SOUTHWEST JIAOTONG UNIVERSITY

RAMS application in Railway signaling system

Lei Jiang

Laboratory of Traffic Information Engineering and Control, Southwest Jiaotong University, China

Email: lei.jiang@ntnu.no

L.jiang@swjtu.edu.cn

1. Introduction of SWJTU
2. Introduction of CTCS
3. RAMS application of CTCS
4. High-speed train collision analysis
5. Future research

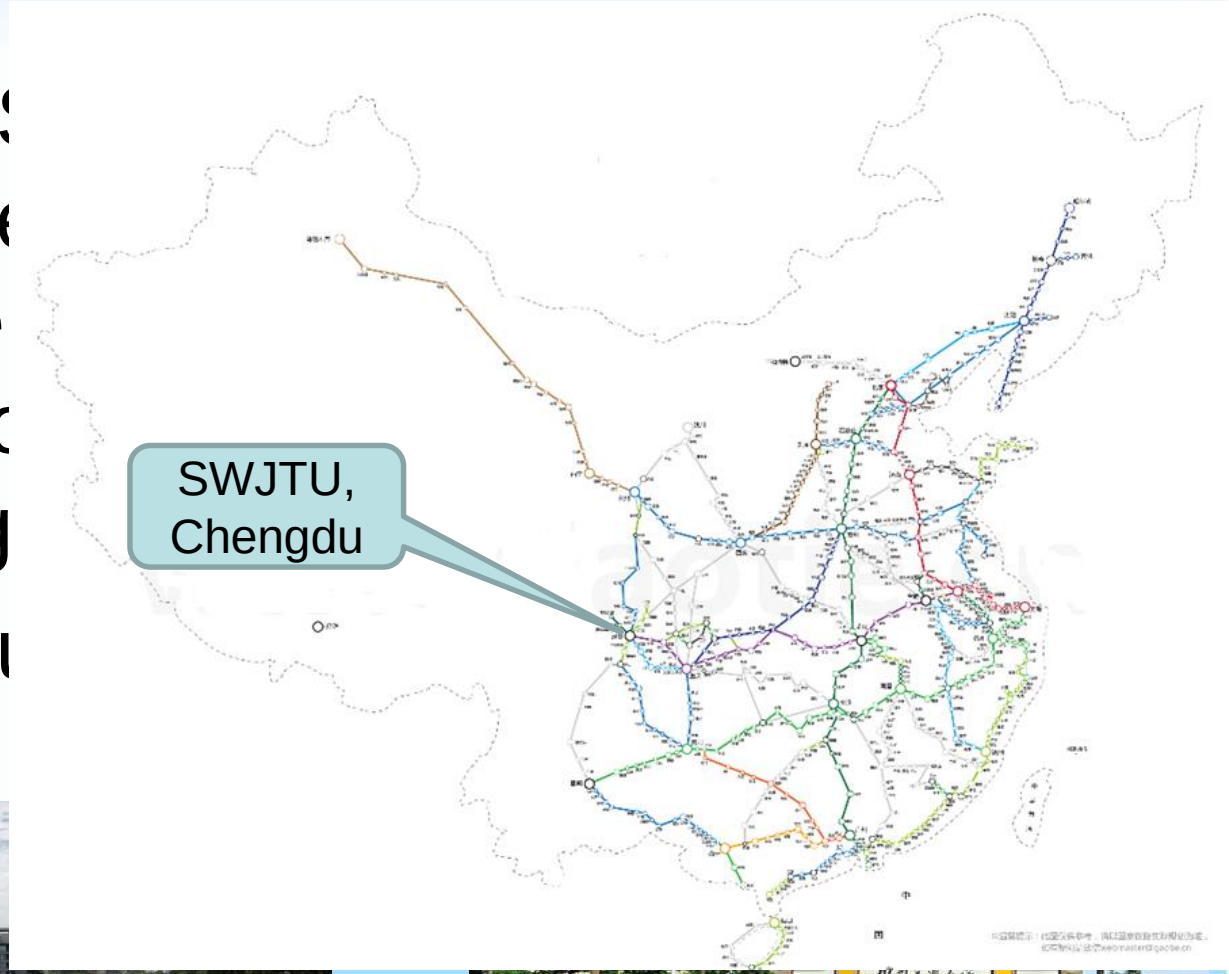
Ph.D. Candidate--
Traffic Information Engineering & Control, 2014-up to now, Southwest Jiaotong University
Master Degree--
Transportation Engineering, 2012, Southwest Jiaotong University
Bachelor Degree--
Telecommunication Engineering (Railway Signaling Control), 2009, Southwest Jiaotong University Emei Campus

Form 2012 to now, lecturer, Department of Railway Information Engineering, Southwest Jiongtong University. Major Courses Include the Reliability and Safety of Railway Signaling System and Chinese Train Control System(CTCS).

1. Introduction of SWJTU

Southwest Jiaotong University (S
and is one of China's oldest highe
as the cradle of China's railway e
East", SWJTU is the birthplace o
transportation, mining & metallurg

More information: http://www.swjtu

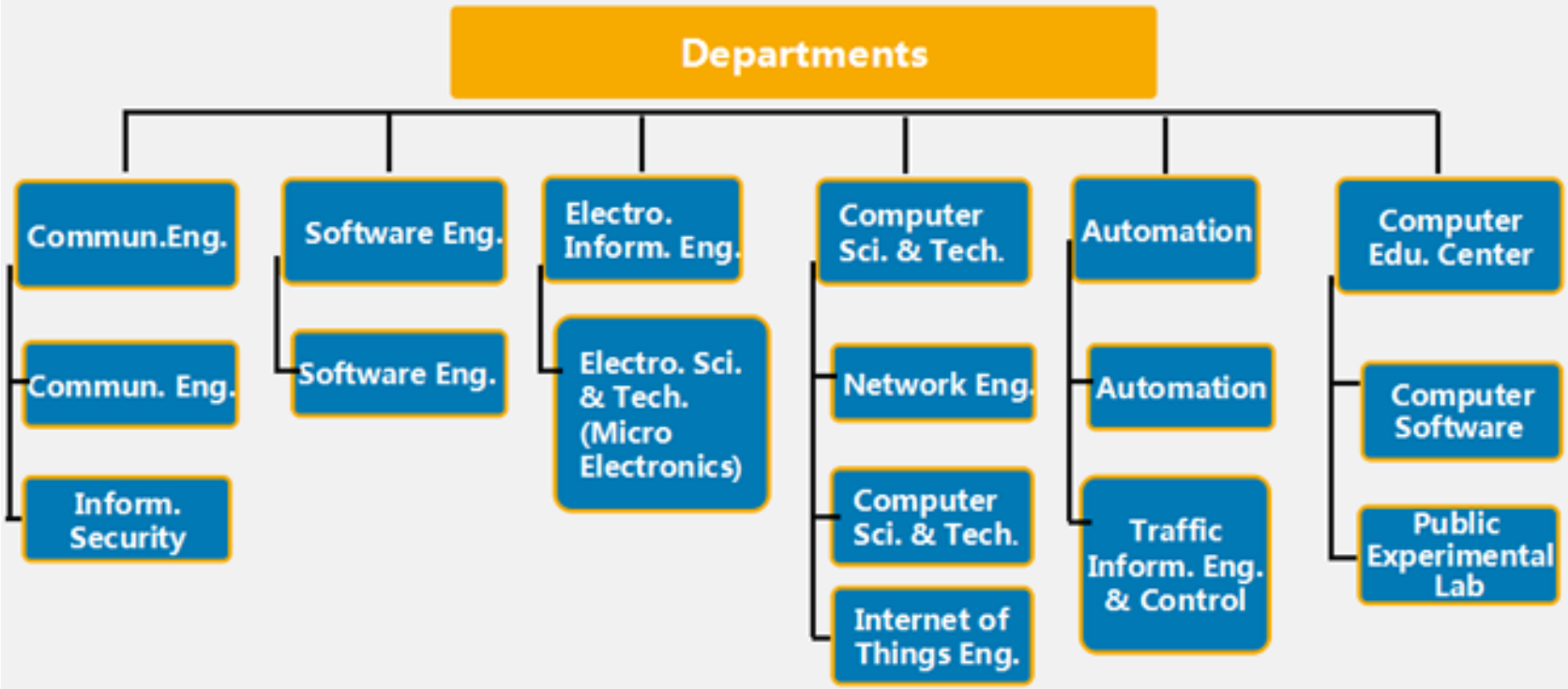


- SWJTU has achieved the goal of having national-level platforms for all specialty disciplines of civil engineering, mechanical engineering, electrical engineering, traffic & transportation engineering and surveying & mapping.

