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

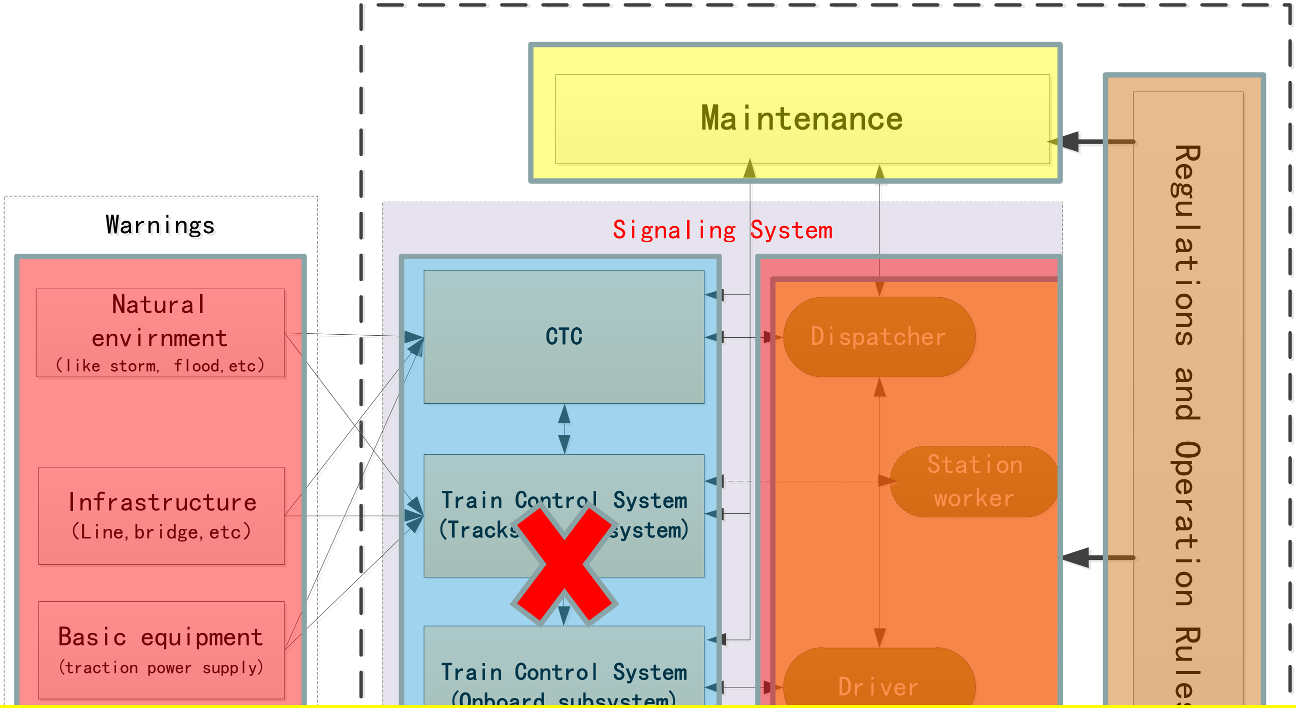
- Motivation
  - Experience of 7.23 accident analysis using STAMP
  - Chinese railway system
- Some ideas about using CAST in operational and physical level
  - Show the dynamic
- 7.23 Yong-Wen railway Accident Analysis
  - Analysis
- Conclusions

Chinese High-speed Railway Accident

- 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



Warnings

Natural envirnment (like storm, flood, etc)

Infrastructure (Line, bridge, etc)

Basic equipment (traction power supply)

Signaling System

Maintenance

CTC

Train Control System (Tracks... system)

Train Control System (Onboard subsystem)

Dispatcher

Station worker

Driver

Regulations and Operation Rules

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

- safe

Experience

- Application of CAST and STPA to railroad safety in China [Dong Airong, MIT, MSc thesis, 2012]
  - The s
  - Every

Did not consider the change of control structure in the operational level

- A system theoretic analysis of the “7.23” Yong-tai-wen railway accident [Suo Dajiang, STAMP workshop 2012]
  - A
  - (

Did not analyze the change of Component’s roles and responsibilities

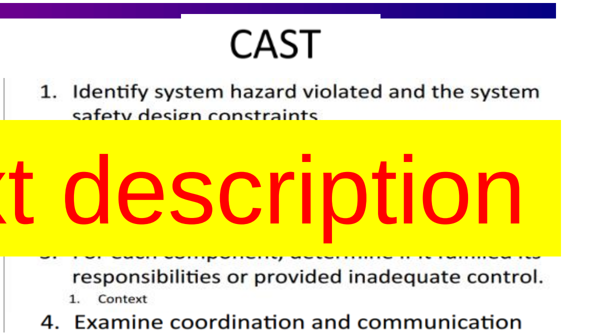
- Using STAMP to learn from Chinese High speed railway accident [Tang Tao & Niu Ru, STAMP workshop 2013]
  -

Did not give a method to show the process clearly.

