Using STAMP to analysis Chinese High Speed Railway Accident
--7.23 Yong-wen Railway Accident

Lecturer: Li Chenling, Ph.D. candidate
State Key Lab. of Rail Traffic Control and Safety
Beijing Jiaotong University, China
Outline

- Motivation
  - Experience of 7.23 accident analysis using STAMP
  - Chinese railway system

- Some ideas about using CAST in operational and physical level
  - Show the dynamic

- 7.23 Yong-Wen railway Accident Analysis
  - Analysis

- Conclusions
Outline

- **Motivation**
  - Experience of 7.23 accident analysis using STAMP
  - Chinese railway system

- Some ideas about using CAST in operational and physical level
  - Show the dynamic

- 7.23 Yong-Wen railway Accident Analysis
  - Analysis

- Conclusions
On 23rd July 2011 at 20:30:05
- Two CRH train in same direction collided together
- Cause 40 deaths, 172 injures, interruption of traffic for 32 hours and 35 minutes
Risk Control Structure of Chinese Railway System

- Safety Protection architecture
  - Safety of High-speed train is the goal

- Human is the backup scheme of technical system

Accidents will happen when the gap between the two kinds of responsibilities appears.
Experience

- Application of CAST and STPA to railroad safety in China [Dong Airong, MIT, MSc thesis, 2012]
  - Did not consider the change of control structure in the operational level
  - Every component related
  - Component’s roles and responsibilities

- A system theoretic analysis of the “7.23” Yong-tai-wen railway accident [Suo Dajiang, STAMP workshop 2012]
  - Did not analyze the change of Component’s roles and responsibilities
  - Did not give a method to show the process clearly.

- Using STAMP to learn from Chinese High speed railway accident [Tang Tao & Niu Ru, STAMP workshop 2013]
  - Did not give a method to show the process clearly.
CAST

- Based on a Static structure
- Only using text to create scenarios

So, we should use a dynamic view to analyze an accident.

System was dynamic in the occurrence of an accident happened.

Control structure kept changing.

Control structure was also a kind of important context for accident investigation.

So, we should use a dynamic view to analyze an accident.
Outline

➢ Background & Motivation
  ● Experience of 7.23 accident analysis using STAMP
  ● Chinese railway system

➢ Some ideas about using CAST in operational and physical level
  ● Show the dynamic

➢ 7.23 Yong-Wen railway Accident Analysis
  ● Analysis

➢ Conclusions
Operational and Physical level

System state from S0 to S1, then to S2, eventually to A (accident happened)

- Control structure and roles & responsibilities
- Rules & Regulations
- Actual Action
- System state from S0 to S1, then to S2, eventually to A (accident happened)

Roles & Resp.

Violated Reqs. & Cons. & mental mode or process mode flaws

Control structure
Using CAST

- **Step 1**: Select Events and determine states and the controllers
- **Step 2**: Determine Rules and Regulations related to Operational and Physical level
- **Step 3**: Obtain the requirements and responsibilities violated and the mental mode or process mode flaws in each change
- **Step 4**: Obtain each controller’s flaws
Outline

➢ Background & Motivation
  ● Experience of 7.23 accident analysis using STAMP
  ● Chinese railway system

➢ Some ideas about using CAST in operational and physical level

➢ 7.23 Yong-Wen railway Accident Analysis
  ● Analysis

➢ Conclusions
Signaling System Used in the Accident
Operational and Physical Level

CTC Dipatcher
- TSR Setting
- Routing
- Status Display

Station Operator
- Status Display

CTC Station Workstation
- TSR Setting
- Route Status
- Block Status
- Track Circuit occupancy Status
- Signal Status

TCC
- Signal Control
- Block Signal
- Track Circuit Coding
- TC Status
- Balise Messaging
- Balise Status

Train Operator
- Signal Display
- Operation Mode
- Overspeed
- Alarm
- Movement Authority Limit
- Line Param

Onboard ATP System
- Speed Limits
- Occupancy Status Ahead

Train Subsystem
- Propulsion
- Brake
- Train Speed
- Cab Signal
- Mode Selection
- Brake Status
Step 1a: Determine the controllers

- Roles
- Responsibilities

Step 1: Select Events and determine states and the controllers.

