STPA for

Automated Urban Guided Transport System

Tang Tao & Yan Fei

State Key Lab of Rail Traffic Control and safety

Beijing Jiaotong University

Outline

1 Background

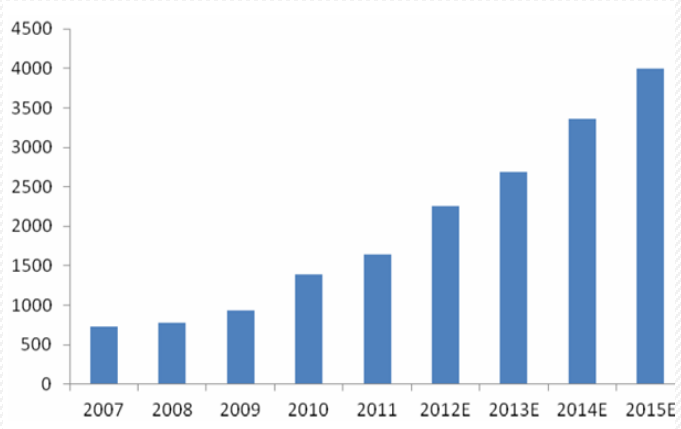
2 What is FAO

3 STPA for train door control in FAO

4 Conclusion

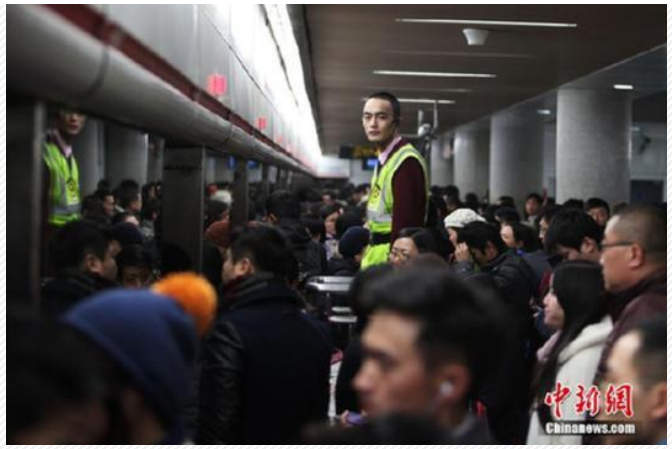
Urban Guided Transport System Development In China

- About 95 lines and 3000 Km urban transit lines are operated in the 22 cities including.
  - ✓ Beijing, 526Km,19 lines operated, 11millions passengers/day
  - ✓ Shanghai, 549Km,16 lines operated, 9millions passengers/day
  - ✓ Guangzhou, 256Km, 8 lines operated,7millions passengers/day
- About 80 lines and 3000 Km are under constructed now. Before 2020, about more than 6000 Km lines will be built.