➢CAST

- ●ct
- ●ate scenarios

+ text description



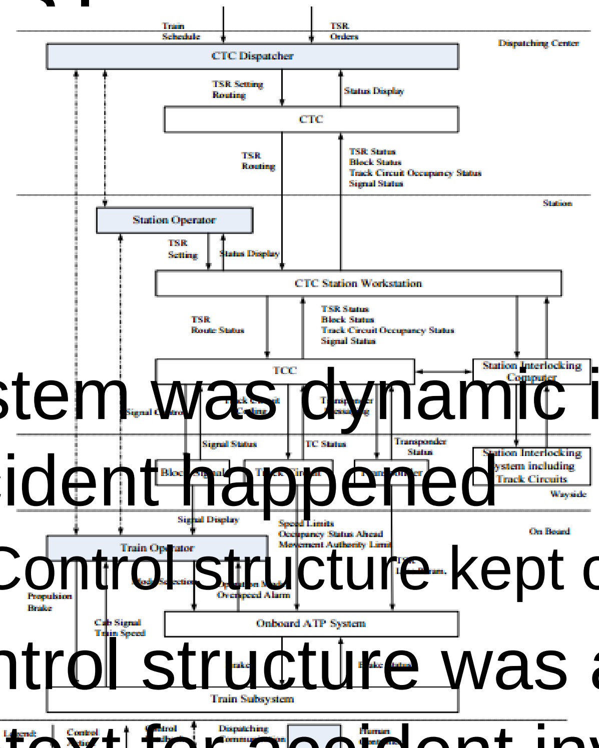
CAST

1. Identify system hazard violated and the system safety design constraints

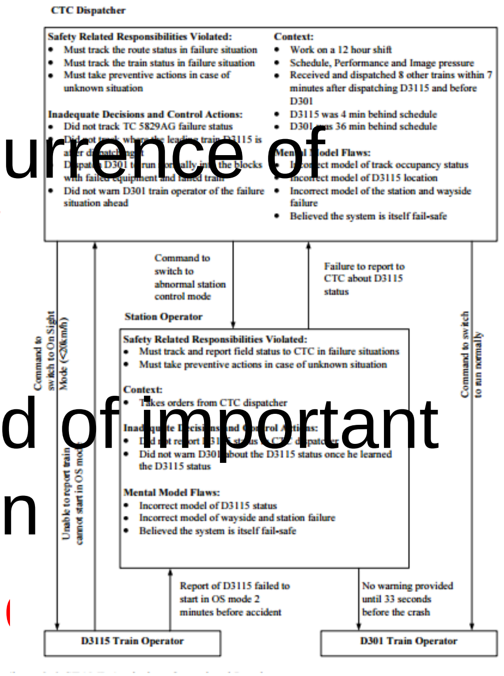
3. For each component, determine if it fulfilled its responsibilities or provided inadequate control.
   1. Context
4. Examine coordination and communication

n to higher

ld eliminate
enforcement
the future.



Train Schedule
TSR Orders
Dispatching Center
CTC Dispatcher
TSR Setting Routing
Status Display
CTC
TSR Routing
TSR Status
Block Status
Track Circuit Occupancy Status
Signal Status
Station
Station Operator
TSR Setting
Status Display
CTC Station Workstation
TSR Route Status
TSR Status
Block Status
Track Circuit Occupancy Status
Signal Status
TCC
Station Interlocking Computer
Signal Control
Track Circuit Coding
Transponder Messaging
Signal Status
TC Status
Transponder Status
Block Signal
Track Circuit
Transponder
Station Interlocking System including Track Circuits
Wayside
Signal Display
Speed Limits
Occupancy Status Ahead
Movement Authority Limit
On Board
Train Operator
TSR Line Param.
Mode Selection
Operation Mode
Overspeed Alarm
Propulsion
Brake
Cab Signal
Train Speed
Onboard ATP System
Brake
Brake Status
Train Subsystem
Legend:
Control Action
Control Feedback
Dispatching Communication
Human Controller