Step 2: Determine Rules and Regulations related to Operational and Physical level

Step 3: Obtain the requirements and responsibilities violated and the mental mode or process mode flaws in each change

Step 4: Obtain each controller’s description with flaws
Step1b: Select Events

Step1: Select Events and determine states and the controllers.

Step2: Determine Rules and Regulations related to Operational and Physical level

Step3: Obtain the requirements and responsibilities violated and the mental mode or process mode flaws in each change

Step4: Obtain each controller’s description with flaws
Step 1c: Determine states

Step 1: Select Events and determine states and the controllers.

Step 2: Determine Rules and Regulations related to Operational and Physical level

Step 3: Obtain the requirements and responsibilities violated and the mental mode or process mode flaws in each change

Step 4: Obtain each controller’s description with flaws
Steps 2: Related Rules and Regulations

1. Regulation of railway technical operation [2007]

2. Railway transportation dispatching rules [2008]

3. Measures for the administration of railway passenger dedicated line [2009]

4. High-speed railway dispatching rules [2009]

5. Shanghai railway traffic organization rules [2007]

6. Joint control of train for Driver and Station worker [2009]
Step3  S0: Normal state

- **Step1:** Select Events and determine states and the controllers.

- **Step2:** Determine Rules and Regulations related to Operational and Physical level

- **Step3:** Obtain the requirements and responsibilities violated and the mental mode or process mode flaws in each change

- **Step4:** Obtain each controller’s description with flaws

**Des**
Monitor stations status (Route Status)[From CTC system]
Step 3  Control structure change

ASC (Regulation Req.)

Normal
Step 3  Roles and responsibilities change

**Dispatcher**
- **Role:** Controller
- **Safety Responsibilities (Requirements):**
  - Monitor traffic conditions in the sections between railway stations (Train status & Line Status) [From CTC system]
  - Monitor stations status (Route Status) [From CTC system]
  - Issue dispatching command [To TCC and CI by CTC system]
  - Get emergency information [From Train driver & Station watcher by GSM-R]

**Station Watcher**
- **Role:** Supervisor
- **Safety Responsibilities (Requirements):**
  - Monitor station status [From CTC TCC CI system]
  - Report emergency information [To Dispatcher by GSM-R]

**Onboard System (ATP)**
- **Role:** Controller
- **Safety Responsibilities (Requirements):**
  - Perform calculation of the control profile based on the data [From TC] and automatically control the train
  - Stop the Train when it receives abnormal or no signal [From TC]
  - Show Train operation status [To Driver by DMI]
  - Overspeed Alarm [To Driver]

**Train**
- **Brake**
- **Propulsion**
- **Cab Signal**

**GSM-R**
- **Operation Mode**
- **Overspeed Alarm**
- **Brake**
- **Propulsion**

**CTC**
- **Operation plan**
- **Status Display**

**MA, TC data**
- **TC status**
- **Get TSR information [From CTC]**

**Station Watcher**
- **Role:** Supervisor
- **Safety Responsibilities (Requirements):**
  - Monitor station status [From CTC TCC CI system]
  - Report emergency information [To Dispatcher by GSM-R]

**Dispatcher**
- **Role:** Controller
- **Safety Responsibilities (Requirements):**
  - Monitor traffic conditions in the sections between railway stations (Train status & Line Status) [From CTC system]
  - Monitor stations status (Route Status) [From CTC system]
  - Issue dispatching command [To TCC and CI by CTC system]
  - Get emergency information [From Train driver & Station watcher by GSM-R]
Step 3  Controllers actions after change

- Controllers’ actual actions

- Dispatcher gives orders to D3115 train Driver
Step 3  S1: Actual ASC

Dispatcher gives orders to D3115 train Driver [DA1]

- **Dispatcher**
  - Role: Controller
  - Safety Responsibilities (Requirements):
    - Monitor traffic conditions in the sections between railway stations (Train status & Line Status) [From Station Watcher]
    - Monitor status (Route Status) [From Station Watcher]
    - Issue dispatching command [To Station Watcher]
    - Get emergency information [From Train driver & Station watch by GSM-R]
  - Safety Responsibilities & Constraints (Requirements):
    - Issue dispatching order to Station watcher only
  - Mental mode flaws:
    - Station watcher should send the line information to train driver in the ASC mode