National Laboratory	the Rail Tra

1.1 Major faculties

- Faculty
- Faculty
- Faculty
- Faculty
- Faculty
- Faculty
- Faculty
- Faculty
- Faculty
- Faculty of Geosciences and Environmental Engineering
- Faculty of Architecture



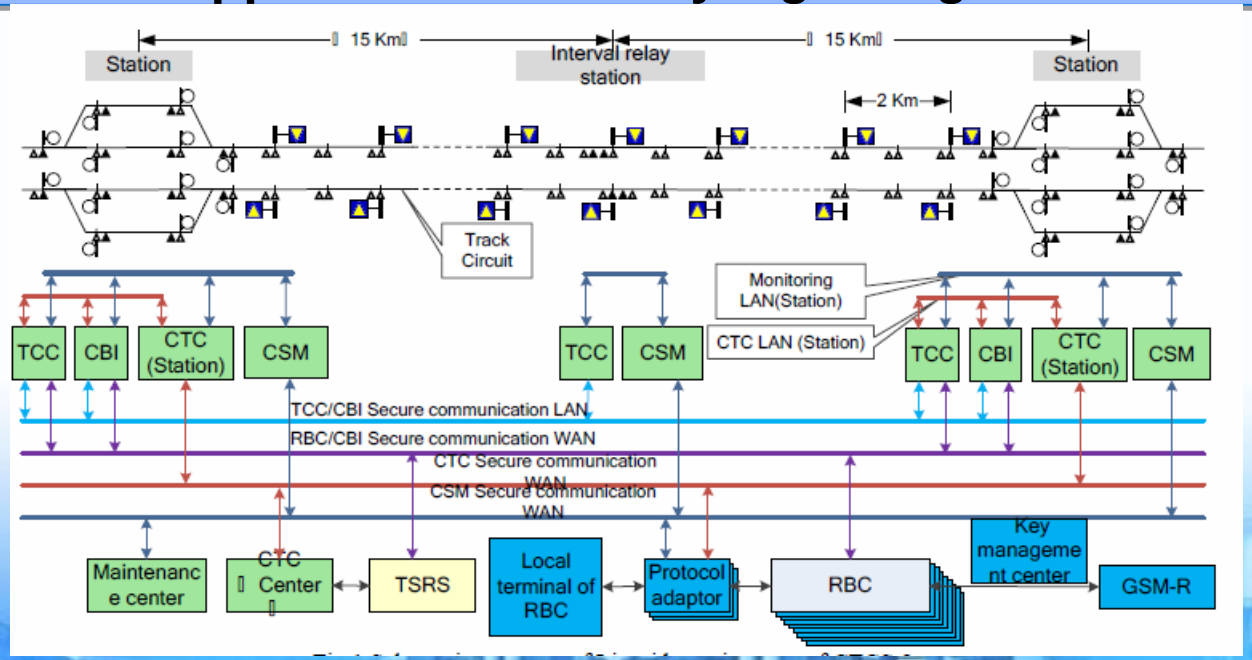
1.2 Projects related to HSR

National 973 Key Project	Fundamentals of broadband wireless communication networks under high mobility scenarios
Major Project, Ministry of Education	Research on the key technologies of intelligent railway traffic safety and engineering structure health monitoring
Major/Key Project, Ministry of Railways	Research on the key technologies of in railway signaling security
	Research on railway signaling equipment security authentication technologies
Major Research Project, China Railway Corporation	Research on Maintenance technologies for signal detection—Study of communications monitoring and maintenance technologies
	Research on Maintenance technologies for signal detection—Study of signaling monitoring and maintenance technologies

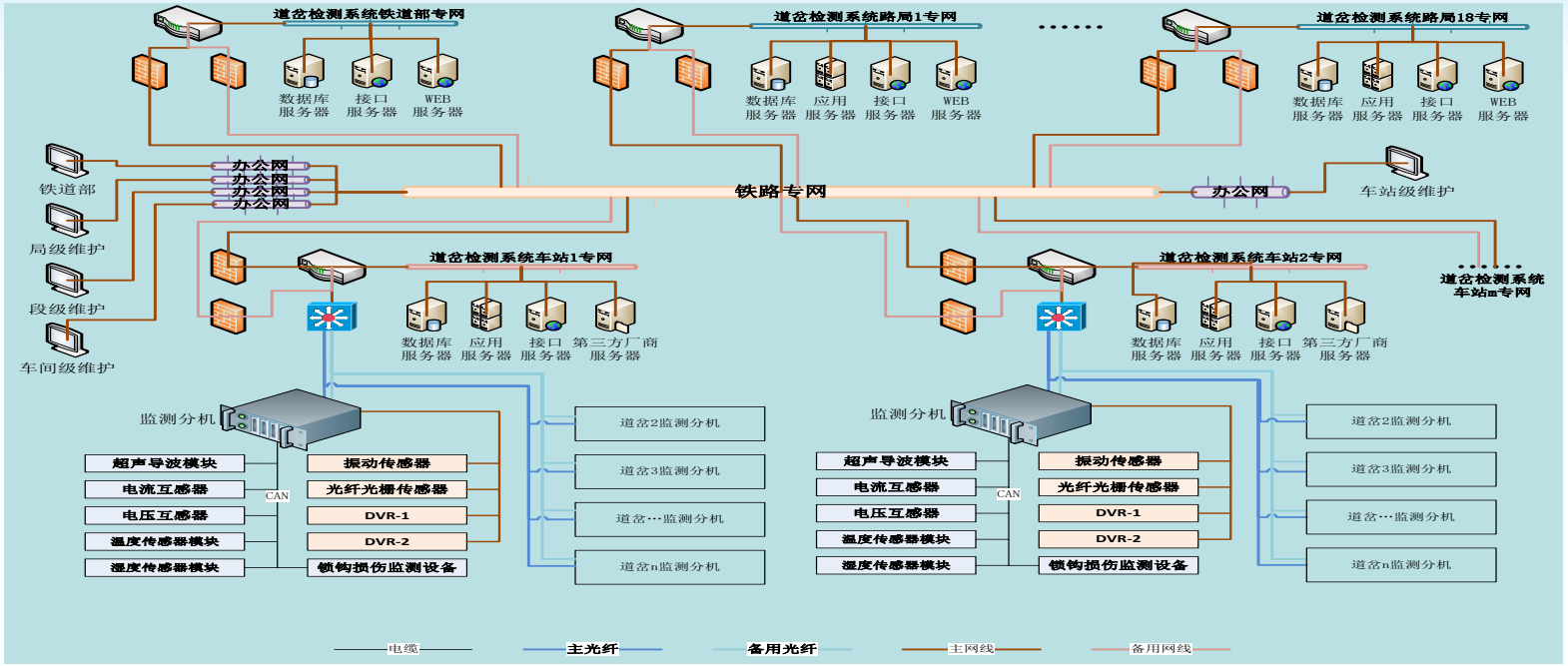
1.3 Research on Traffic Information Engineering and Control

Research

- **High-speed railway signaling technology**
- **Railway signaling network security**
- **Intelligent operational condition monitoring**
- **CTCS-2/3 simulation, design and verification**
- **CBTC-based signaling system, ATO, ATS, etc.,**
- **Automation of railway marshalling**
- **RAMS application in railway signaling**



Health Monitoring and Detection for High-speed Railway Turnouts



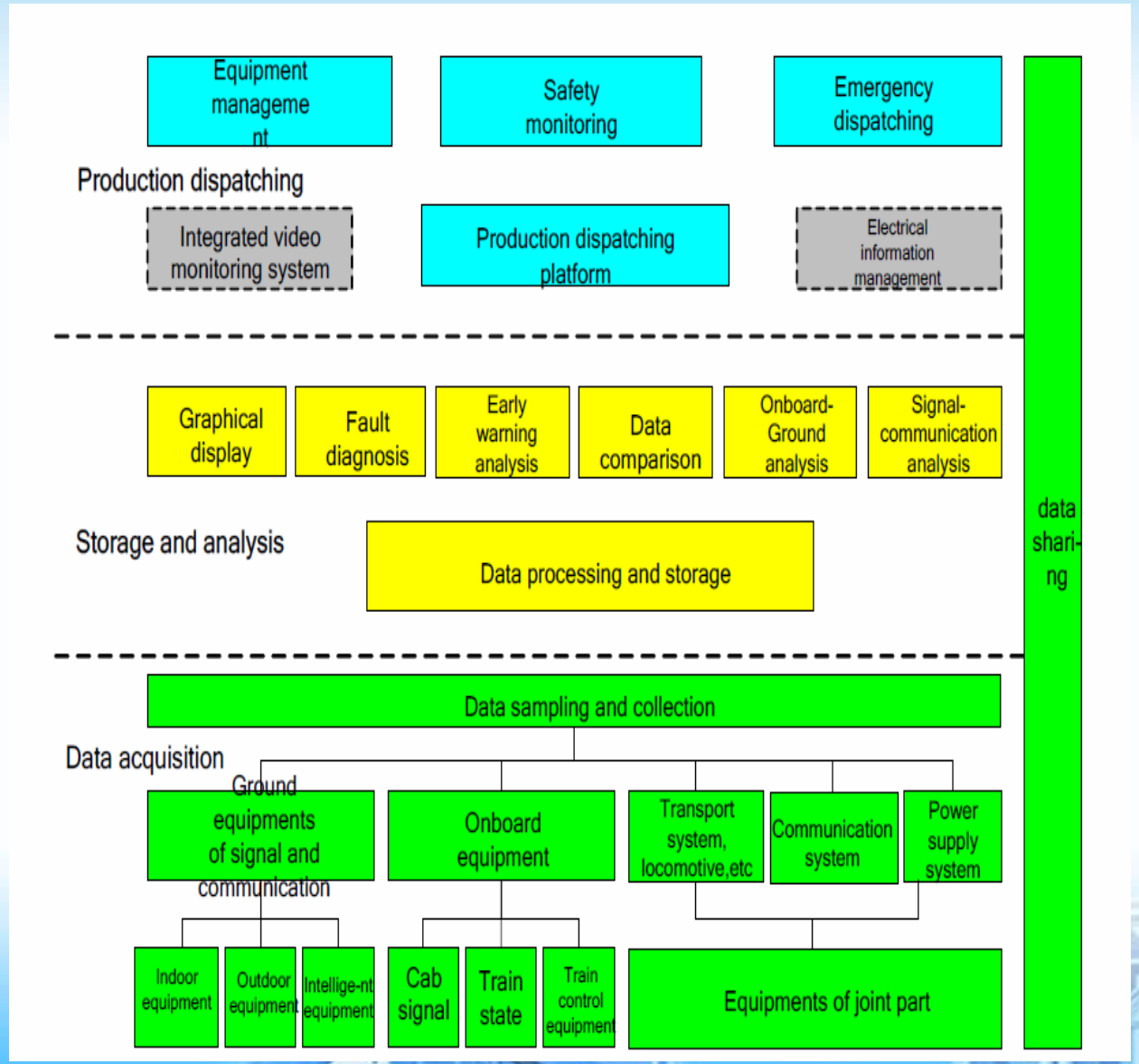
Functions:

