轨道交通控制与安全
国家重点实验室(北京交通大学)
STATE KEY LAB OF RAIL TRAFFIC CONTROL & SAFETY

Using STAMP to Learn from Chinese High Speed Railway Accident

Professor Tang Tao; Dr Niu Ru
State Key Lab. of Railway Traffic Control and Safety
Beijing Jiaotong University, China

Outline

- Background
  - Background Chinese railway
  - Overview of the accident
  - The findings of government's investigation
- Interesting Problems met in further digging
  - Introduction of our work
  - The confusing results gain from event chain model
- Route causes analysis using STAMP
  - The reason we chose STAMP
  - The approach to analysis multi-modes system
  - Our finds from Wenzhou (accident 723)
- Conclusions

Chinese Railway

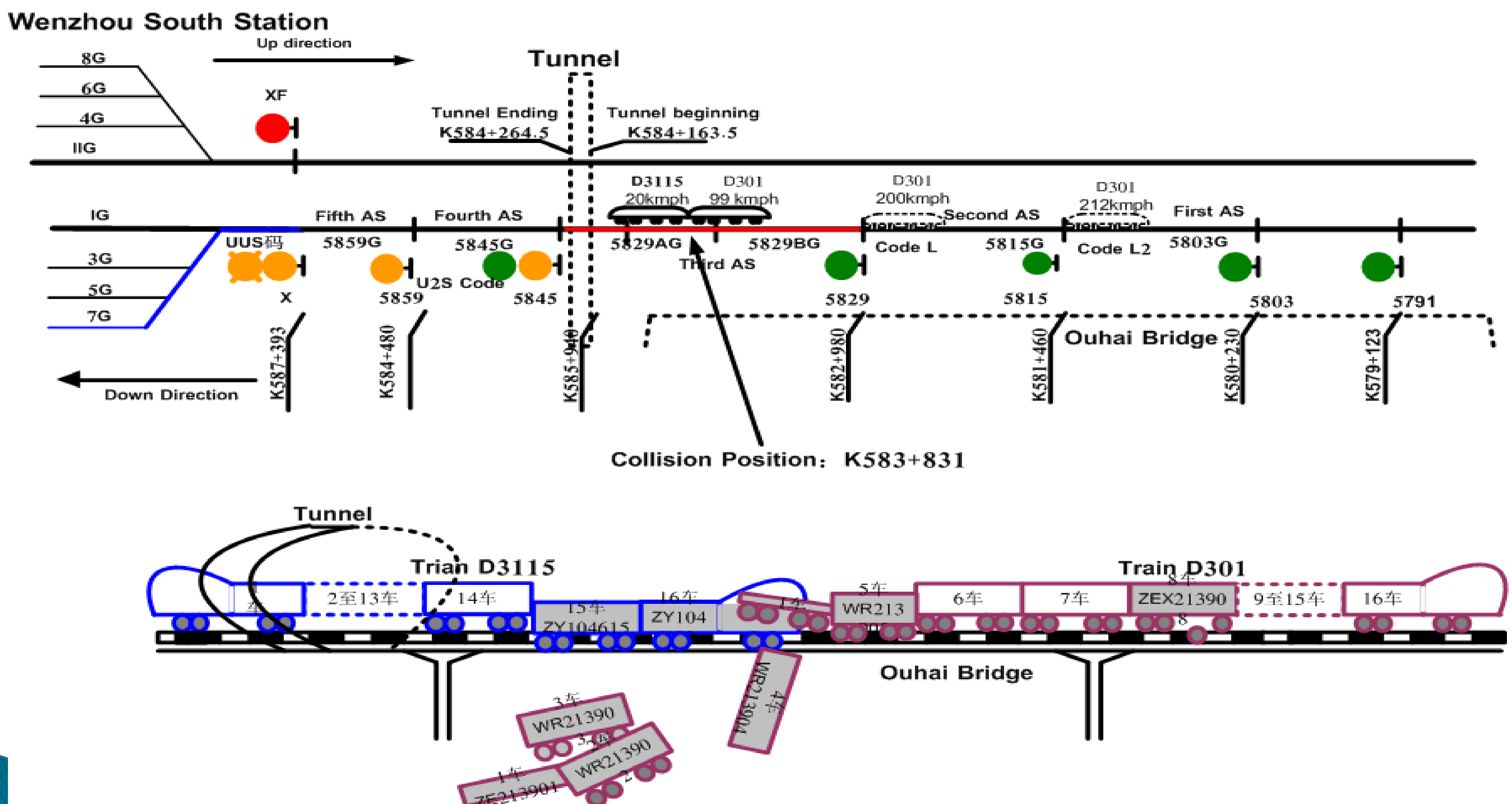
- "China has one of the biggest and busiest rail networks in the world, and trains link almost every town & city. Travelling by trains in China is a safe, comfortable & cheap way, and a Chinese train journey is an experience in itself."
- In railway industry, everyone knows that safety is as precious as life.
- Fact:
  - In 2011, 1.86226 billion people travelled by trains, and totally 961.23 billion passenger-km.
  - According to the statistic data in recent 10 years, Chinese railway is four times safer than Japan.

"Railway Statistical Bulletin for 2011". Ministry of Railway, People's Republic of China. Retrieved February 15, 2012, http://www.china-mor.gov.cn/zwzc/tjxx/zyzb/201202/t20120215_29645.html