The Development of Chinese Mass Transit

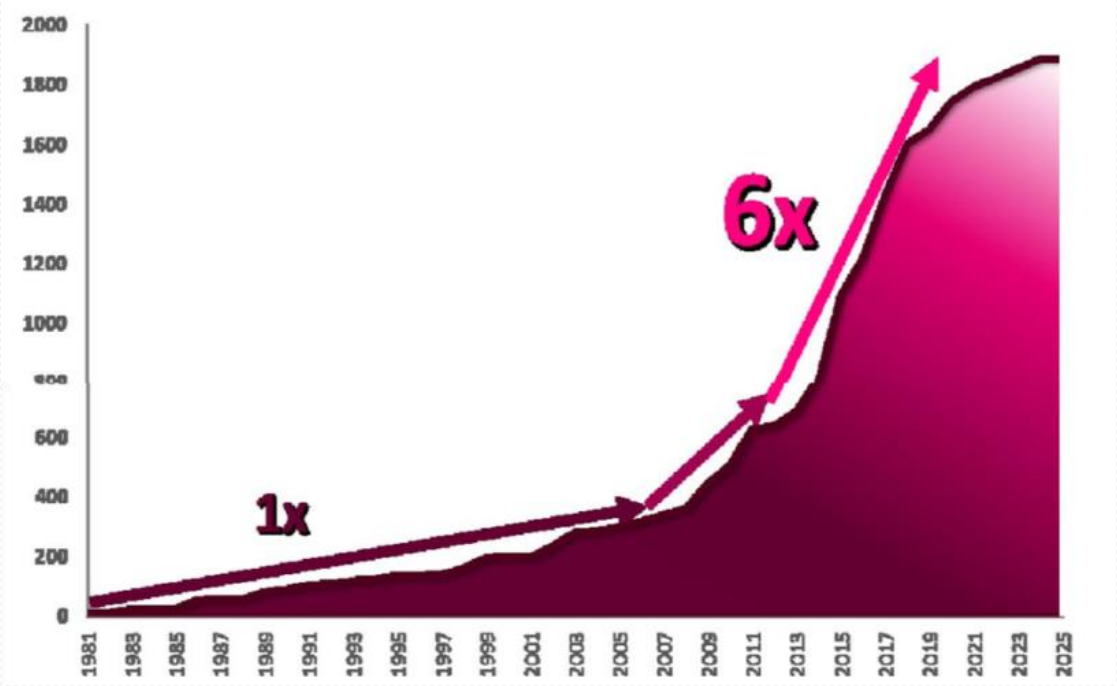
The stations passengers in Beijing in the peak hours



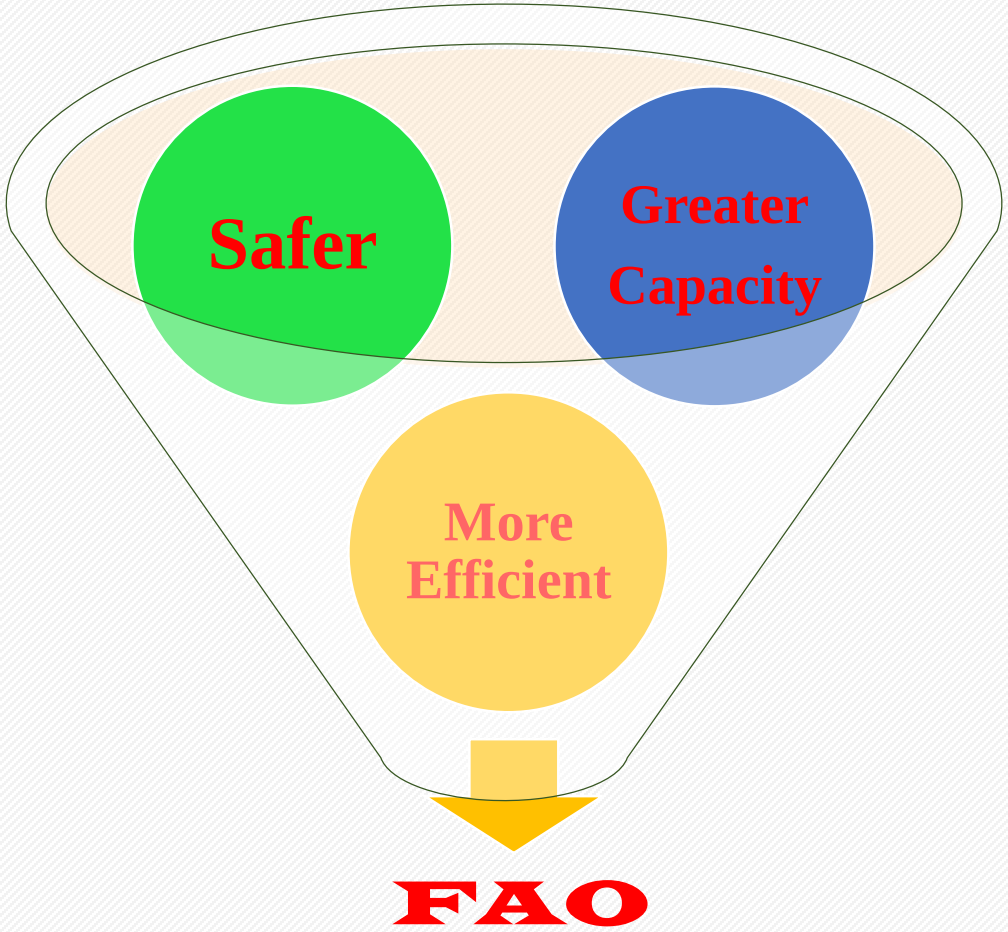
The stations passengers in Shanghai in the peak hours