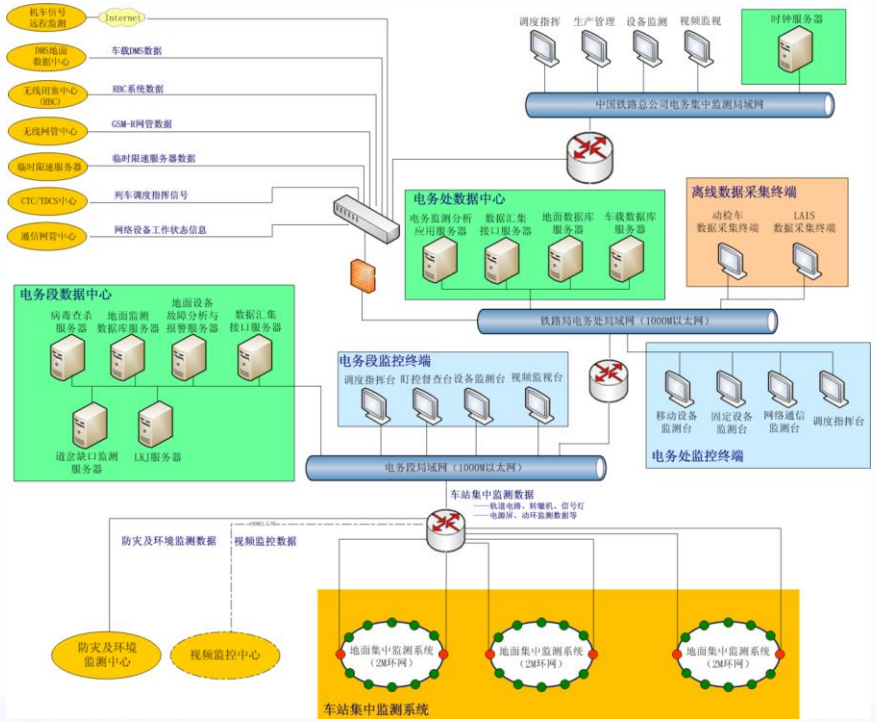
On-line monitoring the temperature, current, voltage of point machine

On-line monitoring the transforming force, close of turnout

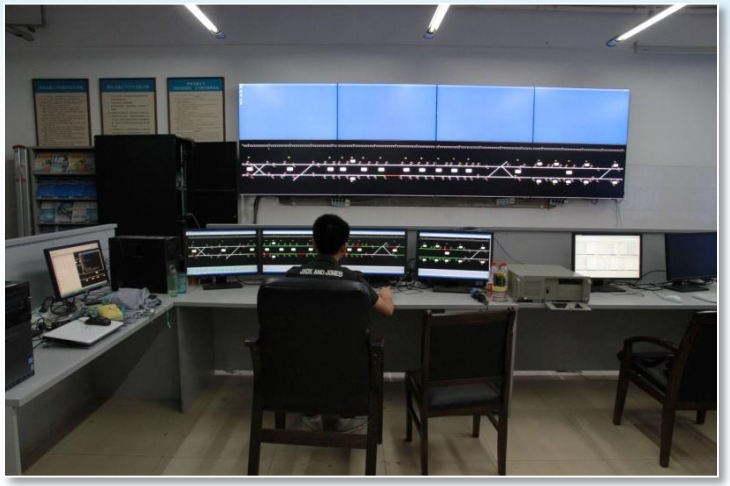
On-line monitoring and detecting the flaw at the bottom of turnout

Integrated Railway Signaling and Communication Monitoring System



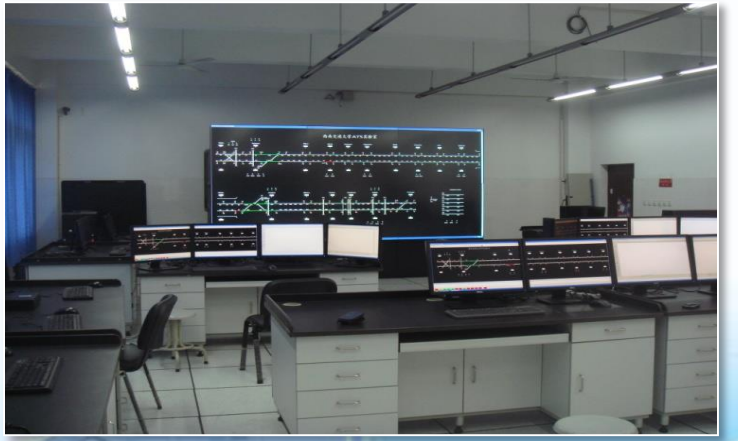


Key Laboratory of Traffic Information Engineering and Control



Dispatching simulation system

Signaling control testing and verification system



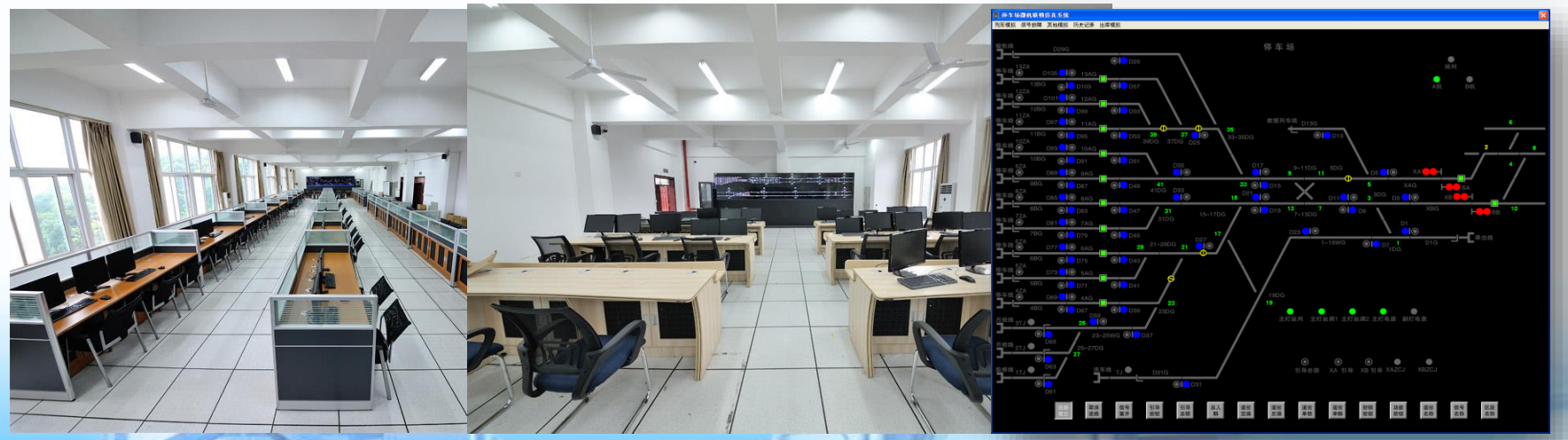
SWJTU ATS system

DCS monitoring system

Key Laboratory of Urban Rail Operation & Control

simulation platform

metro vehicle model



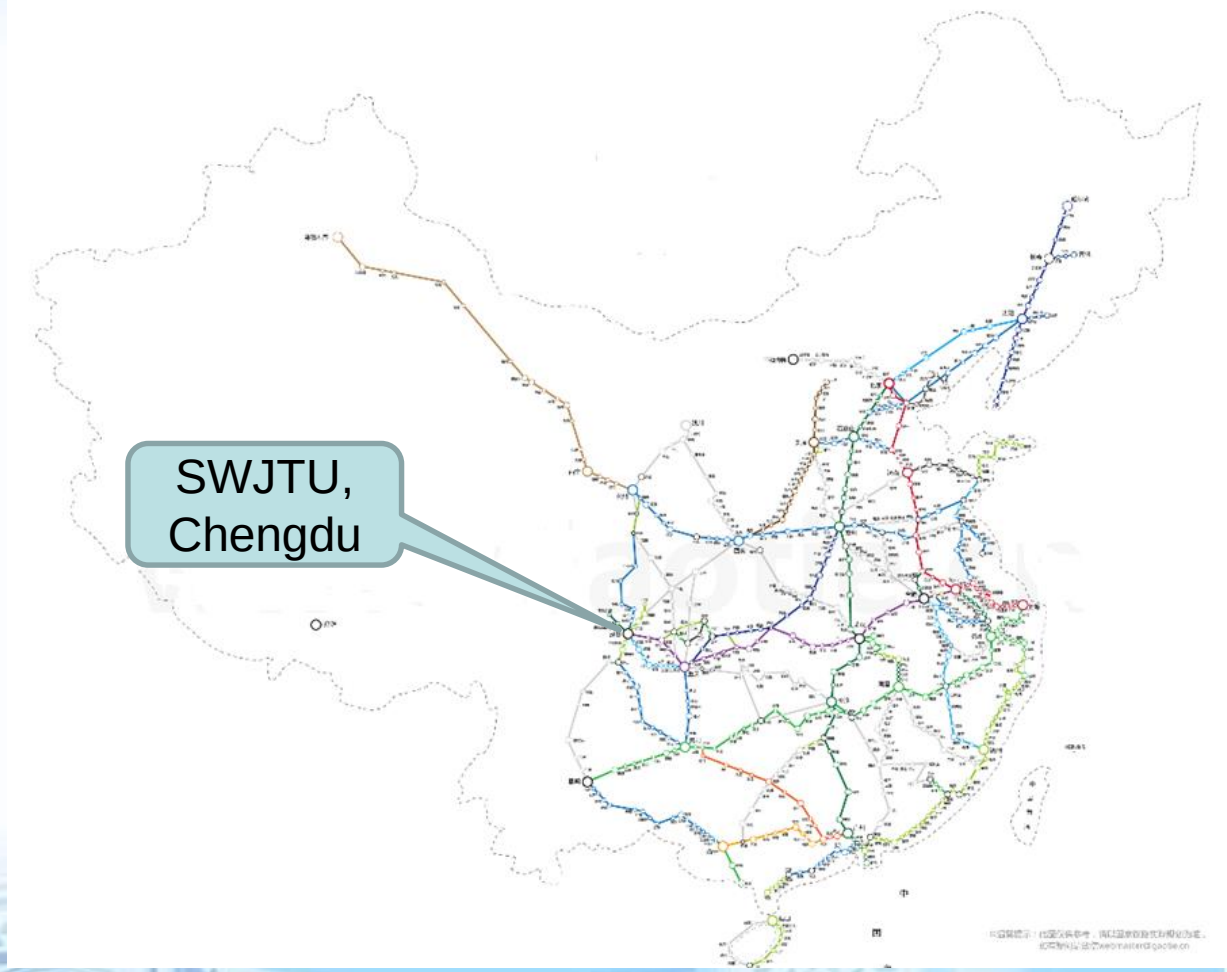
High speed railway dispatch center and Metro Operation control center