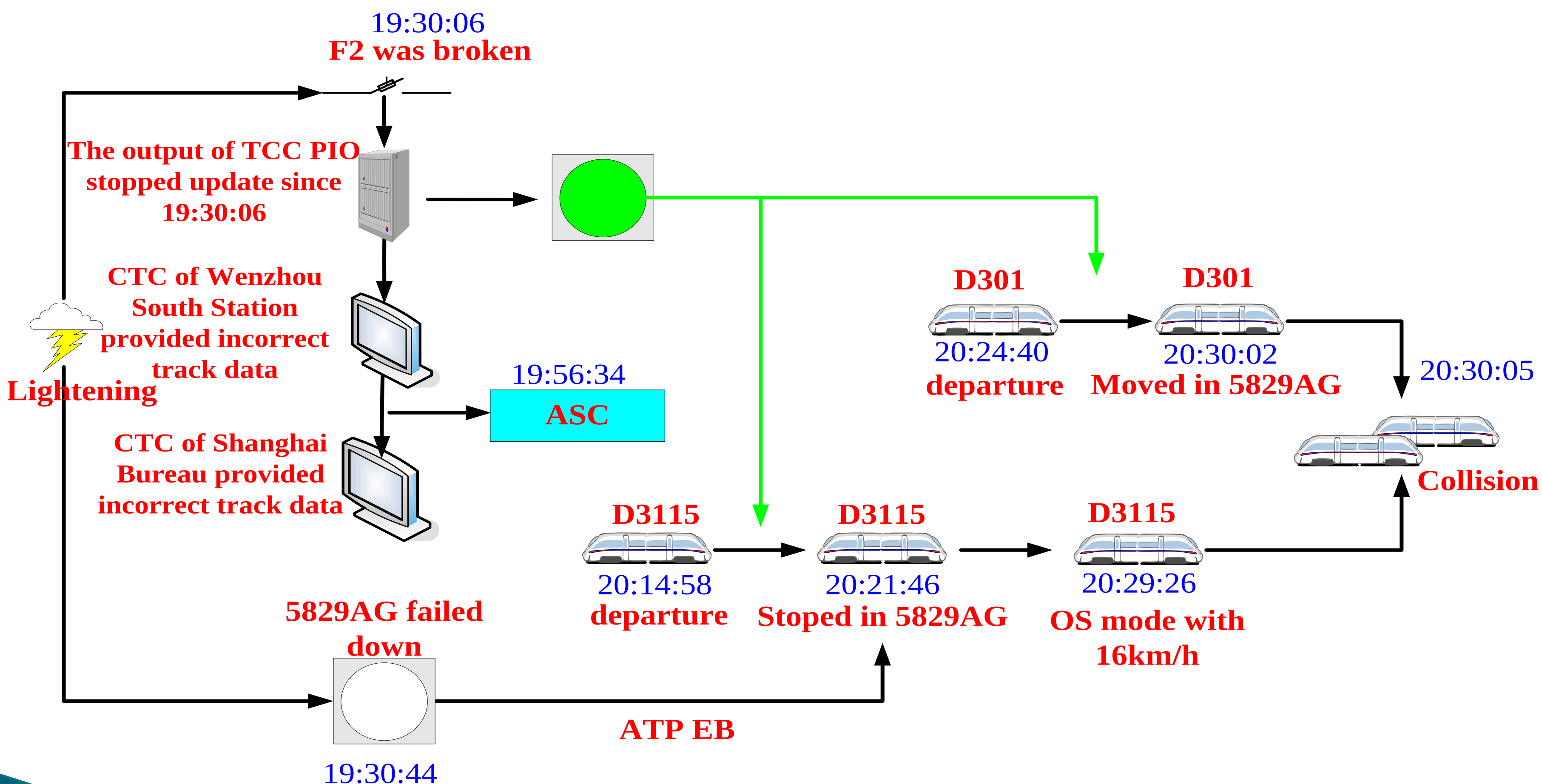
Chinese High-speed Railway Accident

- On the 23 July 2011 at 20:30:05
- Two EMU train in same direction collided together
- Cause 40 deaths, 172 injuries, interruption of traffic for 32 hours and 35 minutes