Technology Trend of Urban Guided Transport System

- Beside adding new lines, Automation is the best method for a metro operator;
- Full Automatic Operation: greater capacity and safer, more efficient;
- RATP in Paris, London Underground and MTR of HongKong has decided to migrate FAO



Metro Automation in 2013 from UITP



FAO Technology in Beijing

Beijing municipal government had decided:

- Yan fang Line which will be operated at the end of 2017 as a national demonstration line of FAO.
- Line 3,12,17,19 and new airport line in Beijing will be built in FAO

Outline

What is FAO

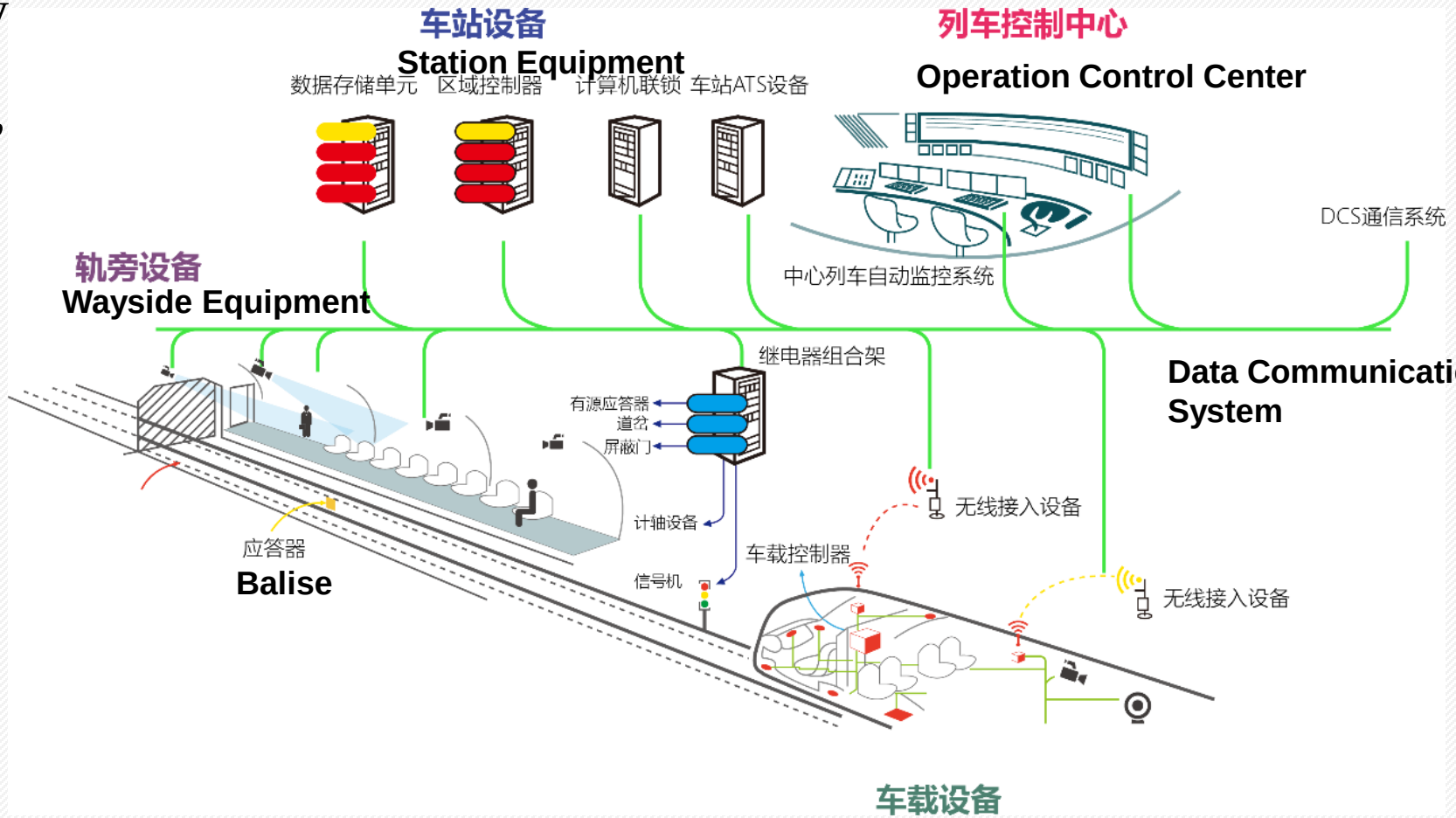
- **UGT can be operated at different grades of automation defined below.**
- **The definition of grades of automation arises from apportioning responsibility for basic train operation functions between operation staffs and system.**