2. Introduction of CTCS

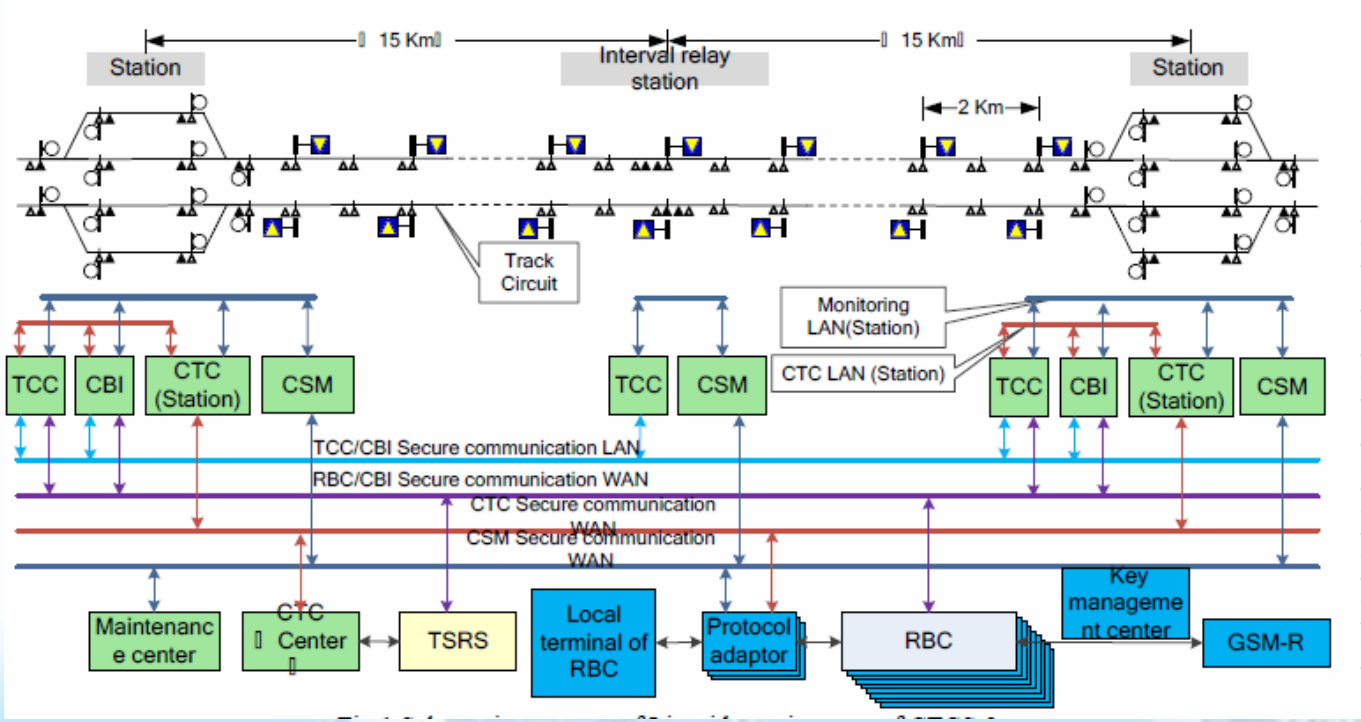
- Two direction of railway development

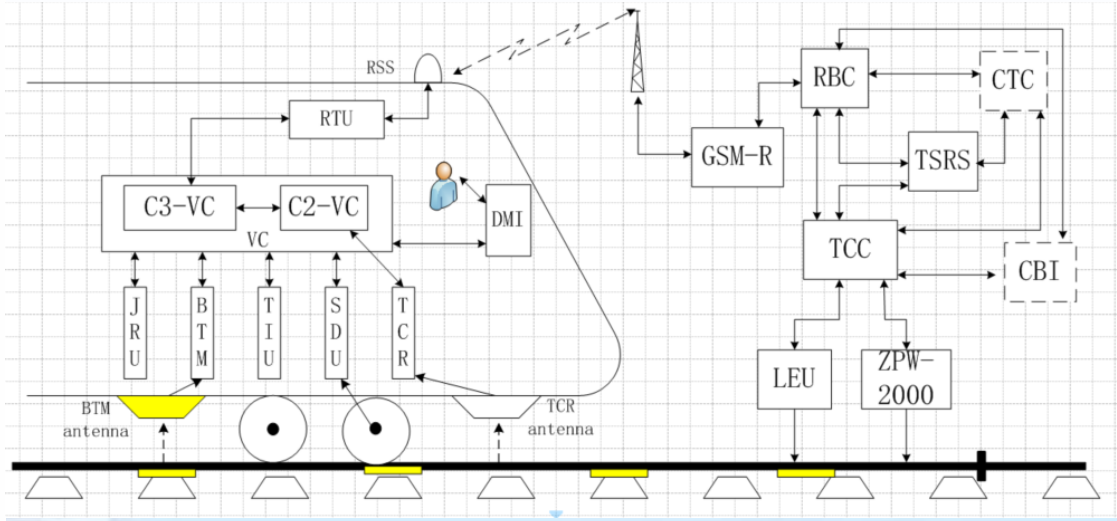
  Heavy haul railway for Freight Transportation

  High speed railway for Passenger Transportation



CTCS：Chinese Train Control System





The Control principle of CTCS-2

Track circuit Function：

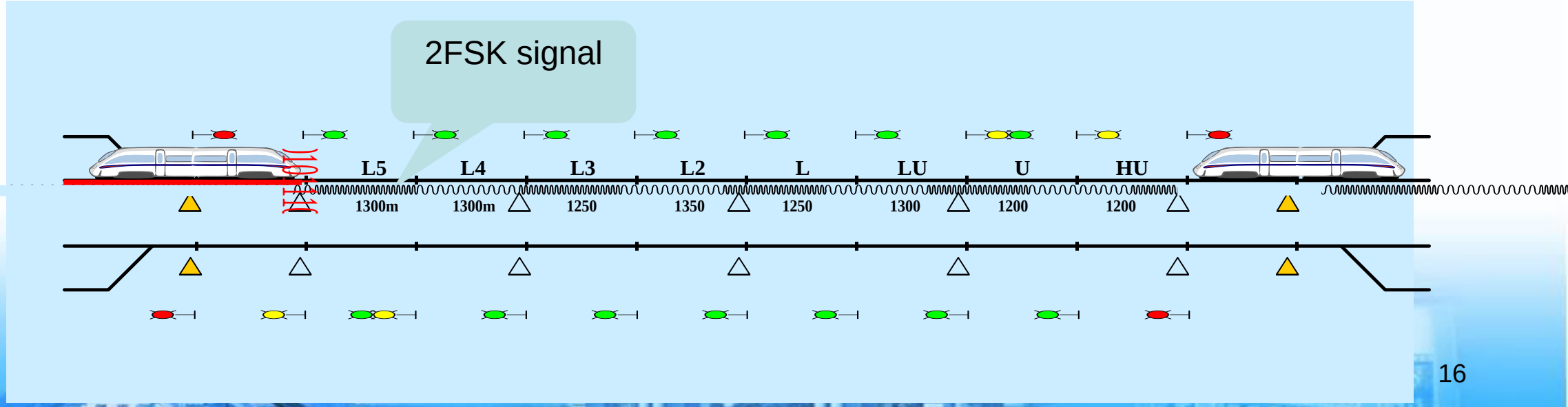
- Train occupancy and location
- Moving authority

