated protection includes a speed measuring module, positioning module, VOBC computing fusion speed module, VOBC computing safety position module, VOBC issuing open door software implementation module, VOBC issuing departure command software implementation module, door state detection module, TCMS processing door closing Command module, TCMS transmission information module, etc. 22 kinds of fault modes can be found, and 4,194,304 kinds of pre-causal scenarios can be obtained by using simple combination algorithm

# Step3: Eliminate the causal scenarios that including some conflicting failure modes

A software module can be used to reduce the pre-causal scenarios by eliminating scenario combinations, by checking that a condition is incorrect and that a condition cannot occur simultaneously.

# Step4: Eliminate the causal scenarios that do not cause hazard after combination

It can be divided into two sub-steps:

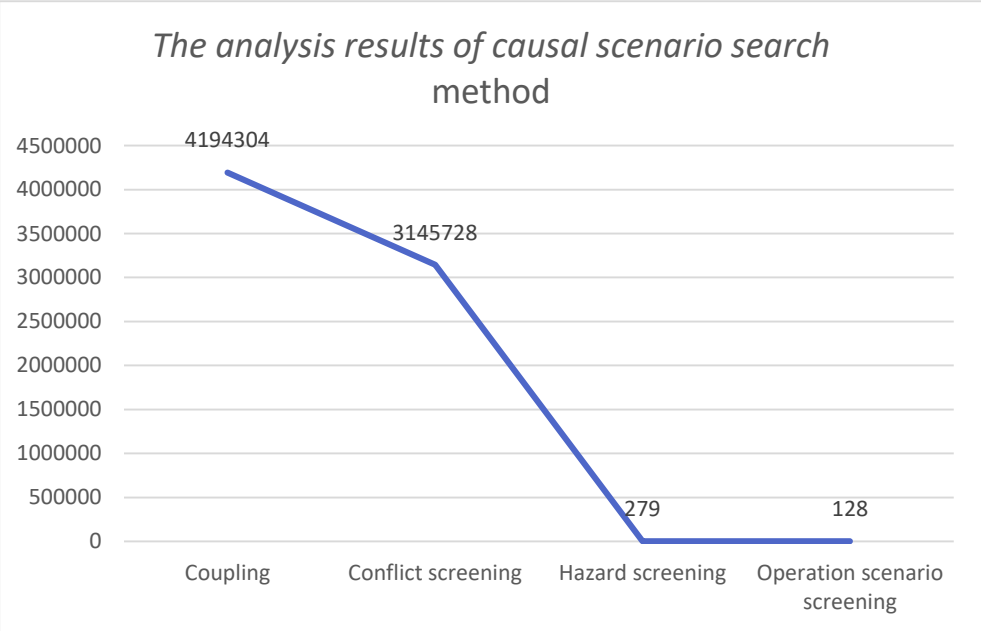
1) Find the minimum coupling factor. Some modules have a single failure mode that can be dangerous, so all cause scenarios that are coupled to it can be eliminated. Similarly, the occurrence of two or more failure modes can be dangerous, eliminating all cause scenarios for higher level coupling.

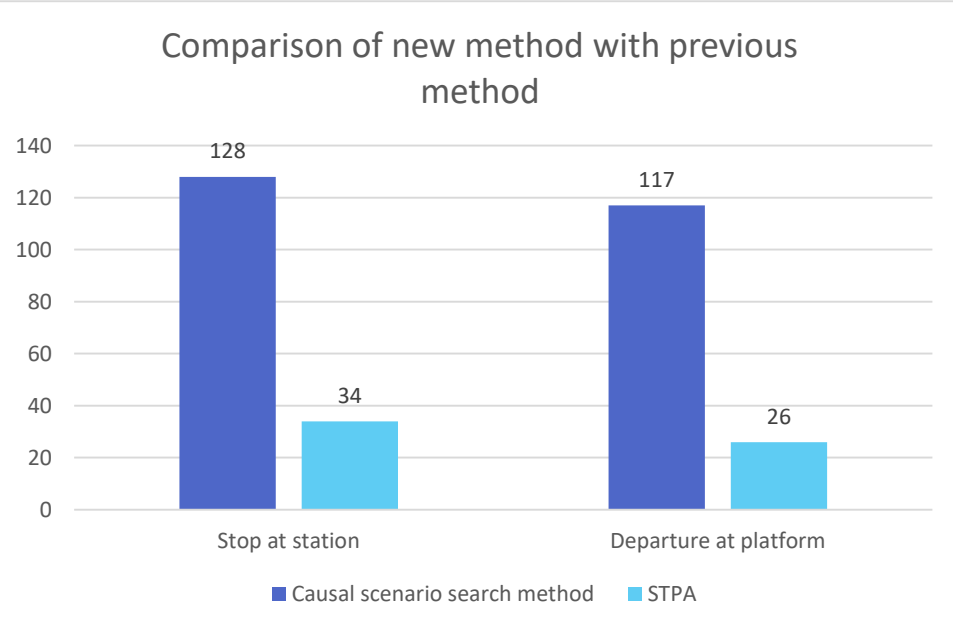
2) Set multiple variables for each UCA and failure mode. For example, UCA3: When the train moves, the door opens. Train status: moving or zero speed stop; door status: open or closed or lost status. Emergency: Yes or No, etc. This step is to establish a correspondence between the UCA and the causal scenario.