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

Command to switch to On Sight Mode (<20km/h)

Unable to report train cannot start in OS mode

Command to switch to run normally

Station Operator

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

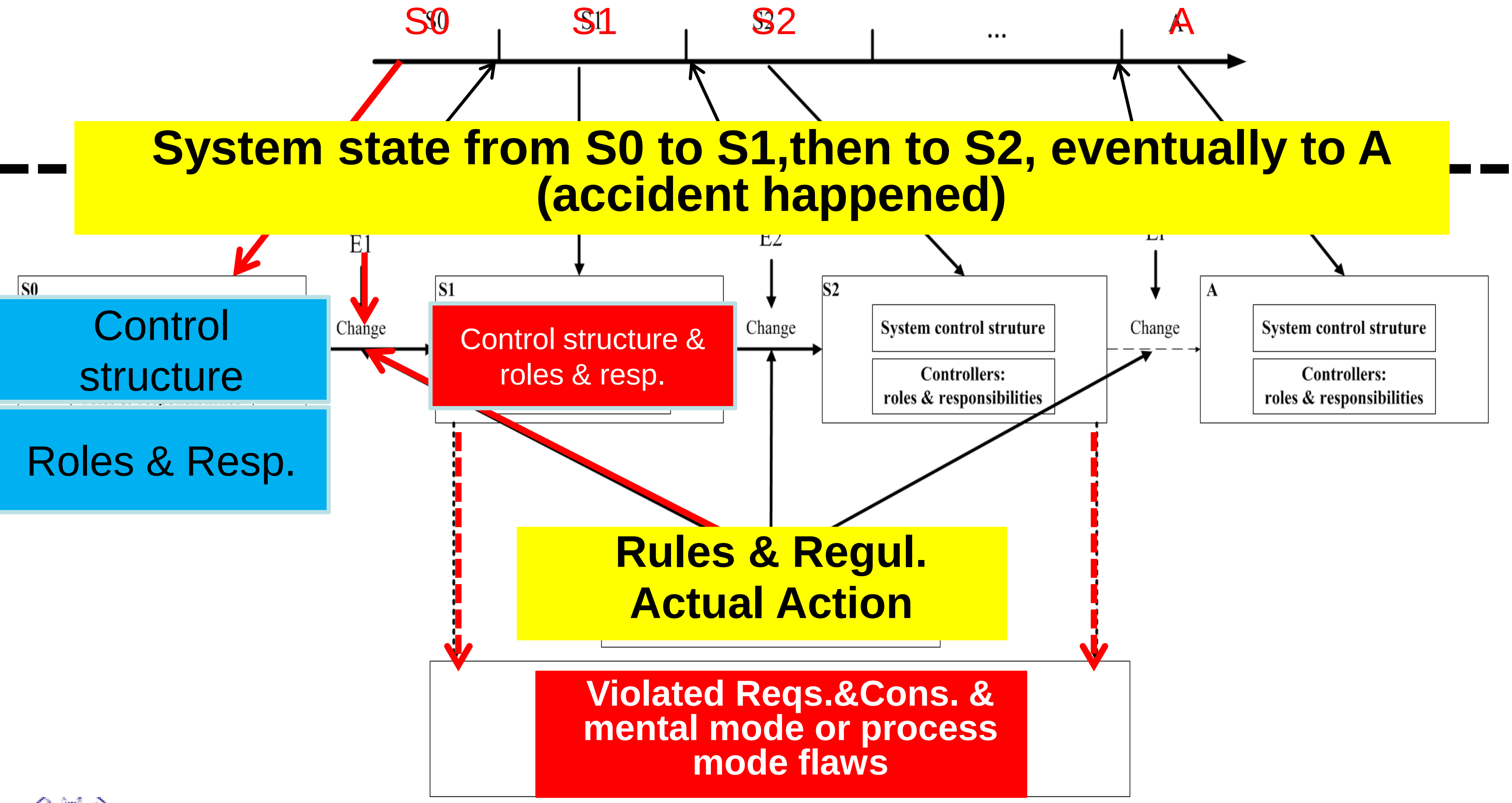
D301 Train Operator

- System was dynamic in the occurrence of accident happened
  - Control structure kept changing
- Control structure was also a kind of important context for accident investigation
- So, we should use a dynamic vi n 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



S0 S1 S2 A

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

Control structure

Roles & Resp.

Control structure & roles & resp.