Balise Function：

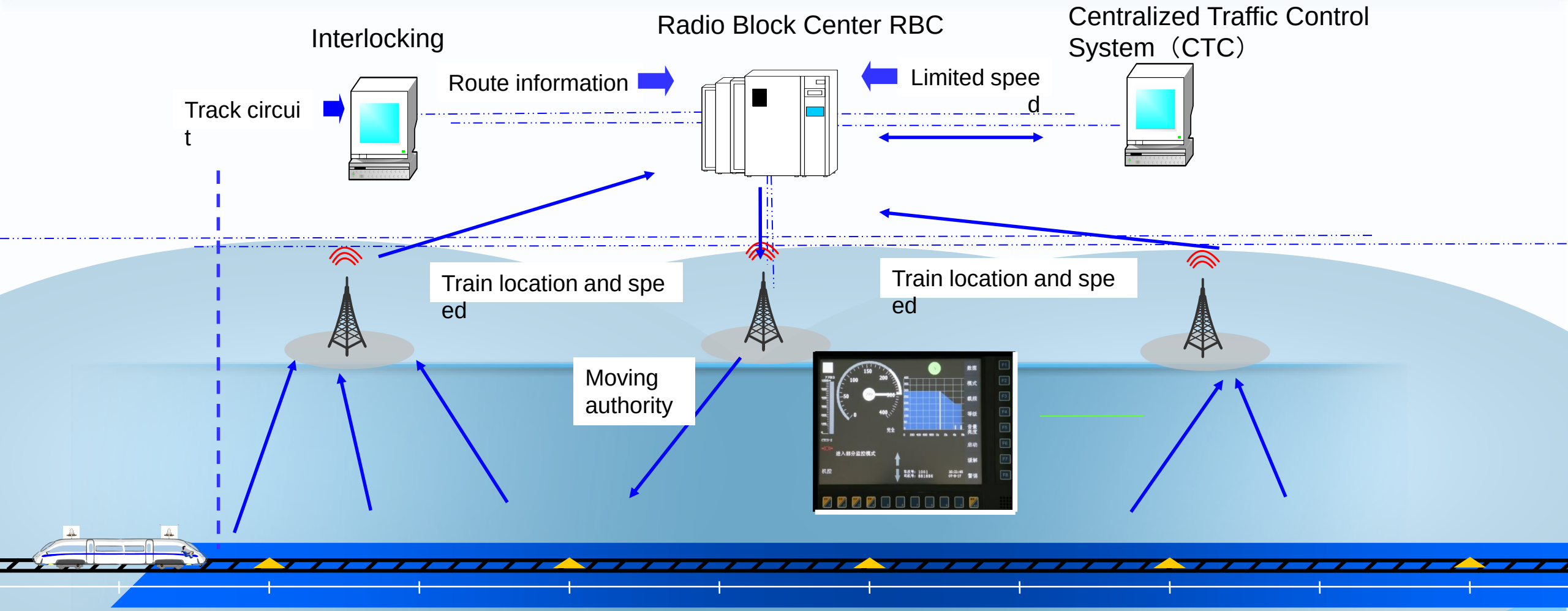
- Temporary limited speed
- Line profile

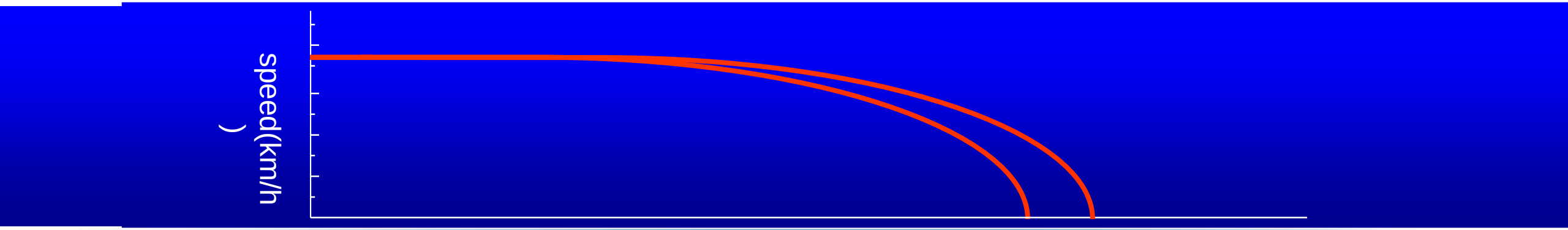
Onboard system Function：

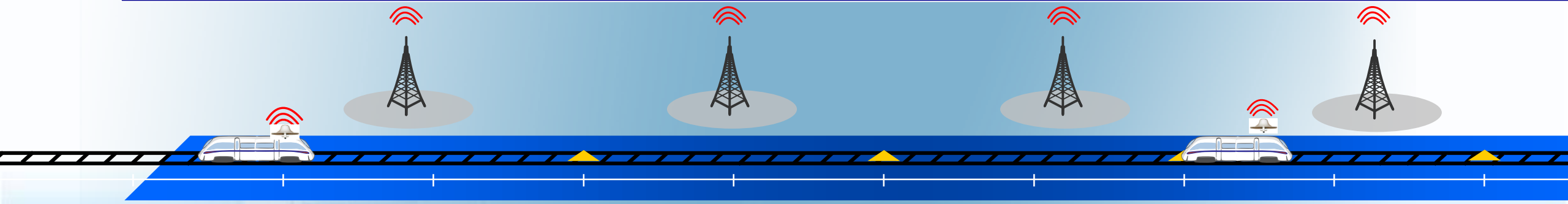
supervises the movement of the train to which it belongs, on basis of information exchanged with the trackside sub-system



The Control principle of CTCS-3




speed(km/h
)



3. RAMS application of CTCS

- EN 50126: Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS);
- EN 50128: Railway Applications - Software for Railway Control and Protection Systems;
- EN 50129: Railway Applications - Communications, signaling and processing systems – Safety related electronic systems for signaling.

The characteristic of Railway signaling system

Complex: hardware/software/human error/working environment

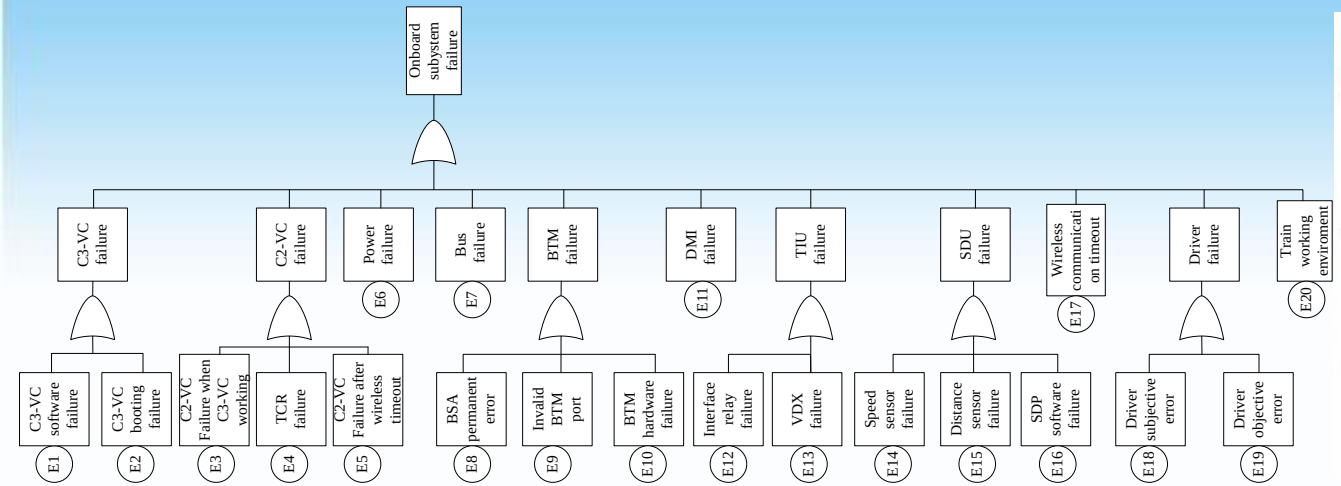
Large scale: the number of interacting components and subsystem has increased drastically.

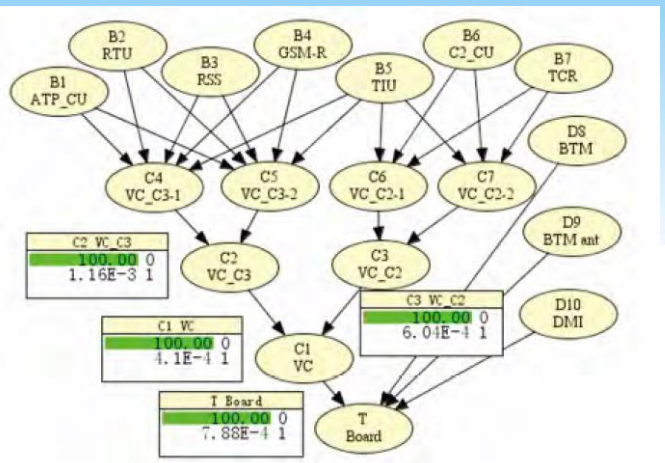
Phased mission system: accelerate, decelerate and constant

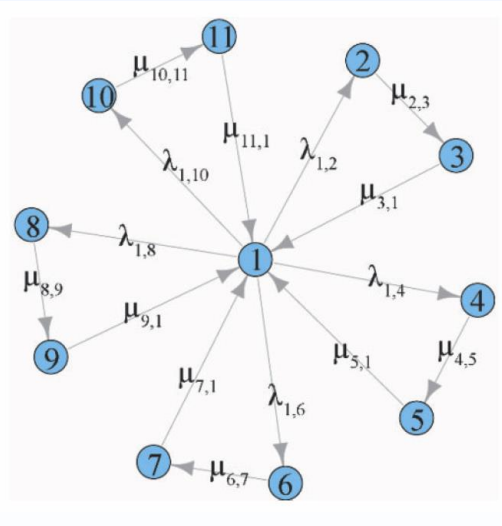
Cyber-physical system: computer-based system