Chinese High-speed Railway Accident



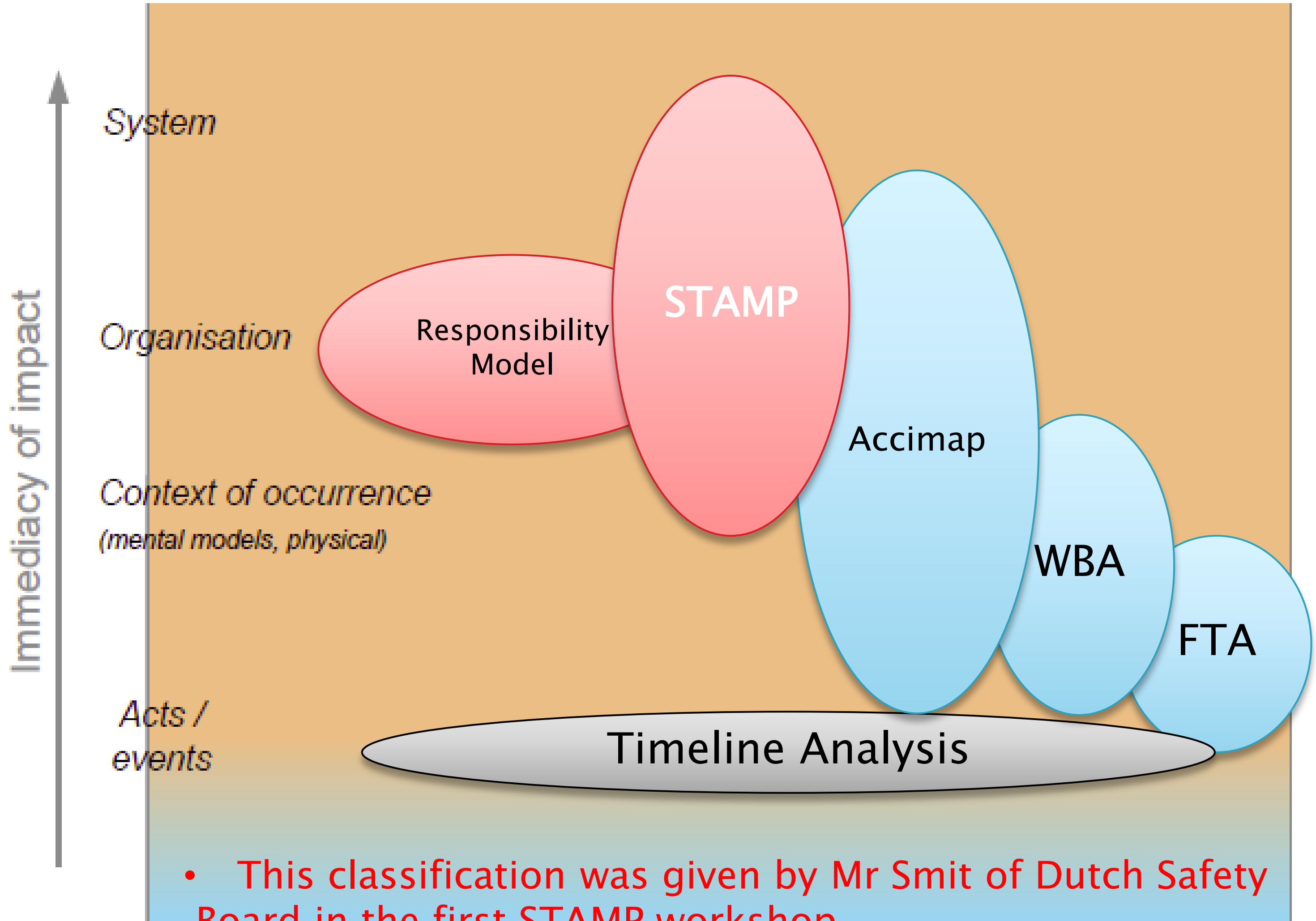
Chinese High-speed Railway Accident



Preliminary Investigation

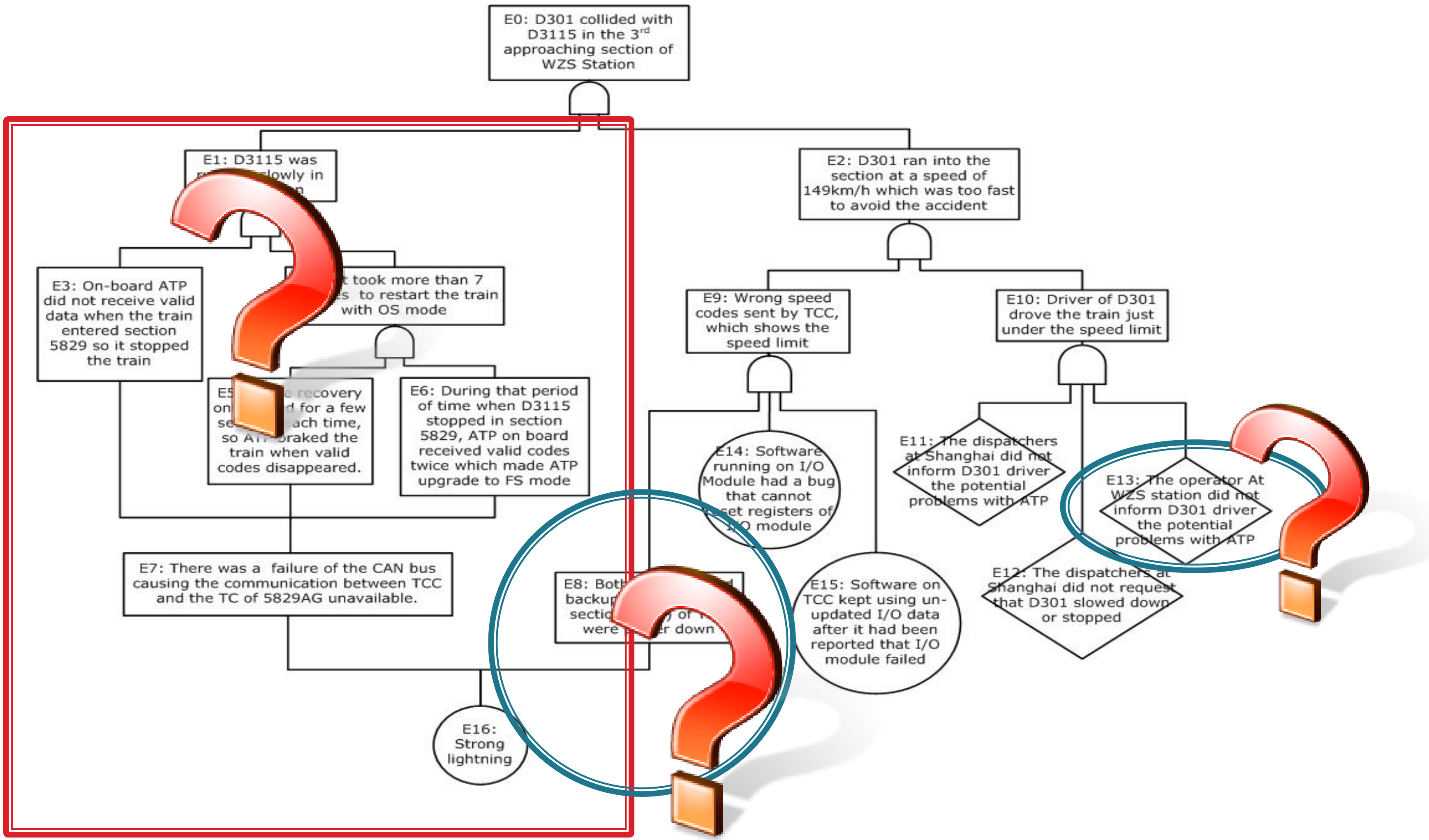
- The Chinese government's preliminary investigation published on Dec. 28th 2011 and concluded that there were
  - Systemic problems in the development of equipment
  - Organisational problems in the railway management authorities
    - Product approval process
    - Construction speed
  - Organisational problems in the railway operation
    - Safety culture
    - Training
    - Emergency disposal
    - Operation errors
  - And execute the personnel punishment as the first step.

Deep Digging of 7.23 Accident

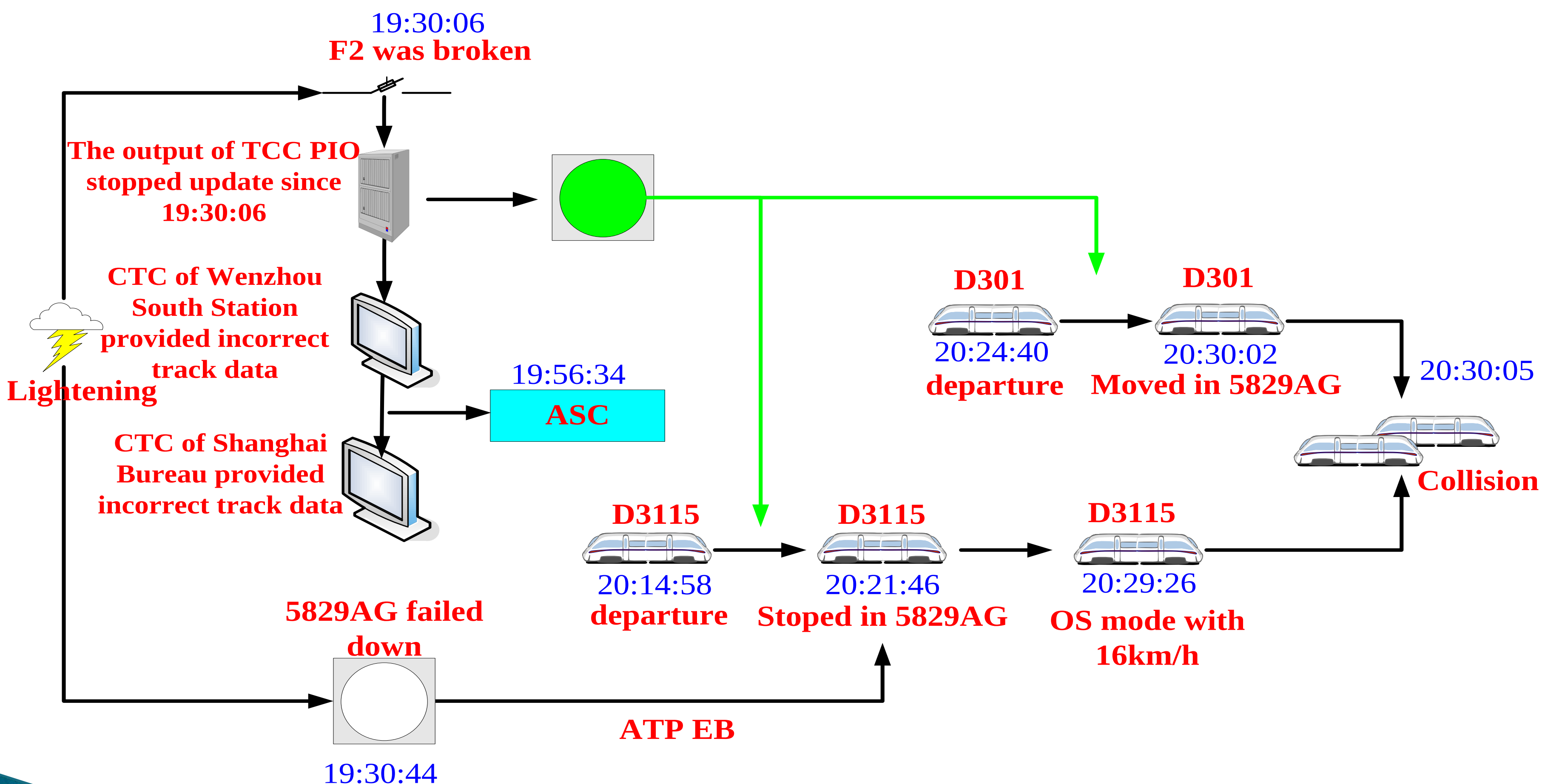


- This classification was given by Mr Smit of Dutch Safety Board in the first STAMP workshop