Rules & Regul.
Actual Action

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

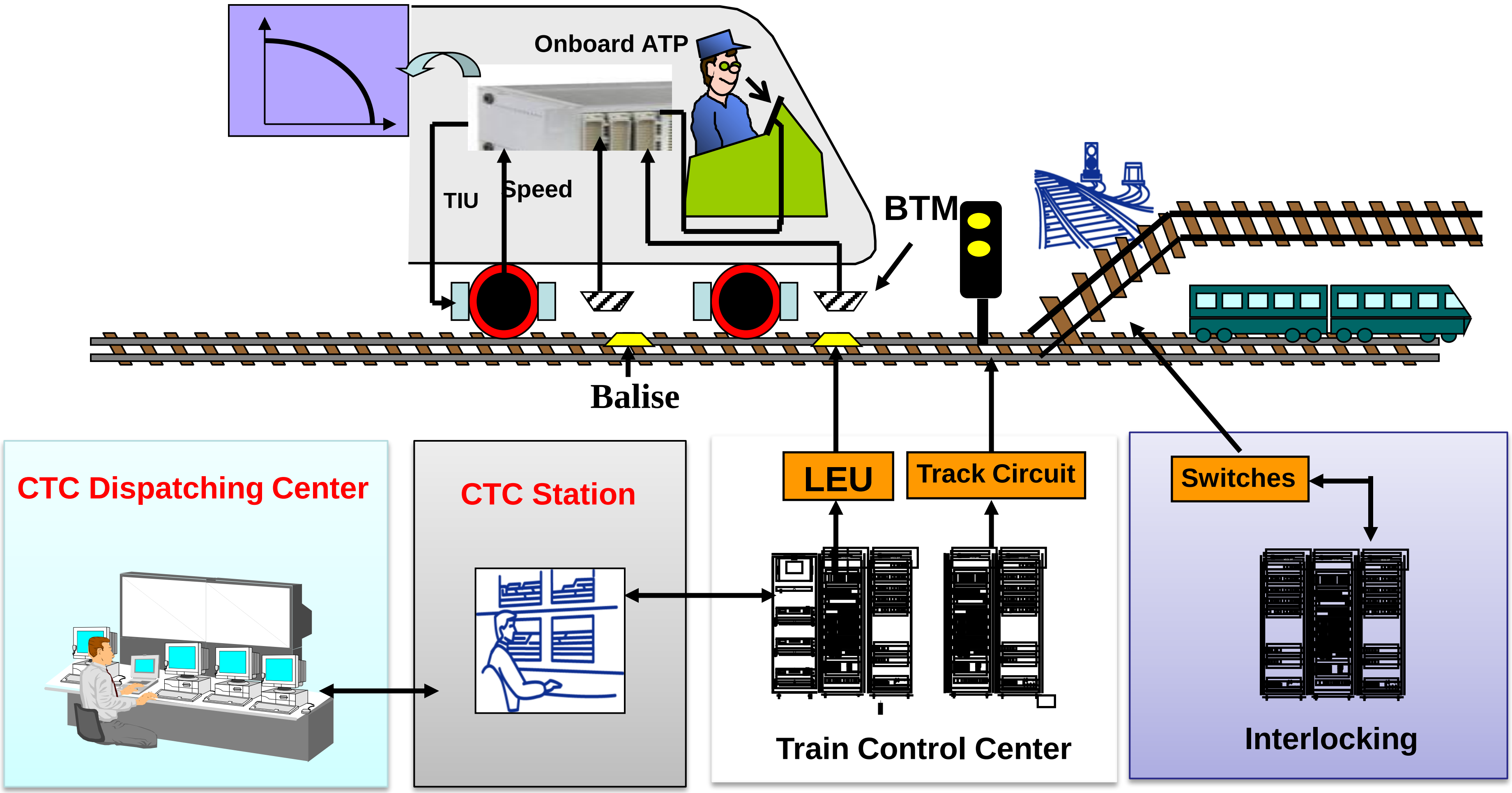
Using CAST

- 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 flaws

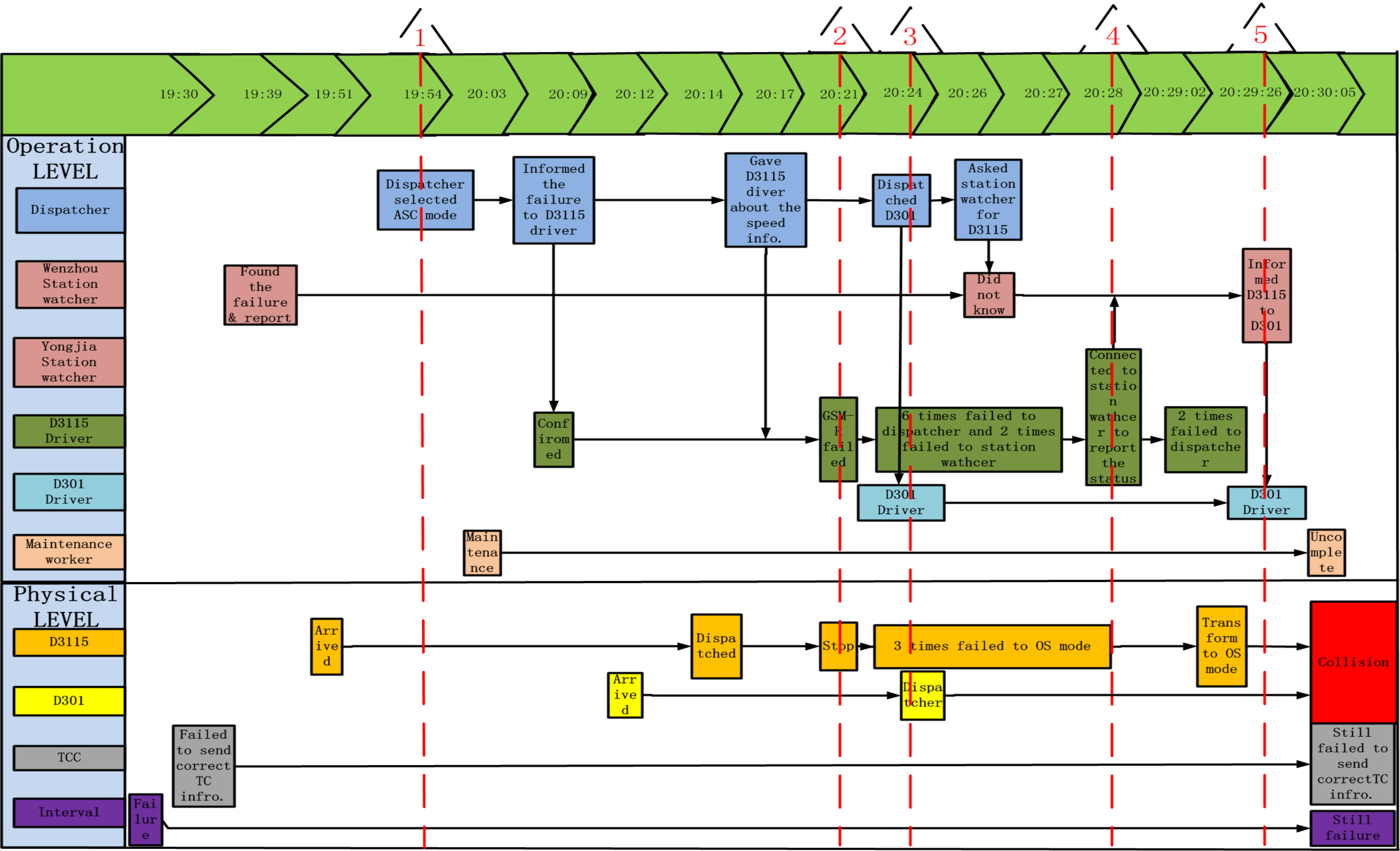
Outline

- 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



Related Events



1 2 3 4 5

19:30 19:39 19:51 19:54 20:03 20:09 20:12 20:14 20:17 20:21 20:24 20:26 20:27 20:28 20:29:02 20:29:26 20:30:05

Operation LEVEL

Dispatcher: Dispatcher selected ASC mode → Informed the failure to D3115 driver → Gave D3115 diver about the speed info. → Dispatched D301 → Asked station watcher for D3115

Wenzhou Station watcher: Found the failure & report → Did not know → Informed D3115 to D301

Yongjia Station watcher

D3115 Driver: Confiromed → GSM-R failed → 6 times failed to dispatcher and 2 times failed to station wathcer → Connected to station wathcer to report the status → 2 times failed to dispatcher