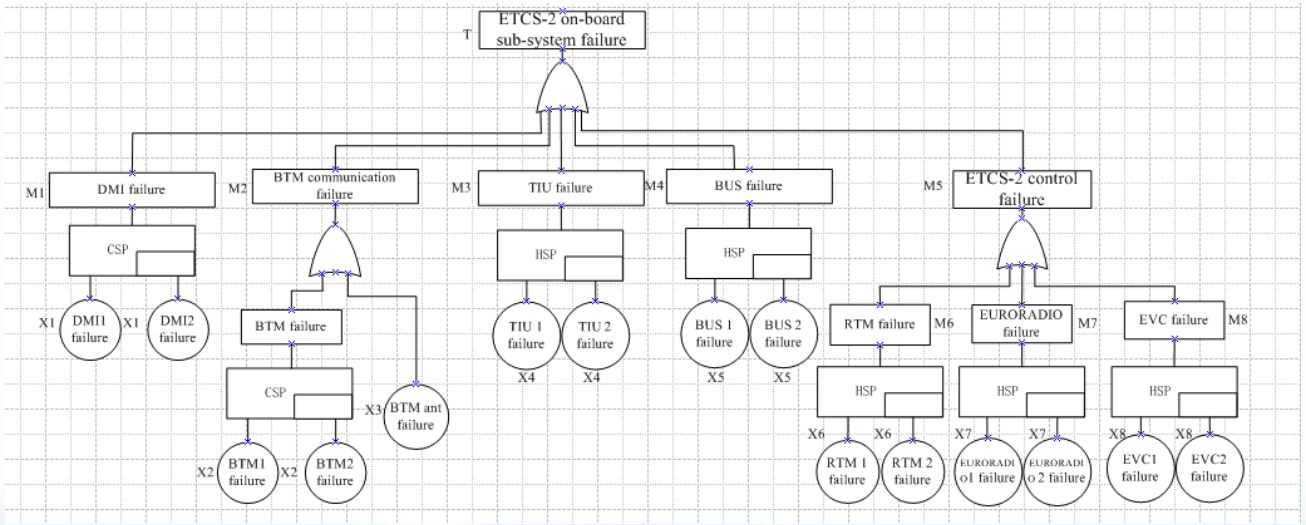
RAM in railway signaling system

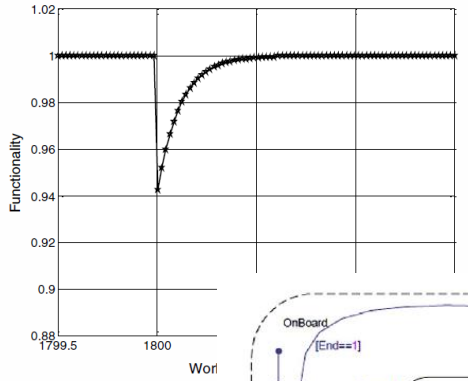
FMEA and FTA for the reliability assessment of ZPW-2000 track circuit.
RBD and Markov Chain Model
Bayesian Network
Dynamic Fault Tree
combining DS evidence and BN
data-driven model for maintenance
Resilience Quantitative Evaluation
dependability analysis
safety and availability analysis
Availability assessment using Statecharts

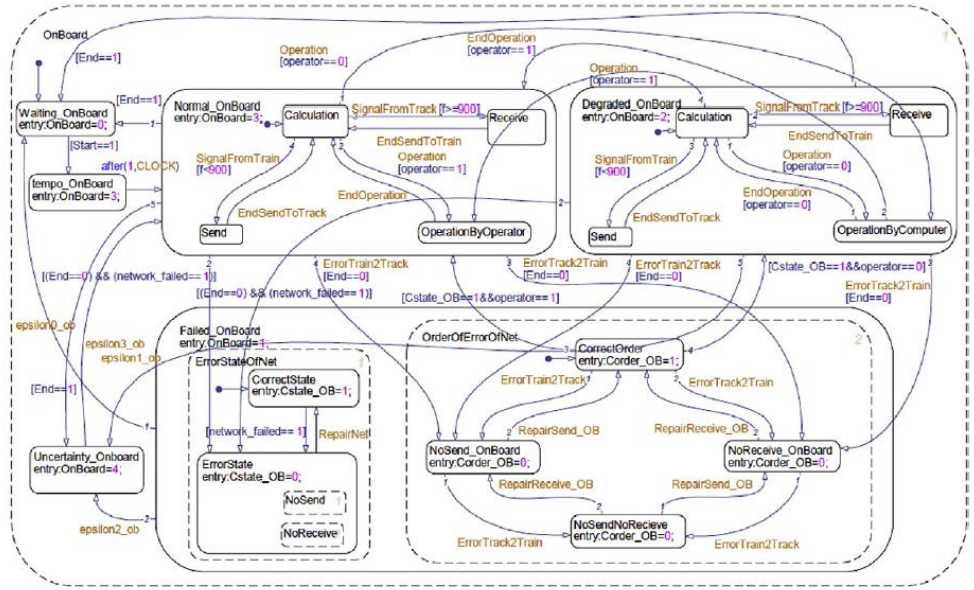

Onboard subsystem failure
C3-VC failure
C2-VC failure
Power failure
Bus failure
BTM failure
DMI failure
TIU failure
SDU failure
Wireless communication timeout
Driver failure
Train working environment
C3-VC software failure
C3-VC booting failure
C2-VC Failure when C3-VC working
TCR failure
C2-VC Failure after wireless timeout
BSA permanent error
Invalid BTM port
BTM hardware failure
Interface relay failure
VDX failure
Speed sensor failure
Distance sensor failure
SDP software failure
Driver subjective error
Driver objective error
E1
E2
E3
E4
E5
E6
E7
E8
E9
E10
E11
E12
E13
E14
E15
E16
E17
E18
E19
E20


B1 ATP_CU
B2 RTU
B3 RSS
B4 GSM-R
B5 TIU
B6 C2_CU
B7 TCR
DS BTM
D9 BTM ant
D10 DMI
C4 VC_C3-1
C5 VC_C3-2
C6 VC_C2-1
C7 VC_C2-2
C2 VC_C3
C3 VC_C2
C1 VC
T Board
C2 VC_C3
100.00 0
1.16E-3 1
C3 VC_C2
100.00 0
6.04E-4 1
C1 VC
100.00 0
4.1E-4 1
T Board
100.00 0
7.88E-4 1


11
2
10
3
8
1
4
9
5
7
6
$\mu_{10,11}$
$\mu_{11,1}$
$\mu_{2,3}$
$\lambda_{1,10}$
$\lambda_{1,2}$
$\mu_{3,1}$
$\lambda_{1,8}$
$\mu_{8,9}$
$\lambda_{1,4}$
$\mu_{9,1}$
$\mu_{5,1}$
$\mu_{4,5}$
$\mu_{7,1}$
$\lambda_{1,6}$
$\mu_{6,7}$


T
ETCS-2 on-board sub-system failure
M1
DMI failure
M2
BTM communication failure
M3
TIU failure
M4
BUS failure
M5
ETCS-2 control failure
CSP
HSP
HSP
HSP
X1
DMI1 failure
X1
DMI2 failure
BTM failure
TIU 1 failure
TIU 2 failure
BUS 1 failure
BUS 2 failure
RTM failure
M6
EURORADIO failure
M7
EVC failure
M8
CSP
X4
X4
X5
X5
HSP
HSP
HSP
X3
BTM ant failure
X6
X6
X7
X7
X8
X8
X2
BTM1 failure
X2
BTM2 failure
RTM 1 failure
RTM 2 failure
EURORADIO1 failure
EURORADIO 2 failure
EVC1 failure
EVC2 failure


Functionality
1.02
1
0.98
0.96
0.94
0.92
0.9
0.88
1799.5
1800


OnBoard
[End==1]
Waiting_OnBoard entry:OnBoard=0;
[Start==1]
tempo_OnBoard entry:OnBoard=3;
after(1,CLOCK)
Normal_OnBoard entry:OnBoard=3;
Calculation
SignalFromTrack [f>=900]
Receive
SignalFromTrain [f<900]
EndSendToTrain
Operation [operator==1]
EndOperation
Send
EndSendToTrack
OperationByOperator
Degraded_OnBoard entry:OnBoard=2;
Calculation
SignalFromTrack [f>=900]
Receive
EndSendToTrain
SignalFromTrain [f<900]
Operation [operator==0]
EndOperation [operator==0]
Send
EndSendToTrack
OperationByComputer
Operation [operator==1]
EndOperation [operator==0]
[(End==0) && (network_failed==1)]
ErrorTrain2Track [End==0]
ErrorTrack2Train [End==0]
[Cstate_OB==1&&operator==1]
[Cstate_OB==1&&operator==0]
ErrorTrack2Train [End==0]
epsilon0_ob
epsilon3_ob
epsilon1_ob
epsilon2_ob
Failed_OnBoard entry:OnBoard=1;
ErrorStateOfNet
CorrectState entry:Cstate_OB=1;
[network_failed==1]
RepairNet
ErrorState entry:Cstate_OB=0;
NoSend
NoReceive
Uncertainty_Onboard entry:OnBoard=4;
OrderOfErrorOfNet
CorrectOrder entry:Corder_OB=1;
ErrorTrain2Track
ErrorTrack2Train
NoSend_OnBoard entry:Corder_OB=0;
NoReceive_OnBoard entry:Corder_OB=0;
RepairSend_OB
RepairReceive_OB
NoSendNoReciev entry:Corder_OB=0;