Basic functions of train operation		On-sight train operation	Non-automated train operation	Semi-automated train operation	Driverless train operation	Unattended train operation
		GOA0	GOA1	GOA2	GOA3	GOA4
Ensure safe movement of trains	Ensure safe route	x (points command/control in system)	system	system	system	system
	Ensure safe separation of trains	x	system	system	system	system
	Ensure safe speed	x	x (partly supervised by system)	system	system	system
Drive train	Control acceleration and braking	x	x	system	system	system
Supervise guideway	Prevent collision with obstacles	x	x	x	system	system
	Prevent collision with persons on tracks	x	x	x	system	system
Supervise passenger transfer	Control passengers doors	x	x	x	x	system
	Prevent injuries to persons between cars or between platform and train	x	x	x	x	system
	Ensure safe starting conditions	x	x	x	x	system
Operate a train	Put in or take out of operation	x	x	x	x	system
	Supervise the status of the train	x	x	x	x	system
Ensure detection and management of emergency situations	Detect fire/smoke and detect derailment, detect loss of train integrity, manage passenger requests (call/evacuation, supervision)	x	x	x	x	system and/or staff in OCC
NOTE x = responsibility of operations staff (may be realised by UGTMS system) system = shall be realised by UGTMS system						

FAO

The structure of AUGT

- Station, Train, Guideway between stations, depots, Control center
- Entities to be protected：Persons, Passengers, Staff, Public, Property



Safety Function of AUGT

- Supervising guideway
  - Prevent collision with obstacle
  - Prevent collision with persons
- Supervising passenger transfer
  - Control passenger doors
  - Prevent injuries to person between cars or between platform and train
  - Ensure safety starting conditions
- Operating a train
  - Put in or take out of operation
  - Supervise the status of the train (UTO)
- Ensuring detection and management of emergency situations