D301 Driver: D301 Driver → D301 Driver

Maintenance worker: Maintenance → Uncomplete

Physical LEVEL

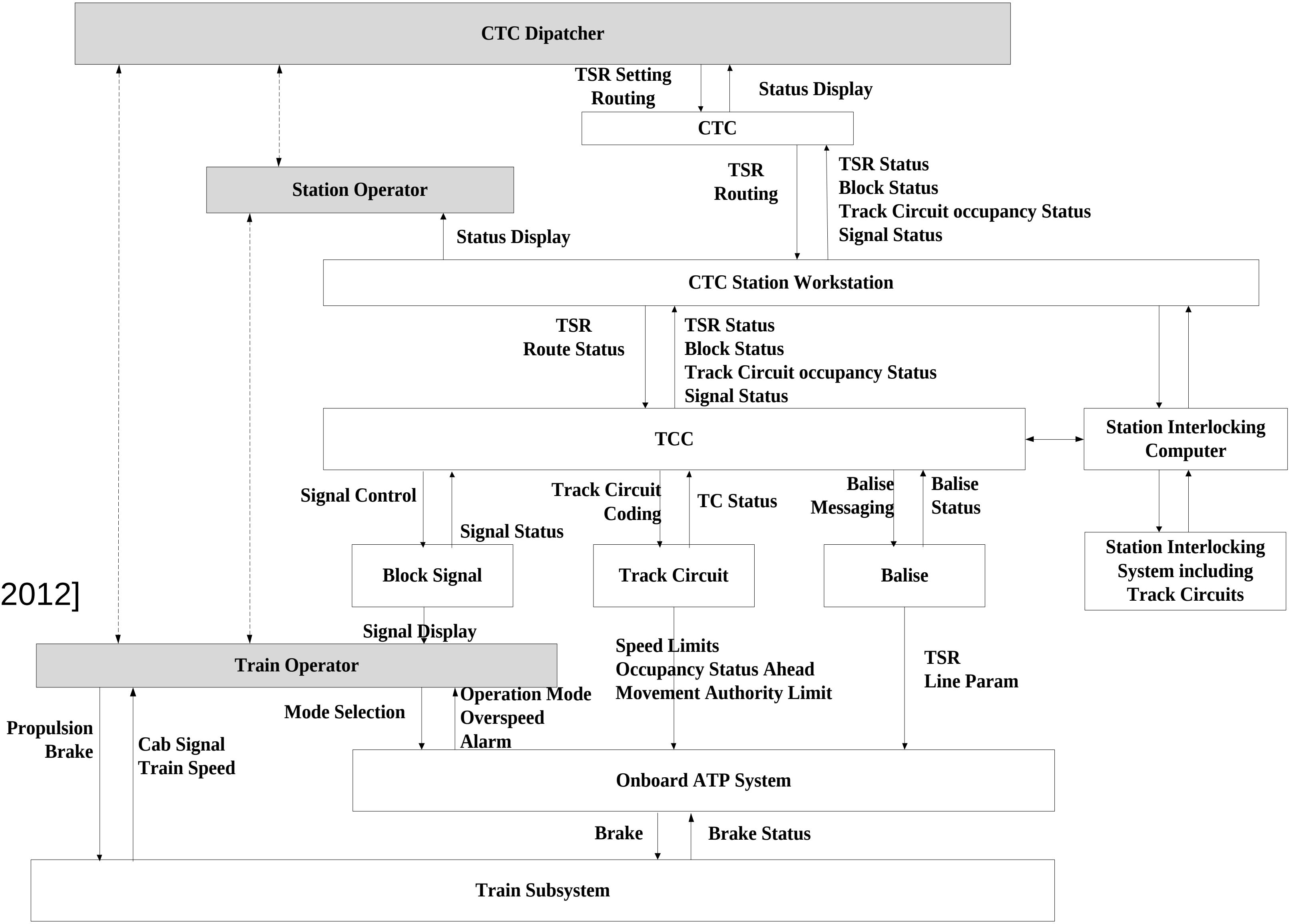
D3115: Arrived → Dispatched → Stop → 3 times failed to OS mode → Transform to OS mode → Collision

D301: Arrived → Dispatcher → Collision

TCC: Failed to send correct TC infro. → Still failed to send correctTC infro.