Safety in Railway signaling system

HAZOP Study on the CTCS-3 Onboard System
Formal method for computer-based interlocking software
Multiformalism Modeling
Model-driven V&V assessment of railway control systems
A Markovian–Bayesian Network for Risk Analysis of High Speed and Conventional Railway Lines Integrating Human Errors
Bayesian Networks-Based Probabilistic Safety Analysis for Railway Lines
Using catastrophe theory to describe railway system safety
Cyber Security Analysis of the European Train Control System
Vulnerabilities analysis for cyber physical system (balise-based train control)

4. High-speed train collision analysis

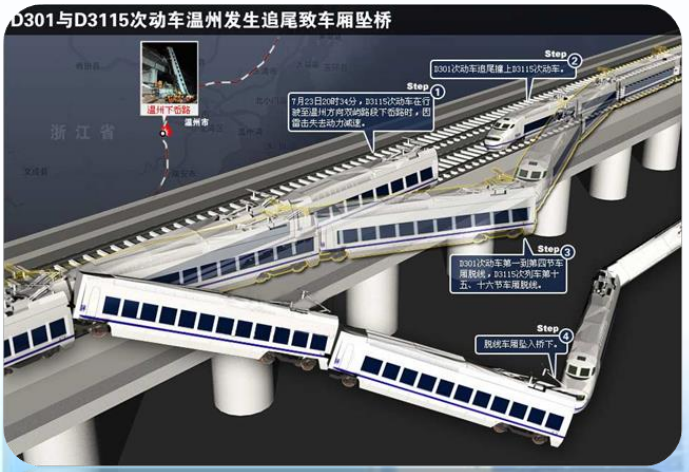
- Although HSRs have had only four fatal accidents in their 50-year history, three of them occurred over the past six years as HSR systems in operation have grown.

- Two types of train accident

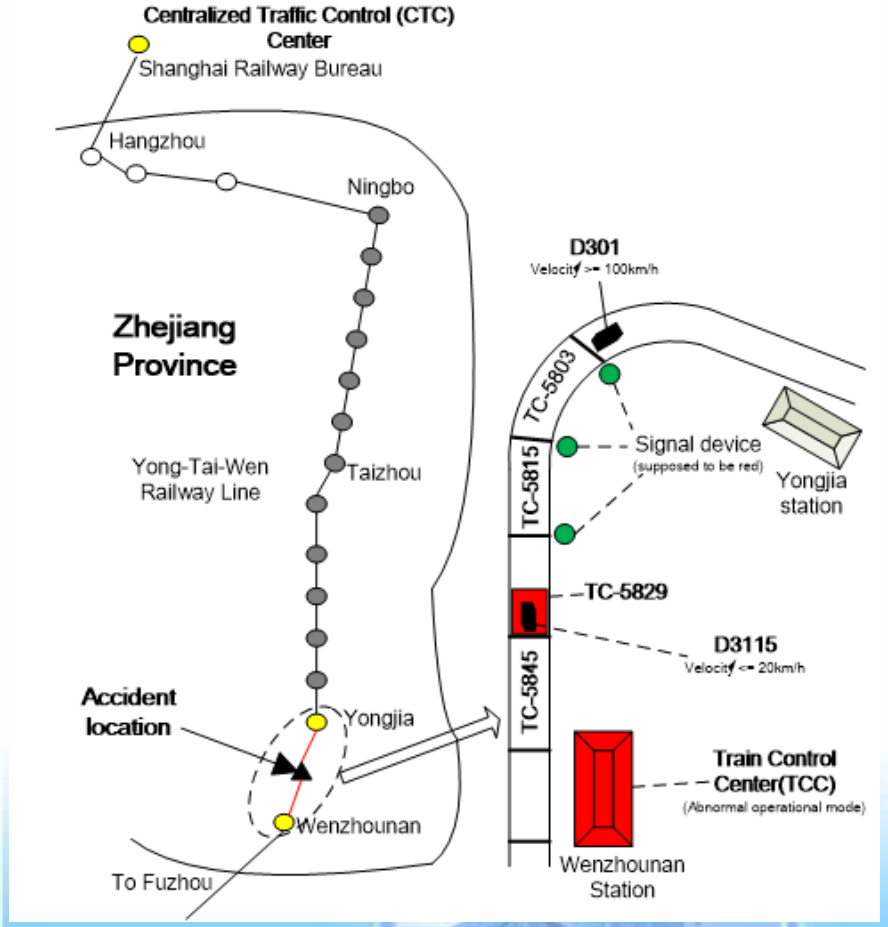
  train collision and derailment

110km/h over limited speed in Spain in 2013
80km/h over limited speed in France in 2015

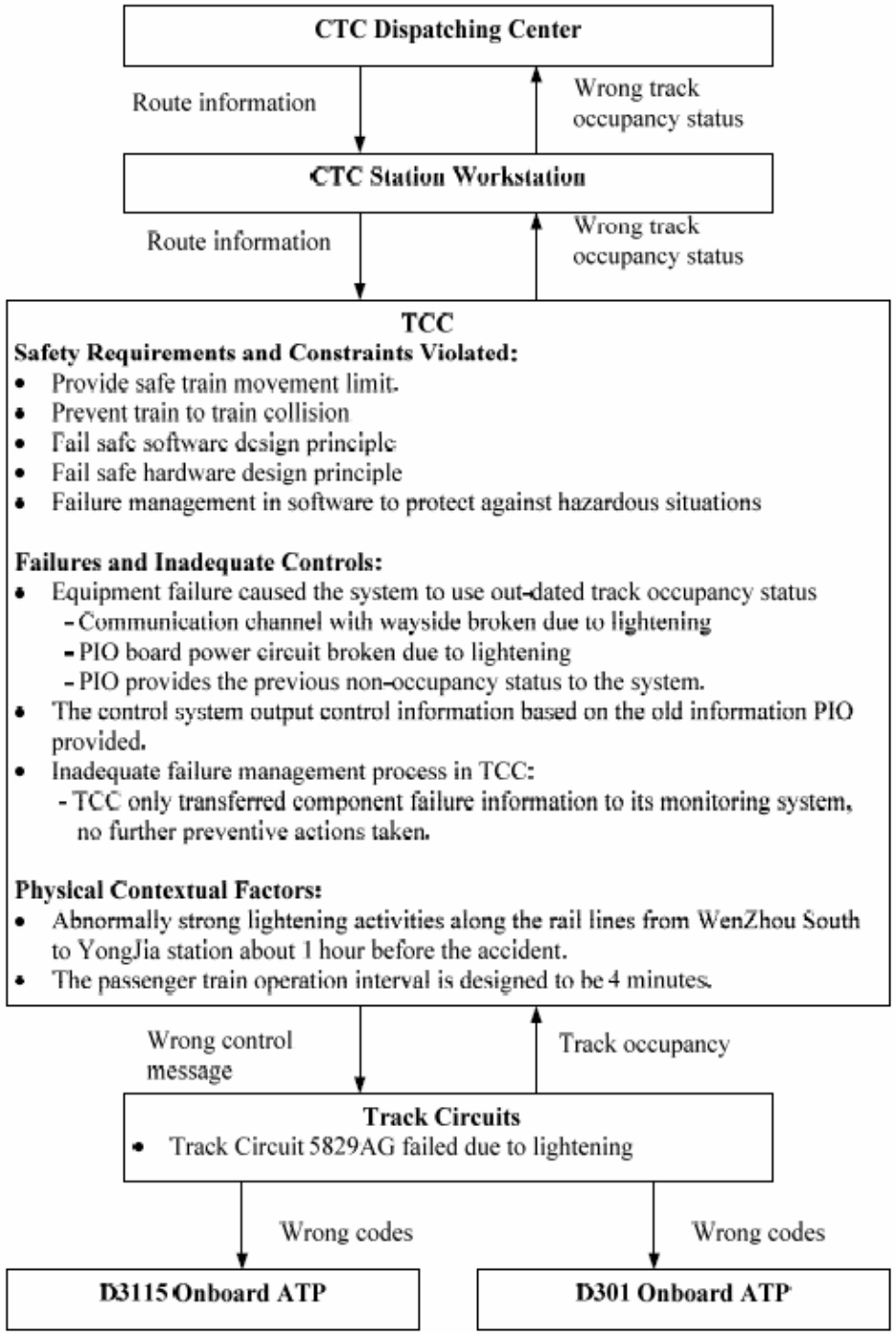
In 2011, a collision of two high speed trains occurred in Wenzhou, China, killing 40 passengers (Wenzhou train collision). A flaw in the signaling systems and several managerial problems were behind the tragedy