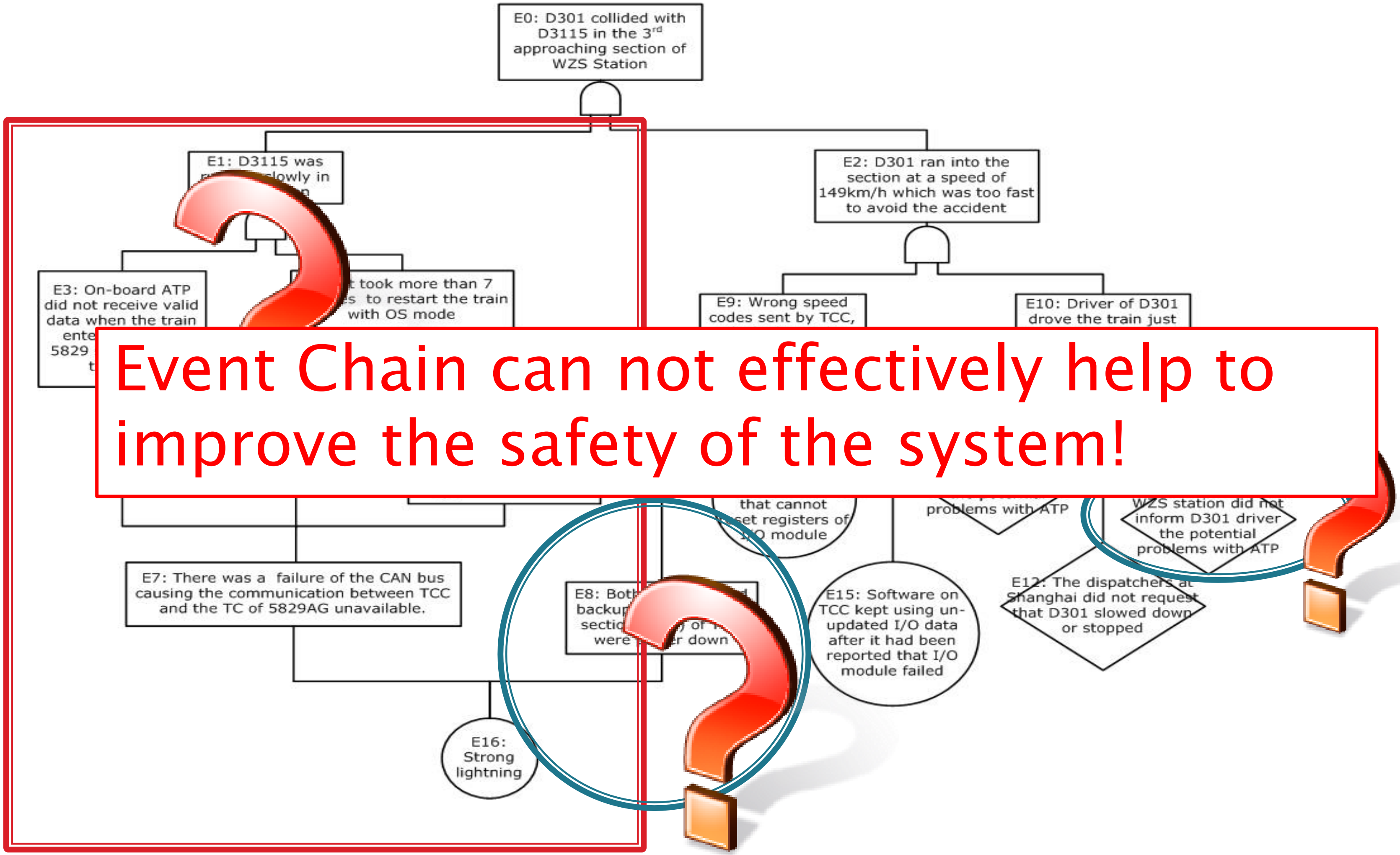
Analysis Results from Event Chain



Chinese High-speed Railway Accident



Analysis Results from Event Chain



Event Chain can not effectively help to improve the safety of the system!

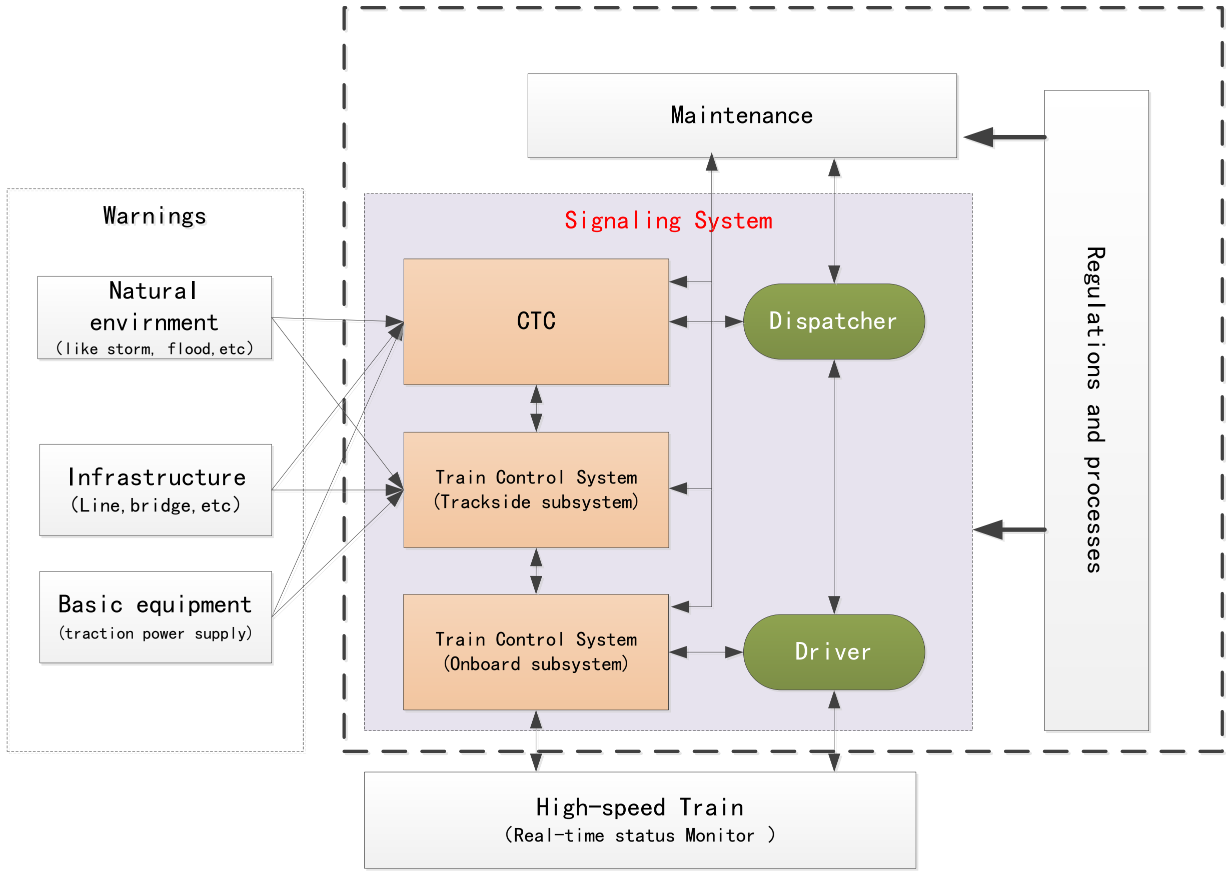
The reasons using STAMP

We found that STAMP is extremely useful when you want to make a “prescription” for a system