Interval: Failure → Still failure

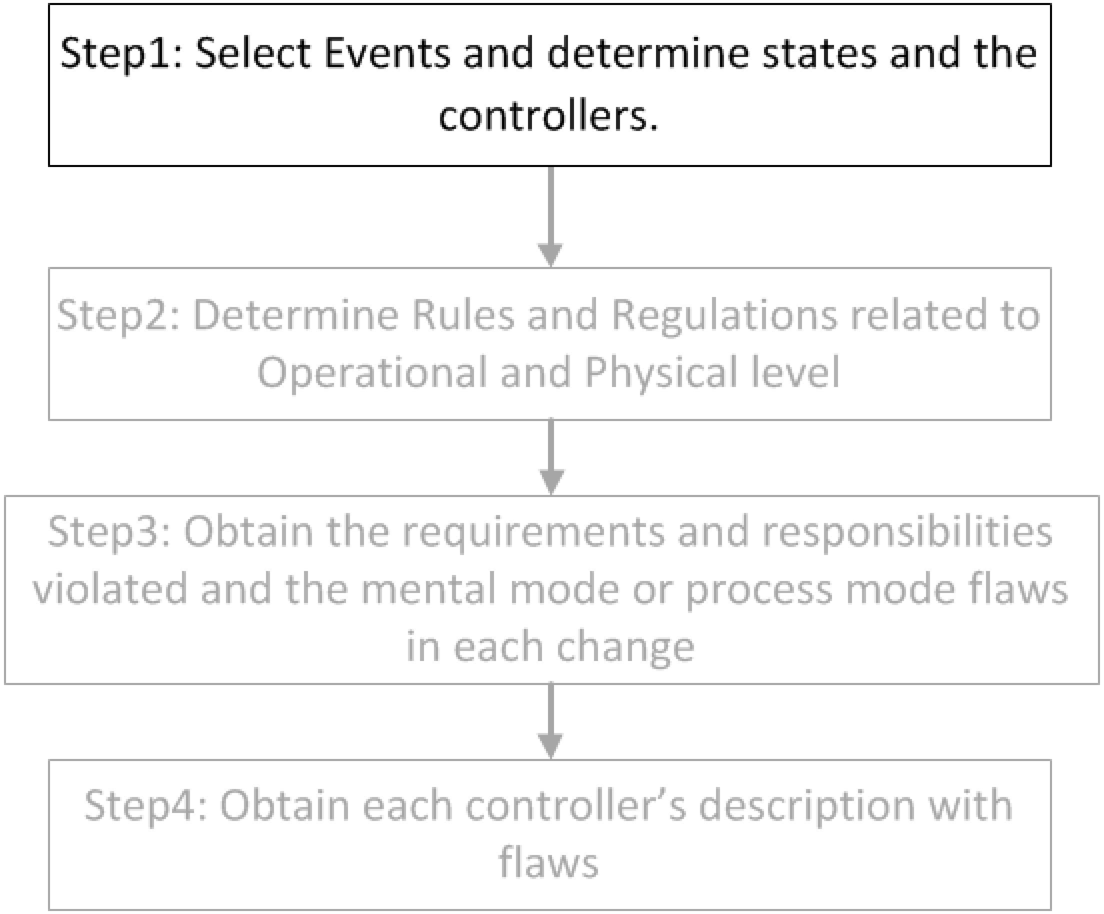
Operational and Physical Level



Airong Dong[2012]

Step1a:
Determine the controllers

- 5 cont
- Roles
- Respo

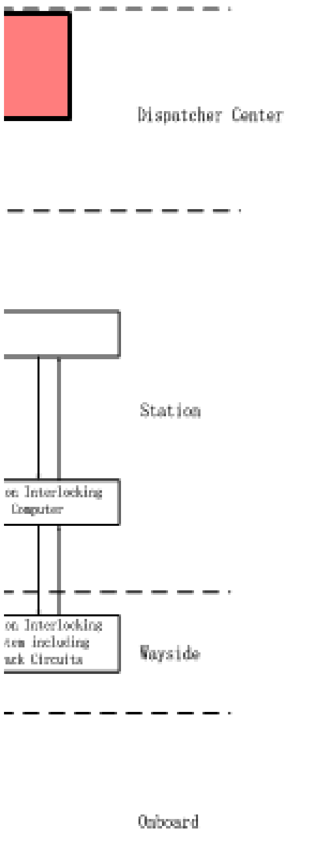


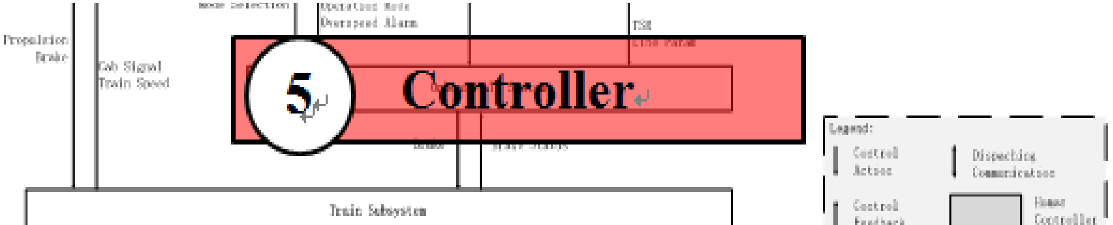
Step1: Select Events and determine states and the controllers.