Outline

1 Background

2 What is FAO

3 STPA for train door control in FAO

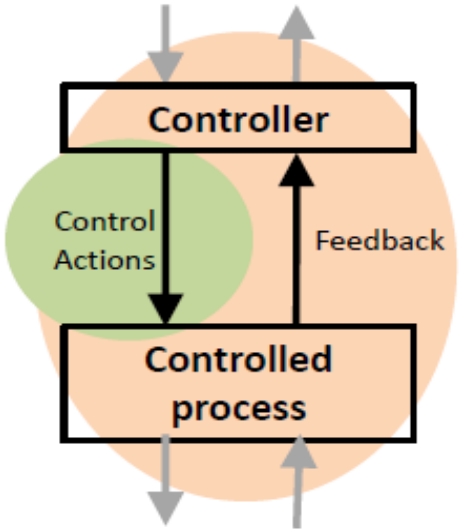
4 Conclusion

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

AUGT Systematic Accidents

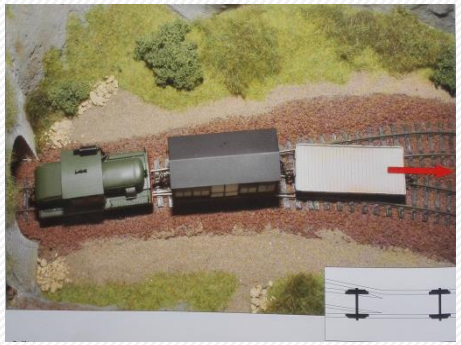
A-1 Train collides with the front train, persons or other obstacles on the track

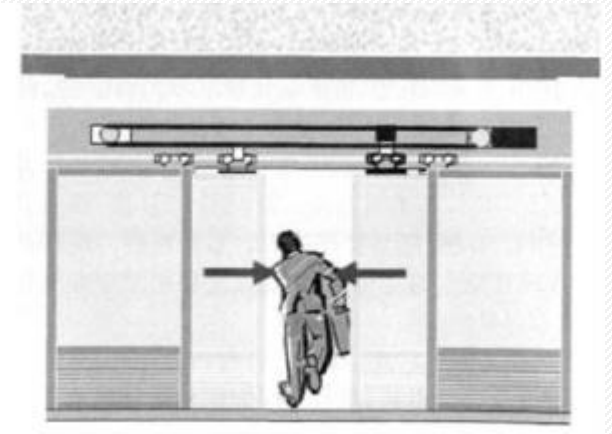
A-2 Train derails when it moves on a track

A-2: Passenger is hurt when he transfer between a train door and a platform screen door (PSD).

Collision

Derailment





Passenger transferring hurts

Door Control Related Accidents and Hazard in FAO

General Accident description: Passenger is hurt when he transfer between a train door and a platform screen door.

A-1: When the train is running, the passengers fall outside the car;

A-2: Passengers were hurt in the passenger door closing process ;

A-3: The passengers were caught in the middle of the door and the door fell off the platform or the train starts to drag the passengers, causing passengers casualties;

H-1: Train departures while door has not been closed completely.[A-1]

H-2: The train did not stop at the parking screen window, open the door. [A-1]

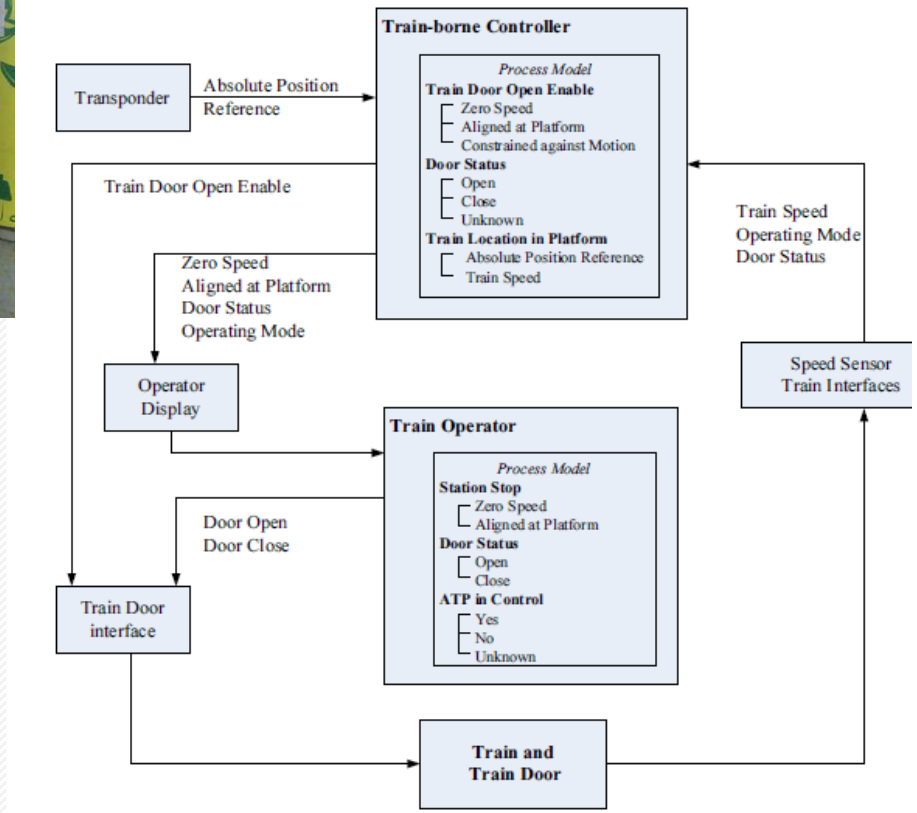
H-3: The train in the process of moving, and open the door. [A-1]