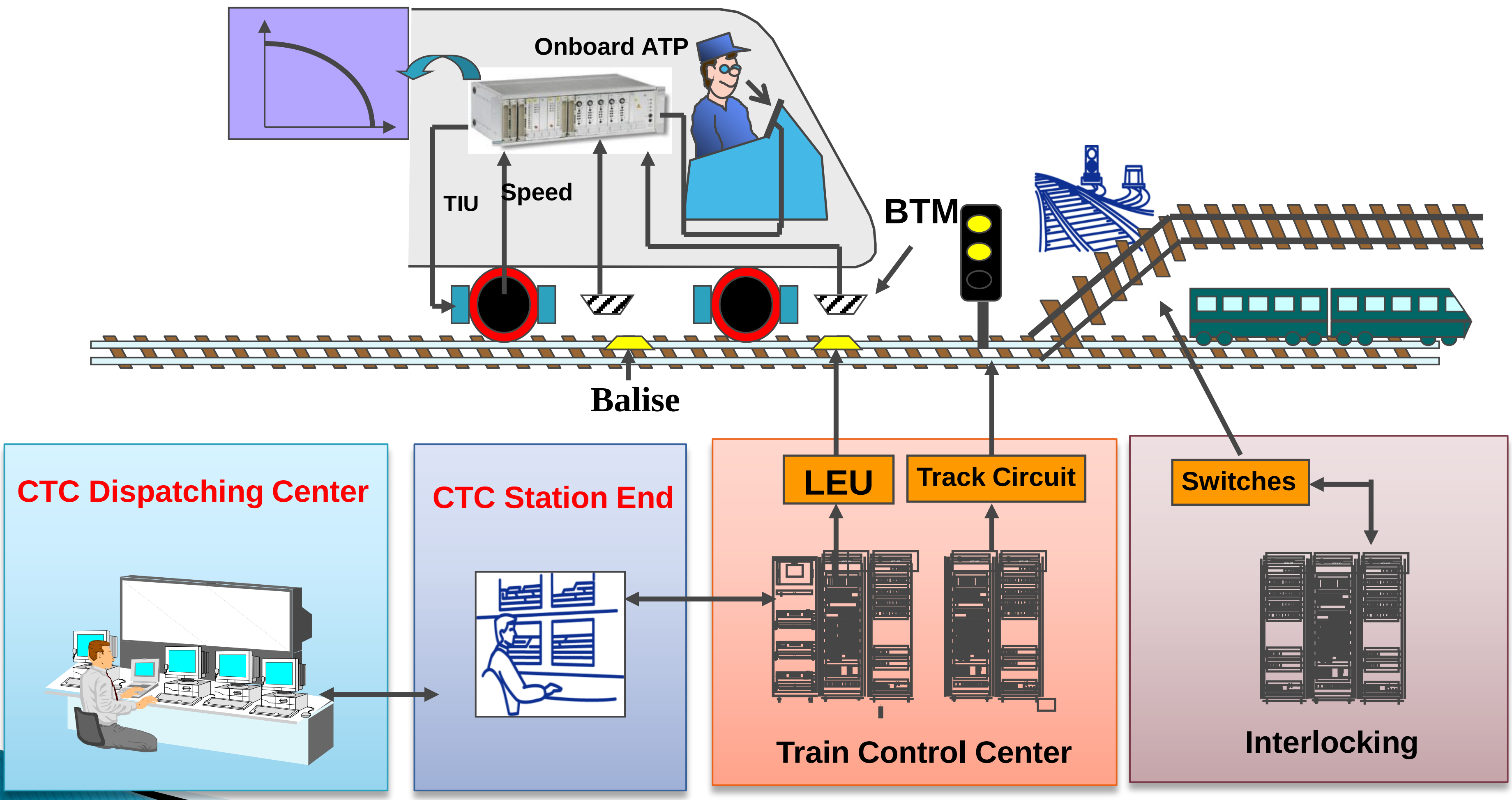
- Start from “hazards” not “Accident” itself;
- Based on the understanding of the defense model of the original system
  - Help to make the suggestions more practical
  - Help to improve the risk control system rather than rebuilt a new one
- Seamlessly and naturally connect technical parts with the organizational parts

Risk Control Structure of Railway System

- Mature Safety Protection architecture
  - Signaling system is the kernal
- Fail-safe based
  - STOP always is the safe side
- Design lots of backup schemes

