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
“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.

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

19:30:06
F2 was broken

The output of TCC PIO stopped update since 19:30:06

Lightening

CTC of Wenzhou South Station provided incorrect track data

CTC of Shanghai Bureau provided incorrect track data

19:56:34
ASC

5829AG failed down

19:30:44
ATP EB

D3115
20:14:58 departure
Stoped in 5829AG

D3115
20:21:46

D301
20:24:40 departure
Moved in 5829AG

D301
20:30:02

D301
20:30:05

Collision

5829AG

20:29:26
OS mode with 16km/h

D301
20:30:02

Movement in 5829AG

D301
20:30:05

Collision
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

E0: D301 collided with D3115 in the 3rd approaching section of W25 Station

E1: D3115 was moving slowly in the section

E2: D301 ran into the section at a speed of 149 km/h, which was too fast to avoid the accident

E3: On-board ATP did not receive valid data when the train entered section S829, so it stopped the train

E4: ATP recovered on-board ATP for a few seconds each time, so ATP braked the train when valid codes disappeared.

E5: It took more than 7 s to restart the train with OS mode

E6: During that period of time when D3115 stopped in section S829, ATP on board received valid codes twice which made ATP upgrade to PS mode.

E7: There was a failure of the CAN bus causing the communication between TCC and the TC of S829AG unavailable.

E8: Both backup sections of TCC were shut down.

E9: Wrong speed codes sent by TCC, which shows the speed limit

E10: Driver of D301 drove the train just under the speed limit

E11: The dispatchers at Shanghai did not inform D301 driver the potential problems with ATP

E12: The dispatchers at Shanghai did not request that D301 slowed down or stopped

E13: The operator at W25 station did not inform D301 driver the potential problems with ATP

E14: Software running on I/O Module had a bug that cannot reset registers of I/O module

E15: Software on TCC kept using un-updated I/O data after it had been reported that I/O module failed

E16: Strong lightning

Beijing Jiaotong University
Chinese High-speed Railway Accident

The output of TCC PIO stopped update since 19:30:06

Lightening

CTC of Wenzhou South Station provided incorrect track data

CTC of Shanghai Bureau provided incorrect track data

5829AG failed down

19:30:06 F2 was broken

19:30:44 ATP EB

19:56:34 ASC

D3115
20:14:58 departure

D3115
20:21:46 Stopped in 5829AG

D301
20:24:40 departure

D301
20:30:02 Moved in 5829AG

20:30:05 Collision

20:29:26 OS mode with 16km/h

20:30:44
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 kernel
- Fail-safe based
  - STOP always is the safe side
- Design lots of backup schemes
Signaling System Used in the Accident

- CTC Dispatching Center
- CTC Station End
- LEU
- Track Circuit
- Train Control Center
- Interlocking
- Switches
- Onboard ATP
- TIU
- Speed
- BTM
- Balise
- CTC Station End
- LEU
- Track Circuit
- Train Control Center
- Interlocking
- Switches
Defense-in-depth Design of CTCS–2

- FS Mode
Defense-in-depth Design of CTCS-2

- PS Mode
Defense-in-depth Design of CTCS-2

- OS Mode
Defense-in-depth Design of CTCS-2

- ASC Mode
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.
Violation

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

- Still, the same sw error..., which shows degree to ASC mode was a improper decision.
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 be based on the existing safety assurance model of the system.
- With the help of STAMP, we found the valid causes of the 7.23 Accident, proved the effectiveness of these causes and clarified several common misunderstandings.
- We show an approach to analyzing a multi-mode system with STAMP. And we found two more causes of the accident.
Thank you!