H-4: When passengers get on or off, the door is closed. [A-2] [A-3]

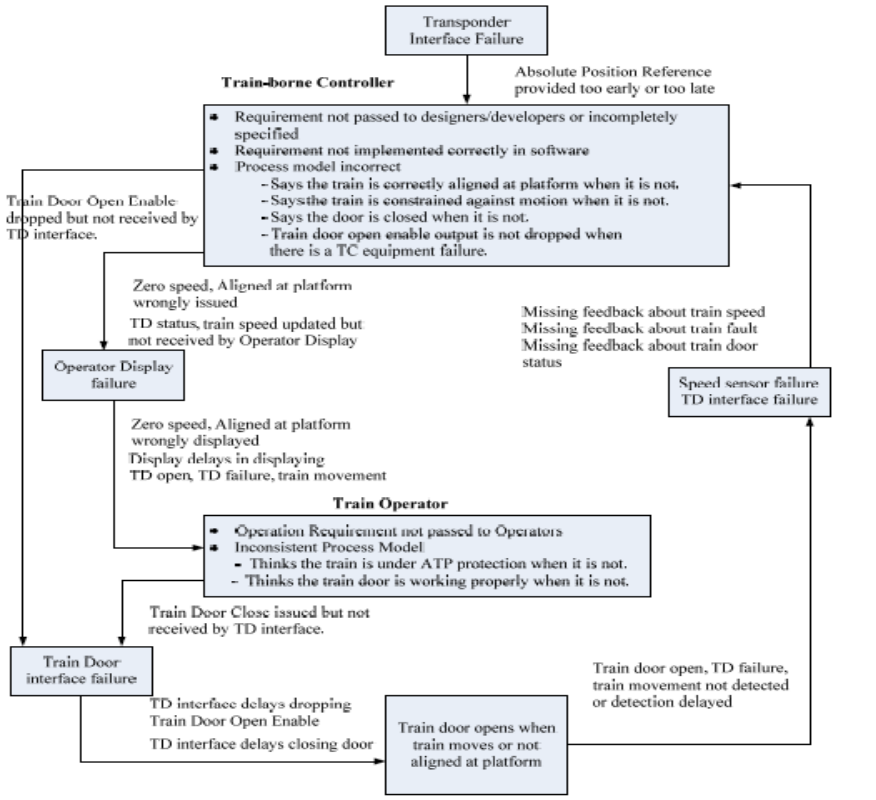
Process Model for Train Door Control in Manual Mode

Hazard: Door opens with train in motion or not aligned at platform

From Airong Dong master thesis,2012



Process Model



Causal Factor Analysis

Train Door and Platform Screen Door

- Train door is used for passenger transfer
- The platform screen doors(PSDs) are used for
  - Safety: Train piston wind & Fall off platform
  - Energy conservation: Air condition
  - Prevent suicide
- The function requirement in IEC62290