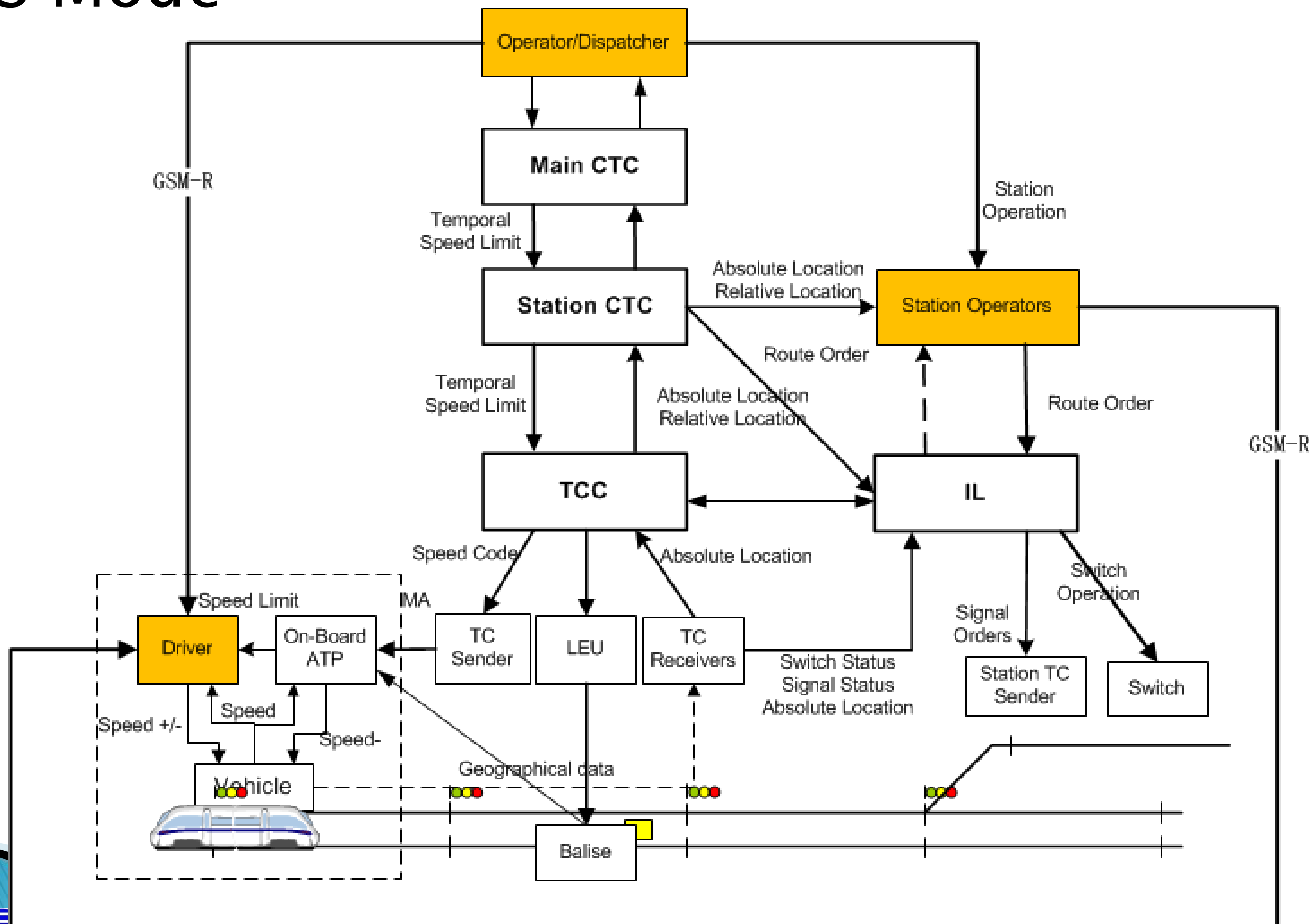


Signaling System Used in the Accident



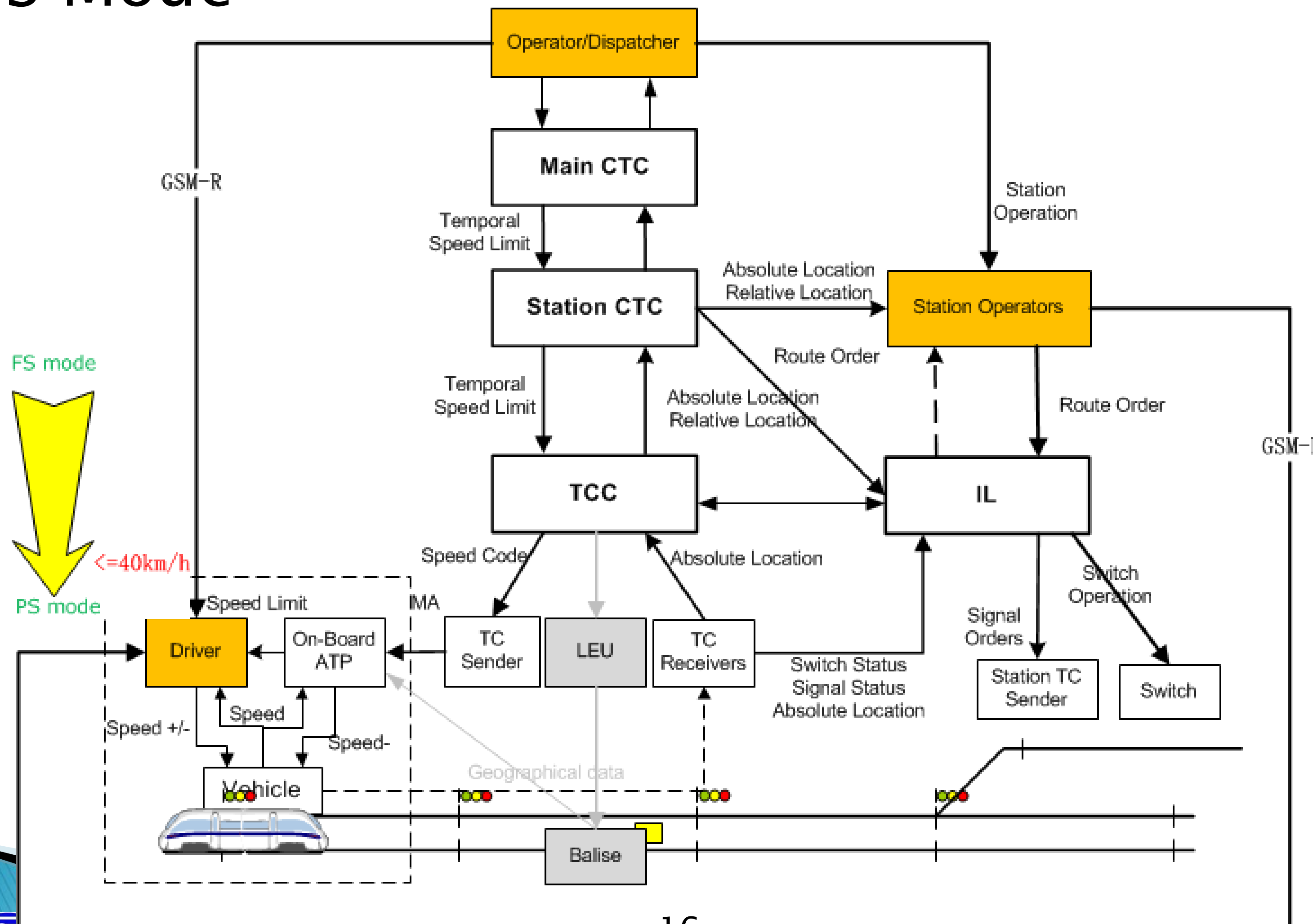
Defense-in-depth Design of CTCS-2

- FS Mode



Defense-in-depth Design of CTCS-2

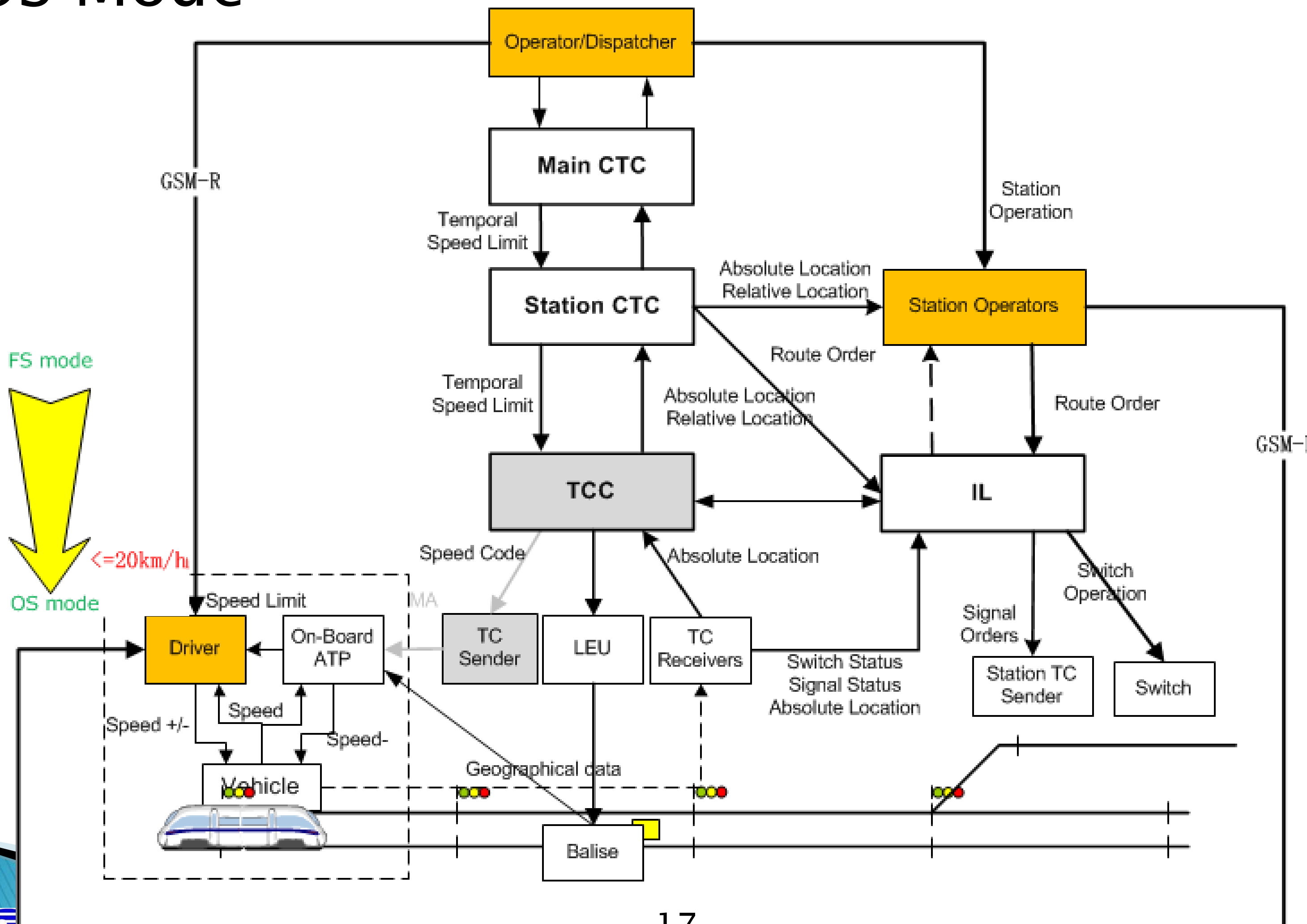
- PS Mode



RCS 国家重点实验室（北京交通大学）STATE KEY LAB OF RAIL TRAFFIC CONTROL & SAFETY
Beijing Jiaotong University

Defense-in-depth Design of CTCS-2