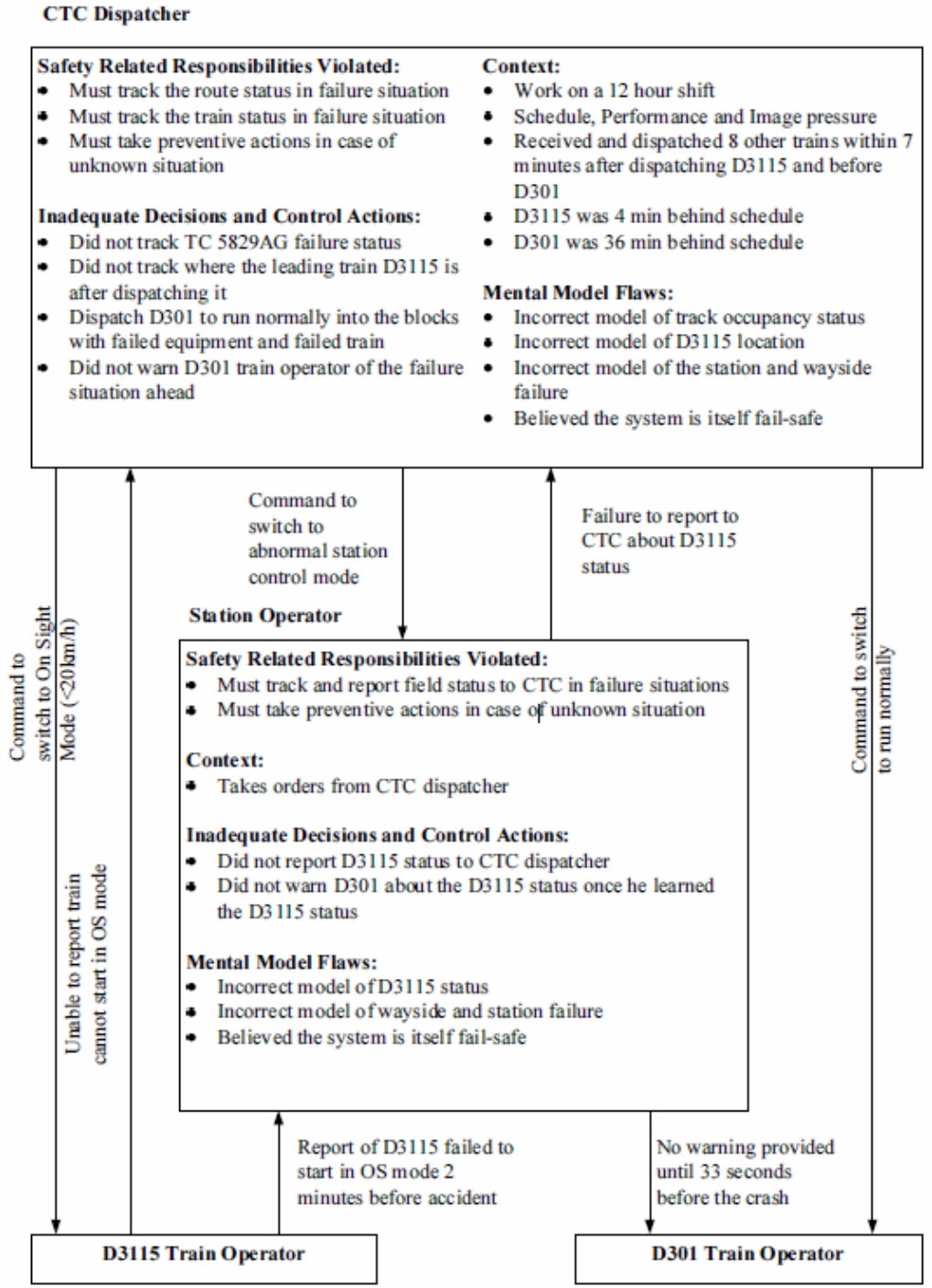


Analysis of Yong-Wen train collision



Time	Station operator	Dispatcher in CTC	The front train D3115	The following train D301
20:17		Ordered D3115 to transferred to On Sight mode (V<20km/h) if there is a red light in the interval		
20:21			Reached 5829AG and stopped automatically for the TC Failure. Failed to transfer to On Sight mode	
20:22	Failed to call D3115		Failed to call dispatcher and station operator	
20:24		Ordered D301 to leave		Left Yongjia Station
20:28			Failed to call dispatcher and station operator	
20:29			Transferred to on-sight mode successfully and restart	
20:30				D301 (90km/h) crashed into D3115 (16km/h)


CTC Dispatching Center
Route information
Wrong track occupancy status
CTC Station Workstation
Route information
Wrong track occupancy status
TCC
Safety Requirements and Constraints Violated:
• Provide safe train movement limit.
• Prevent train to train collision
• Fail safe software design principle
• Fail safe hardware design principle
• Failure management in software to protect against hazardous situations
Failures and Inadequate Controls:
• Equipment failure caused the system to use out-dated track occupancy status
- Communication channel with wayside broken due to lightening
- PIO board power circuit broken due to lightening
- PIO provides the previous non-occupancy status to the system.
• The control system output control information based on the old information PIO provided.
• Inadequate failure management process in TCC:
- TCC only transferred component failure information to its monitoring system, no further preventive actions taken.
Physical Contextual Factors:
• Abnormally strong lightening activities along the rail lines from WenZhou South to YongJia station about 1 hour before the accident.
• The passenger train operation interval is designed to be 4 minutes.
Wrong control message
Track occupancy
Track Circuits
• Track Circuit 5829AG failed due to lightening
Wrong codes
Wrong codes
D3115 Onboard ATP
D301 Onboard ATP


CTC Dispatcher
Safety Related Responsibilities Violated:
• Must track the route status in failure situation
• Must track the train status in failure situation
• Must take preventive actions in case of unknown situation
Inadequate Decisions and Control Actions:
• Did not track TC 5829AG failure status
• Did not track where the leading train D3115 is after dispatching it
• Dispatch D301 to run normally into the blocks with failed equipment and failed train
• Did not warn D301 train operator of the failure situation ahead
Context:
• Work on a 12 hour shift
• Schedule, Performance and Image pressure
• Received and dispatched 8 other trains within 7 minutes after dispatching D3115 and before D301
• D3115 was 4 min behind schedule
• D301 was 36 min behind schedule
Mental Model Flaws:
• Incorrect model of track occupancy status
• Incorrect model of D3115 location
• Incorrect model of the station and wayside failure
• Believed the system is itself fail-safe
Command to switch to abnormal station control mode
Failure to report to CTC about D3115 status
Station Operator
Command to switch to On Sight Mode (<20km/h)
Unable to report train cannot start in OS mode
Command to switch to run normally
Safety Related Responsibilities Violated:
• Must track and report field status to CTC in failure situations
• Must take preventive actions in case of unknown situation
Context:
• Takes orders from CTC dispatcher
Inadequate Decisions and Control Actions:
• Did not report D3115 status to CTC dispatcher
• Did not warn D301 about the D3115 status once he learned the D3115 status
Mental Model Flaws:
• Incorrect model of D3115 status
• Incorrect model of wayside and station failure
• Believed the system is itself fail-safe
Report of D3115 failed to start in OS mode 2 minutes before accident
No warning provided until 33 seconds before the crash
D3115 Train Operator
D301 Train Operator

Future research

- utilizing the field data to reliability analysis
- Bayesian Networks-Based Probabilistic Safety Analysis in railway signaling system

Reference:

1.Liu X, Saat MR, Barkan CPL. Freight-train derailment rates for railroad safety and risk analysis. *Accid Anal Prev*. 2017; 98: 1-9.

2.Ghosh S, Das A, Basak N, Dasgupta P, Katiyar A. Formal Methods for Validation and Test Point Prioritization in Railway Signaling Logic. *IEEE Trans Intell Transp Syst*. 2017; 18: 678-89.

3.de Bruin T, Verbert K, Babuska R. Railway Track Circuit Fault Diagnosis Using Recurrent Neural Networks. *IEEE Trans Neural Netw Learn Syst*. 2017; 28: 523-33.

4.Nakamura H. How to Deal with Revolutions in Train Control Systems. *Engineering*. 2016; 2: 380-6.

5.Madigan R, Golightly D, Madders R. Application of Human Factors Analysis and Classification System (HFACS) to UK rail safety of the line incidents. *Accid Anal Prev*. 2016; 97: 122-31.

6.Kubo N, Higuchi M, Takasu T, Yamamoto H, Ieee. Performance Evaluation of GNSS-based Railway Applications. *2015 International Association of Institutes of Navigation World Congress (Iain)*. 2015: 8.

7.Fort A, Mugnaini M, Vignoli V, Gaggii V, Pieralli M. Fault tolerant design of a field data modular readout architecture for railway applications. *Reliab Eng Syst Saf*. 2015; 142: 456-62.

8.Xie G, Liang YM, Qian FC, Hei XH, Ieee. Reliability Methodology and Theory for Development of Novel Railway Signalling Systems. *2014 33rd Chinese Control Conference*. New York: Ieee, 2014, p. 6461-4.

9.Casola V, Esposito M, Flammini F, Mazzocca N, Pragliola C. Performance Evaluation of Video Analytics for Surveillance On-Board Trains. In: BlancTalon J, Kasinski A, Philips W, Popescu D, Scheunders P, (eds.). *Advanced Concepts for Intelligent Vision Systems, Acivs 2013*. Berlin: Springer-Verlag Berlin, 2013, p. 414-25.

10.Wullems C. Towards the adoption of low-cost rail level crossing warning devices in regional areas of Australia: A review of current technologies and reliability issues. *Saf Sci*. 2011; 49: 1059-73.

11. Woo SW, O'Neal DL, Pecht M. Reliability design of residential sized refrigerators subjected to repetitive random vibration loads during rail transport. *Eng Fail Anal*. 2011; 18: 1322-32.

12.Flammini F, Vittorini V, Mazzocca N, Pragliola C. A Study on Multiformalism Modeling of Critical Infrastructures. In: Setola R, Geretshuber S, (eds.). *Critical Information Infrastructures Security*. Berlin: Springer-Verlag Berlin, 2009, p. 336-+.

13.Flammini F, Marrone S, Mazzocca N, Vittorini V. A new modeling approach to the safety evaluation of N-modular redundant computer systems in presence of imperfect maintenance. *Reliab Eng Syst Saf*. 2009; 94: 1422-32.

14.Panja SC, Ray PK. Reliability analysis of a 'Point-and-Point machine' of the Indian railway signaling system. *Qual Reliab Eng Int*. 2007; 23: 833-48.

15.Renpenning F. *Reliability prediction in railway signalling*. Godalming: Springer-Verlag London Ltd, 2004, p.2256-61.

Thank you!