- **Station Watcher**
  - Role: Controller
  - Safety Responsibilities (Requirements):
    - Monitor station status [From TCC CI system]
    - Monitor Train status [From Train driver by GSM-R]
    - Report emergency information [To Dispatcher by GSM-R]
  - Safety Responsibilities & Constraints (Requirements):
    - Issue dispatching order to Train driver in time
    - Station watcher should send the line information to train driver in the ASC mode
  - Mental mode flaws:
    - Station watcher should send the line information to train driver in the ASC mode

- **Train Driver**
  - Role: Controller
  - Safety Responsibilities (Requirements):
    - Monitor ATP & Train status [From DMI]
    - Selection ATP operation mode [To ATP by MDI]
    - Give out Propulsion & Brake [To Train by Trig]
    - Report emergency information [To Dispatcher by GSM-R]
    - Get Section information and Route information [To Dispatcher by GSM-R] and to keep train safe
  - Operation Mode Overspeed Alarm
    - Propulsion Brake Cab Signal

- **Onboard System (ATP)**
  - Role: Controller
  - Safety Responsibilities (Requirements):
    - Perform calculation of the control profile based on the data [From TC] and automatically control the train
    - Stop the Train when it receives abnormal or no signal [From TC]
    - Show Train operation status [To Driver by DMI]
    - Overspeed Alarm [To Driver]
  - MA, TC data
  - Safety Responsibilities & Constraints (Requirements):
    - From TC
  - TC status

- **TCC**
  - Role: Controller
  - Safety Responsibilities (Requirements):
    - Track the section status between two stations [From TC]
    - Encode signal [To TC] and give the movement authority to the Train [by TC]
    - Control the signal light [To signal light]
    - Give alarm for emergency information [To Station Watcher]
    - Get TSR information [From Station Watcher]
  - MA, TC data
  - Status Display

- **Train**
  - Brake status

- **MA, TC data**
Step 1: Select Events and determine states and the controllers.

Step 2: Determine Rules and Regulations related to Operational and Physical level

Step 3: Obtain the requirements and responsibilities violated and the mental mode or process mode flaws in each change

Step 4: Obtain each controller’s description with flaws

Safety Related Responsibilities:
- Must track the route
- Must track the train
- Must take preventive action in the situation

Inadequate Decisions:
- Did not track TC 587
- Did not track TC 301
- Did not warn D301 train operator of the failure situation ahead

Requirements:
- Correct model of the station and lineside fail-safe
- Must not dispatch trains in a way that could lead to a train to train collision

Constraints:
- Must not dispatch trains in a way that could lead to a train to train collision
- Must not dispatch trains in a way that could lead to a train to train collision
- Must not dispatch trains in a way that could lead to a train to train collision

Additional notes:
- Unresolved system failures
- Emergency situations

Train operator description:
- Incorrect model of the station and lineside failure
- Believed the system is itself fail-safe
New Flaws

- Dispatcher gives an order to D301 train driver order under ASC mode [Control dysfunction]

- The failure of joint control mechanism between Wenzhounan Station watcher and D301 train driver [Control dysfunction]

- Dispatcher order in ASC mode & the incompletion Rules& Regulations. [Limit the flexibility of the driver, Increase the risk]

- Inadequate description of the conditions of mode transition in SRS of CTCS-2. [Limit the flexibility of the driver, Increase the risk]
First flaw

Dispatcher gives orders to D3115 train Driver [DA1]
First flaw

Dispatcher gives orders to D3115 train Driver [DA1]

Created Problems

Dispatcher should send

Station watcher should send

NO one sent this information
Conclusion

- A dynamic analysis method based on CAST is created.

- The CAST can be combined with dynamic analysis process.

- This analysis accurately finds more interaction factor contributed to the accident.
Q&A!

State Key Laboratory of Rail Traffic Control and Safety
Beijing Jiaotong University, Beijing, China
Thank you!

State Key Laboratory of Rail Traffic Control and Safety
Beijing Jiaotong University, Beijing, China