Platform screen door

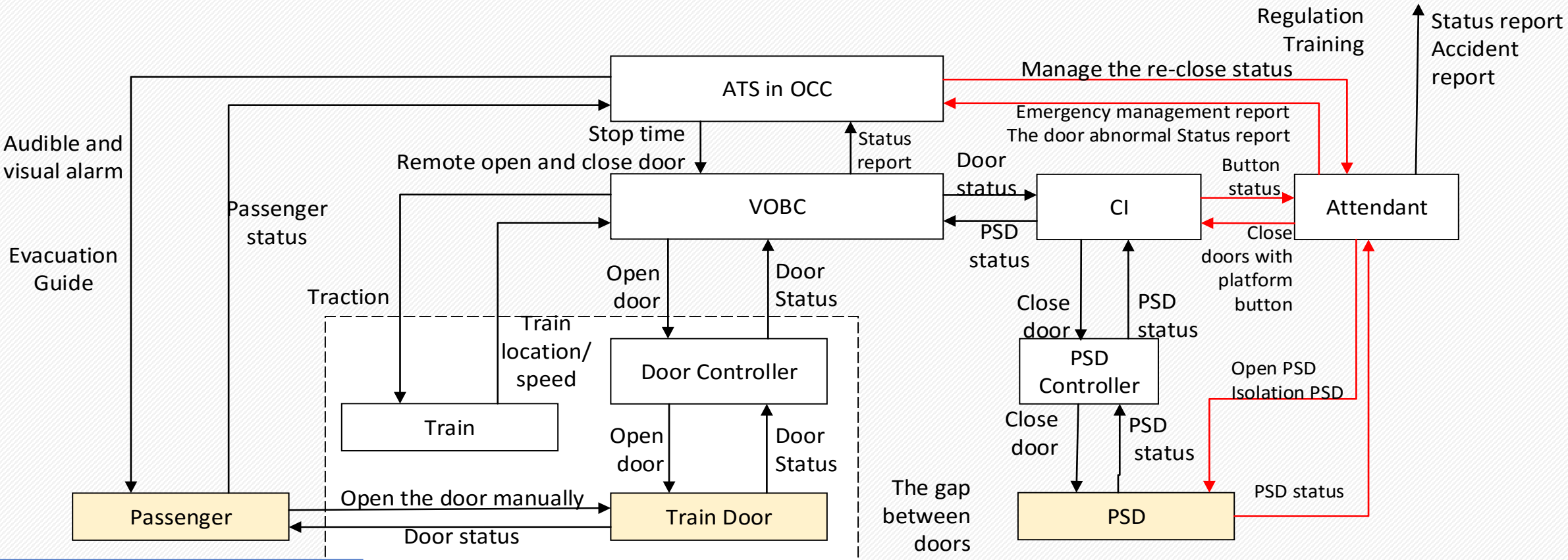
There is a Gap!

6.2.2.5 Supervise passenger transfer

6.2.2.5.1 General

Ensuring safe passenger transfer through the following functions is a mandatory system requirement for GOA4. For lower grades of automation these functions may be in whole or in part the responsibility of the train driver or operations staff on the platform in combination with the system:

System Control Structure of Doors



Passengers are regarded as controlled objects

Unsafe Control Actions

Control Action	“Not Providing” cause hazard	“Providing” cause hazard	Incorrect Timing /order	Stopped too soon or applied tool long
Open Train Door		UCA5：Train door open when train is not at the station UCA6：Train open door while the speed is not zero		
Close Train Door			UCA7：Train door close too early on platform	
Open PSD		UCA8：PSD opens when the train has not arrived at the platform		
Close PSD			UCA9：PSD closes too early on platform	