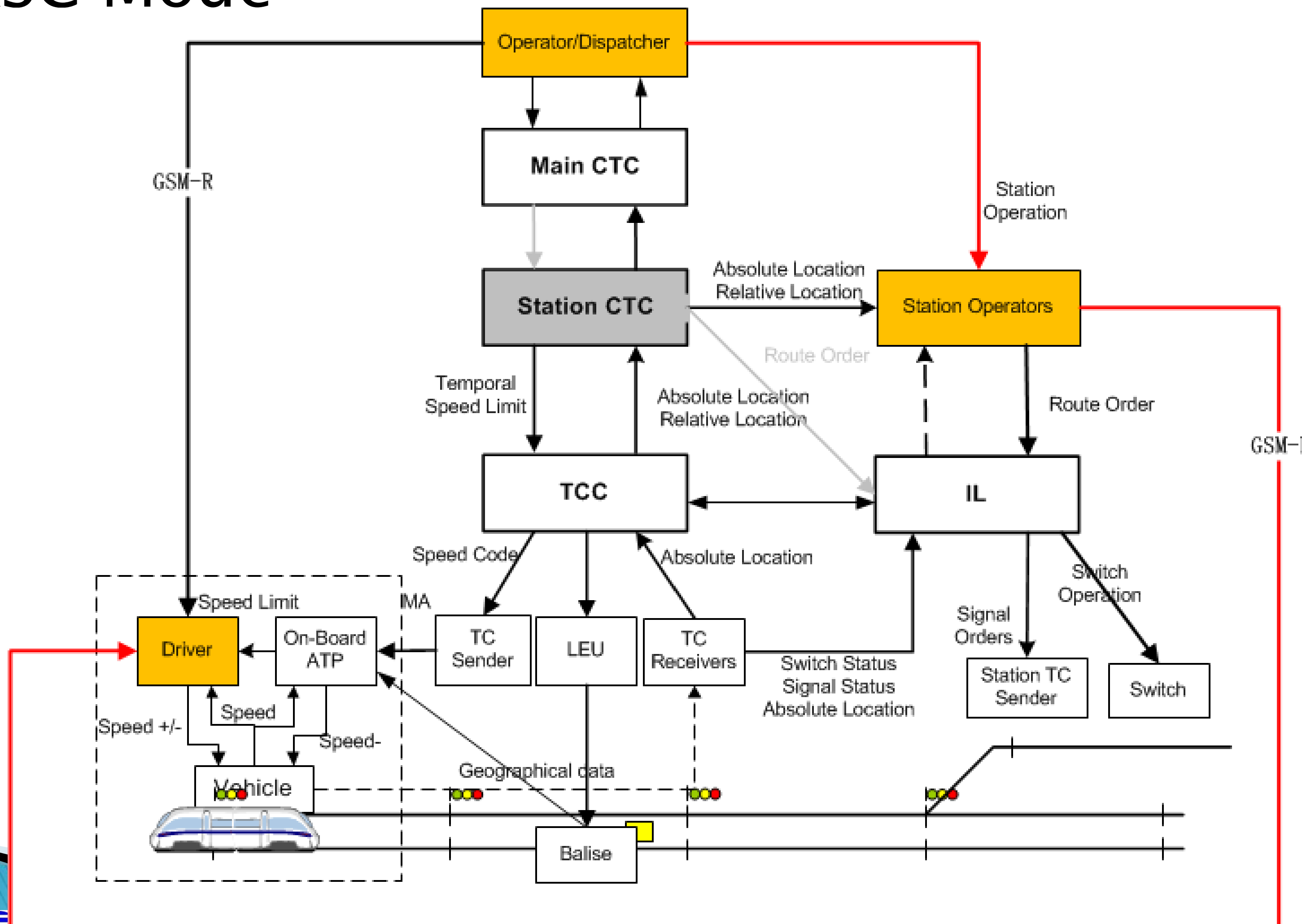
- OS Mode



RCS 国家重点实验室（北京交通大学） STATE KEY LAB OF RAIL TRAFFIC CONTROL & SAFETY
Beijing Jiaotong University

Defense-in-depth Design of CTCS-2

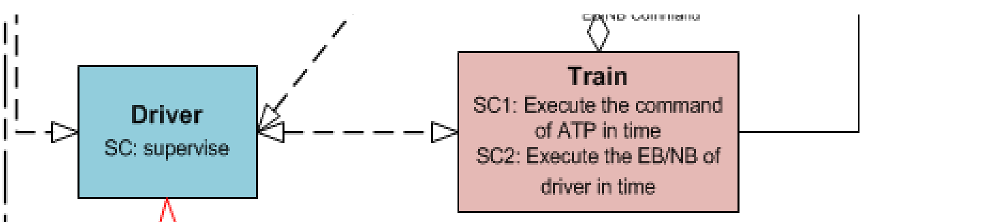
- ASC Mode



STAMP Models (1)

- Violations
  - TCC violate the SC, and generate unsafe MA;
  - The statuses of the section under control failed to update.