# Step5: Eliminate the causal scenarios that do not occur in current operational scenario

First, safety protections should be extracted in the operational scenario. For example, in the “stop in the station” scenario, there is gate protection, and the “sleep” scenario does not require gate protection. However, even if there are door protection in different scenarios, the corresponding causal scenarios are different, such as emergency evacuation scenarios and normal inbound parking. The protection of the door during the outbound process and the protection of the doors at the platform need to be targeted to specific operations.

# Results


The analysis results of causal scenario search method
4500000
4000000
3500000
3000000
2500000
2000000
1500000
1000000
500000
0
4194304
3145728
279
128
Coupling
Conflict screening
Hazard screening
Operation scenario screening


Comparison of new method with previous method
140
120
100
80
60
40
20
0
128
34
117
26
Stop at station
Departure at platform
Causal scenario search method
STPA

# Contents

# Discussion

STPA - In order to capture more abnormal scenarios in the process of train movement, we present several factors to help engineers identify causal scenarios, which are environmental factors, human factors and equipment factors.

In the process of shifting from manual driving to full automation, the degree of automation of the train control system is increased, and more unknown risks are introduced. This paper shows the treatment strategy and safety assurance measures for the uncertainty of a FAO system, so as to improve safety of the rail transit system.

An optimized causal scenarios search method based on the STPA method was used to analyze the safety of a scenario of an FAO system. The analysis results proved the feasibility and superiority of the optimized method in the fully automatic system to give more guidance to analysts and reduce manual work pressure. For each operational scenario, it can identify its specific causal scenario and propose more targeted measures. In addition, the safety assurance process also includes comprehensive testing, verification, and validation. These activities are aimed at ensuring that FAO systems provide safer and more secure services than existing CBTC systems.

# Contents

# Conclusion

- ✓As the first FAO line with complete independent intellectual property rights, Yanfang Line has been operating stably and efficiently for more than one and half years since its opening. The data shows that the average commitment rate of Yanfang Line is 99.998%, and the average punctuality rate is 99.995%. Through the assessment of the Municipal Transportation Commission, the results of Yanfang Line are all "excellent", which fully reflects the safe, efficient, stable and reliable automatic operation system of Yanfang Line. We believe that through the rigorous safety analysis, comprehensive safety management and multi-phase verification proposed in this paper, the FAO system can provide safer, more efficient and more energy-efficient solutions for urban rail transit systems worldwide

**ACKNOWLEDGEMENTS**

*The research presented in this paper has been supported by Beijing Natural Science Foundation（L181006）, Beijing Laboratory of Urban Rail Transit and Beijing Higher Institution Engineering Research Center of Urban Rail Transit CBTC System.*

# Conclusion

**Start with a method built on appropriate assumptions and build a model to illuminate solutions**

***"Essentially all models are wrong, but some are useful."***

*GEP Box and NR Draper (1987)*

*Empirical Model Building and Response Surfaces,424.*

# Conclusion

## References

1. IEC 62267-2009 Railway applications: automated urban guided transport(AUGT) :safety requirements[S].IEC,2009.
2. Leveson N. Engineering a safer world: Systems thinking applied to safety[M]. Mit Press, 2011.
3. Leveson N G. A new accident model for engineering safer systems[J].Safety Sci,2004,42(4):237-270.
4. Sybert H. Stroeve , Mariken H.C. Everdij Agent-based modelling and mental simulation for resilience engineering in air transport[J].Safety Science 93 (2017) 29–49.
5. Fei-Yue Wang, Lingxi Li, Li Li. Steps toward Parallel Intelligence, IEEE/CAA JOURNAL OF AUTOMATICA SINICA, VOL. 3, NO. 4, OCTOBER 2016.
6. Hollnagel, E. (2004). Barriers and accident prevention. Aldershot, UK: Ashgate.
7. Hollnagel, E. (2012). FRAM – The Functional Resonance Analysis Method. Farnham, UK: Ashgate.
8. Sybert H. Stroeve, Mariken H.C. Everdij. Agent-based modelling and mental simulation for resilience engineering in air transport, Safety Science 93 (2017) 29–49.

# Thanks for your attention

Dr. Fei Yan
Email: fyan@bjtu.edu.cn

IRSE
INSTITUTION OF RAILWAY SIGNAL ENGINEERS

北京交通大學
BEIJING JIAOTONG UNIVERSITY