Causal Factor for Unsafe Door Control

No.	Unsafe Control Actions	Causal Factor	Notes
UCA4	Train departures while door has not been completely closed	System think train door close but in fact it did not	
		Train status lost caused by sensor failure	
UCA5	Door opens with the train not aligned at platform	Electric map not consist with reality	
		Speed measurement error	
		Control equipment failure	
		Wrong train location judgment	
UCA6	Door opens with the train in motion	Speed measurement error	
		Wrong Zero speed judgment	
		Control equipment failure	
		Speed measurement error	
UCA7	Train Close the door too early on the platform	Close train door when stop time not end	
		Stop time not consist with requirements	
		Close train door cause by control equipment failure	
		Train status lost caused by sensor failure	
		Close train door when there is a person in the gap	

Causal Factor for Unsafe PSD Control

No.	Unsafe Control Actions	Causal Factor	Notes
UCA8	PSD opens when the train has not arrived at the platform	PSD is opened by operator of TIAS by error	
		FAO system tells PSD controller that the train has stopped at the platform by error.	
		Wrongly open PSD	
UCA9	PSD closes too early on platform	Close PSD when stop time not end	
		Stop time not consist with requirements	
		Designed closing time is not consistent of the train door	
		Wrongly close PSD	
		PSD status lost caused by sensor failure	
		PSD closes when there is a passenger in the gap.	

Scenario No.	Function	Accident	HAZARD List for Emergency Scenarios
1	Enter into mainline	A-1	The train at speed is not zero, and the door open
2	Stop at platform	A-1	The train did not stop in the parking window, and the door opened
3	Stop at platform	A-1	The train did not stop in the station's parking window, and the platform door opened
4	Departure from platform	A-2	Train stop time to arrive, did not provide closed alarm signal
5	Departure from platform	A-2	The train speed is zero, which is parked in the parking window, the passenger is in the car door, and the door is closed
6	Departure from platform	A-2	Passenger ride down the process of closing the door
7	Departure from platform	A-2	Train stop time to arrive, did not provide closed alarm signal
8	Departure from platform	A-2	The train speed is zero, stop in the parking window, passengers in the platform between the door, the door closed
9	Departure from platform	A-3	Between the door and the platform door clip to the passengers
10	Reverse from the line end	A-2	Train at the end of the station or reentry station, passenger ride down the process of closing the door
11	Evacuation passengers after service	A-5	Clear off the state fails to keep the door open
12	Door closing for second time	A-5	Door close encounter obstacles not open
13	Door closing for second time	A-5	When the platform door is closed, the obstacles are not opened
14	Door closing for second time	A-2	The train has not closed the door three times after the opening and closing, did not enter the anti pinch mode
15	Interval evacuation	A-5	Did not keep the door open when evacuating in section
16	Interval evacuation	A-5	Platform is not open to open the door when the evacuation。
17	Interval evacuation	A-5	Did not keep the door open when evacuating in section
18	Interval evacuation	A-5	Under the evacuation of the platform did not keep the door open
19	Door failure isolation platform door	A-2	The door cannot be opened, but the platform door is open
20	Platform door failure isolation door	A-2	The platform door cannot be opened, but the door is opened

Methodology Comparison

Comparison	STPA	HAZOP
Advantages	System view and focusing on the interaction and the safety constraints between components of system	Focusing on the information flow and good at the analysis of operational scenario
Disadvantages	Detail Design analysis which can be enhanced by scenario based STPA	Need to generate the core hazard from hazard record sheet
Fit for the analysis of AUGT	Need focusing on the control process model in each operational scenario	Depends on the description of Scenario and lack of system level analysis

Contents

Conclusion

- STPA is more focusing on the safety related interaction and we can easily find the main clue by safety constraints compared to HAZOP;
- In the AUGT operation, more attention should be paid to the Door and PSD control . It is best to use some sensors to detect the gap between a train door and a PSD.
- Passengers should be told to care about the gap between Door and PSD and obey the guidance of the voice alarm or the warning of the staff.
- Staff on the platform should watch out for the potential danger.

THANKS !

email:
Prof. Tang Tao
ttang@bjtu.edu.cn
Dr. Yan Fei
fyan@bjtu.edu.cn