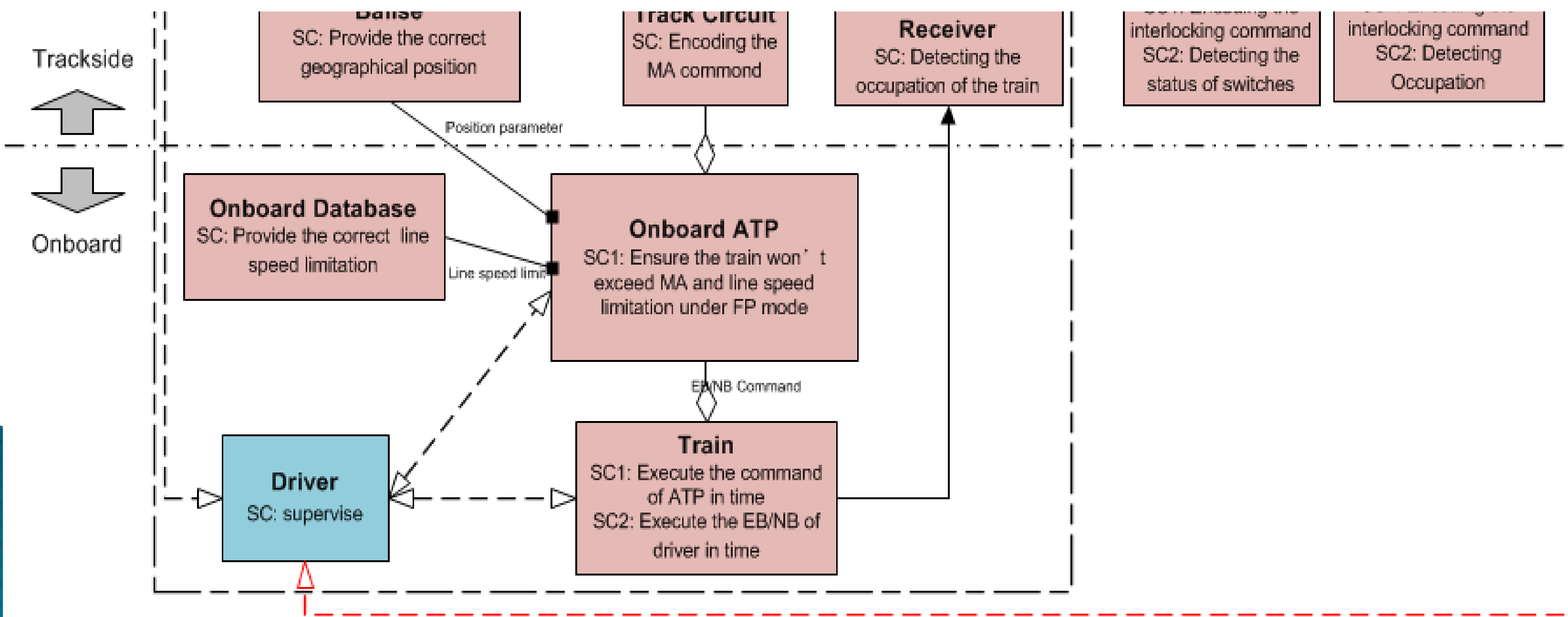
- So, SW error of TCC is the main reason of this accident.
- And, the power supply circuit obviously do not have the responsibility to ensure any of these two SCs.
- The GSM-R communication are not hazard control channels.



g University

- Violation
  - The statuses of the section under control failed to update.

- Still, the same sw error…, which shows degreed to ASC mode was a improper decision.

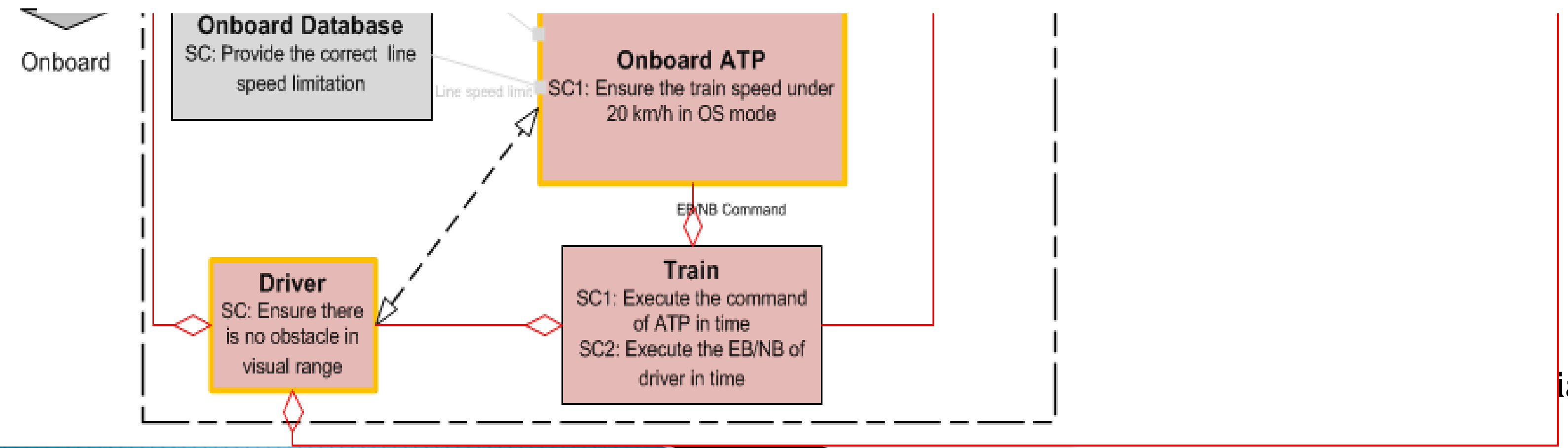


STAMP Models (2)

STAMP Models (3)

- Violation
  - None!!

- So, D3115(front train) failed to move out 5829AG in time is a misunderstanding of the accident, and any improvement suggestions resulted from this are not practical.
- And, even now, there is no SC for the QoS of GSM-R Channels.



- Suggestions:
  - More dependable diagnosis process should be used
    - Add TCCs handover checking
    - Add warning function in CTC to inform the dispatchers
    - Add consistency checking function of IL and TCC route data. (too complex to carry out)
  - Give more training to maintainers to explicit the signaling system is not absolutely fail-safe any more.
  - Redefine the emergency trigger scheme.

- There are four existing diagnosis processes can be use in this accident:

a) Maintenance may find out TCC was down and apply Emergence Disposal
b) Dispatcher may find out when train missing on CTC screen
c) Watchman may find out the inconsistency of CTC and IL when D3115 moved in
d) The driver of D301 may find out if the dispatcher inform him about TC failures

- Time lags and measurement inaccuracies not accounted for
  - Lack of time constrain of maintenance

Conclusion

- Accident analysis should based on the existing safety assurance model of the system.
- With the help of STAMP, we found the valid causes of 7.23 Accident, proved the effectiveness of these causes and clarified several common misunderstandings.
- We show an approach to analysis multi-mode system with STAMP. And we found two more causes of the accident.

Thank you!