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

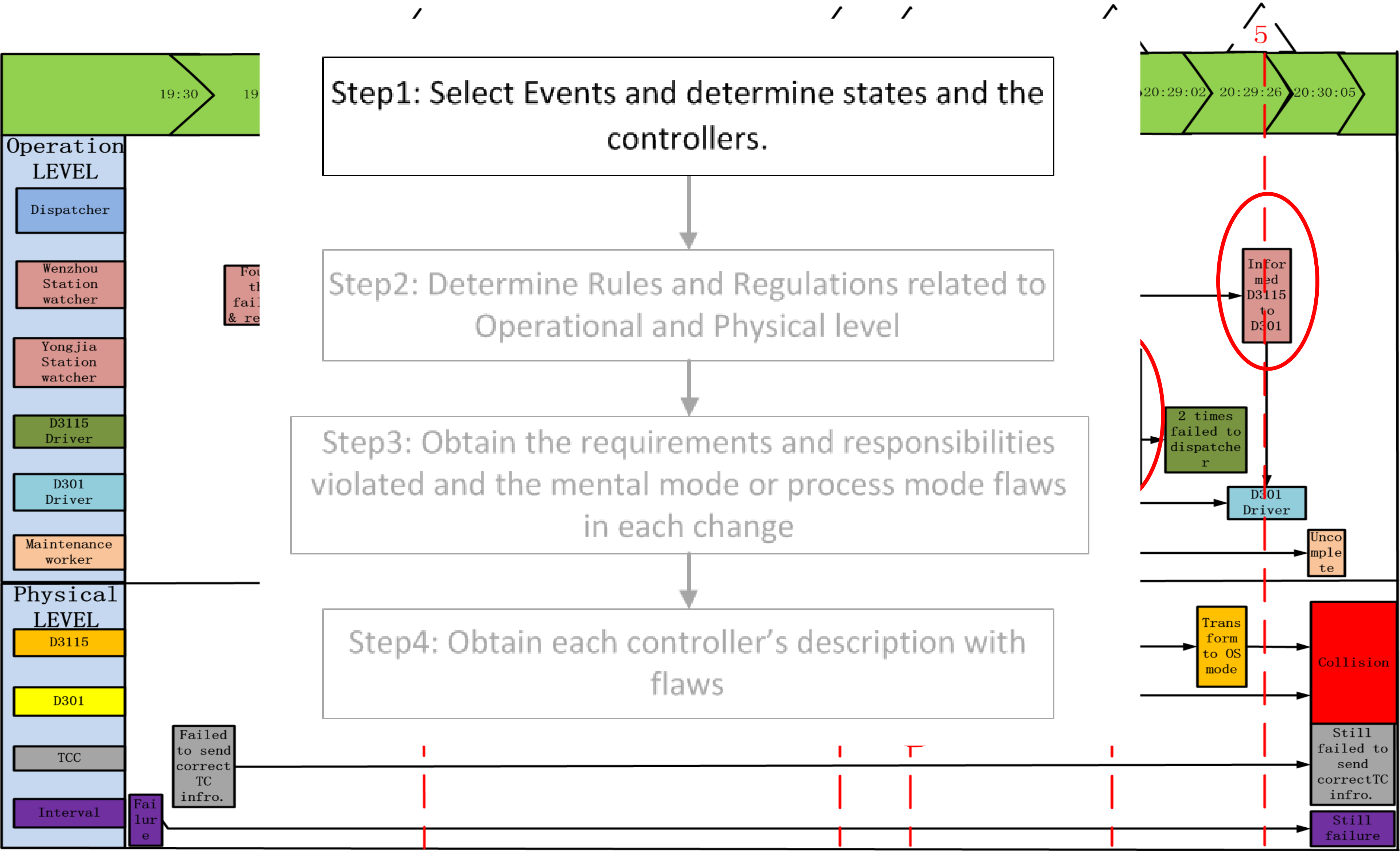
Step3: Obtain the requirements and responsibilities violated and the mental mode or process mode flaws in each change

Step4: Obtain each controller's description with flaws





Step1b:
Select Events



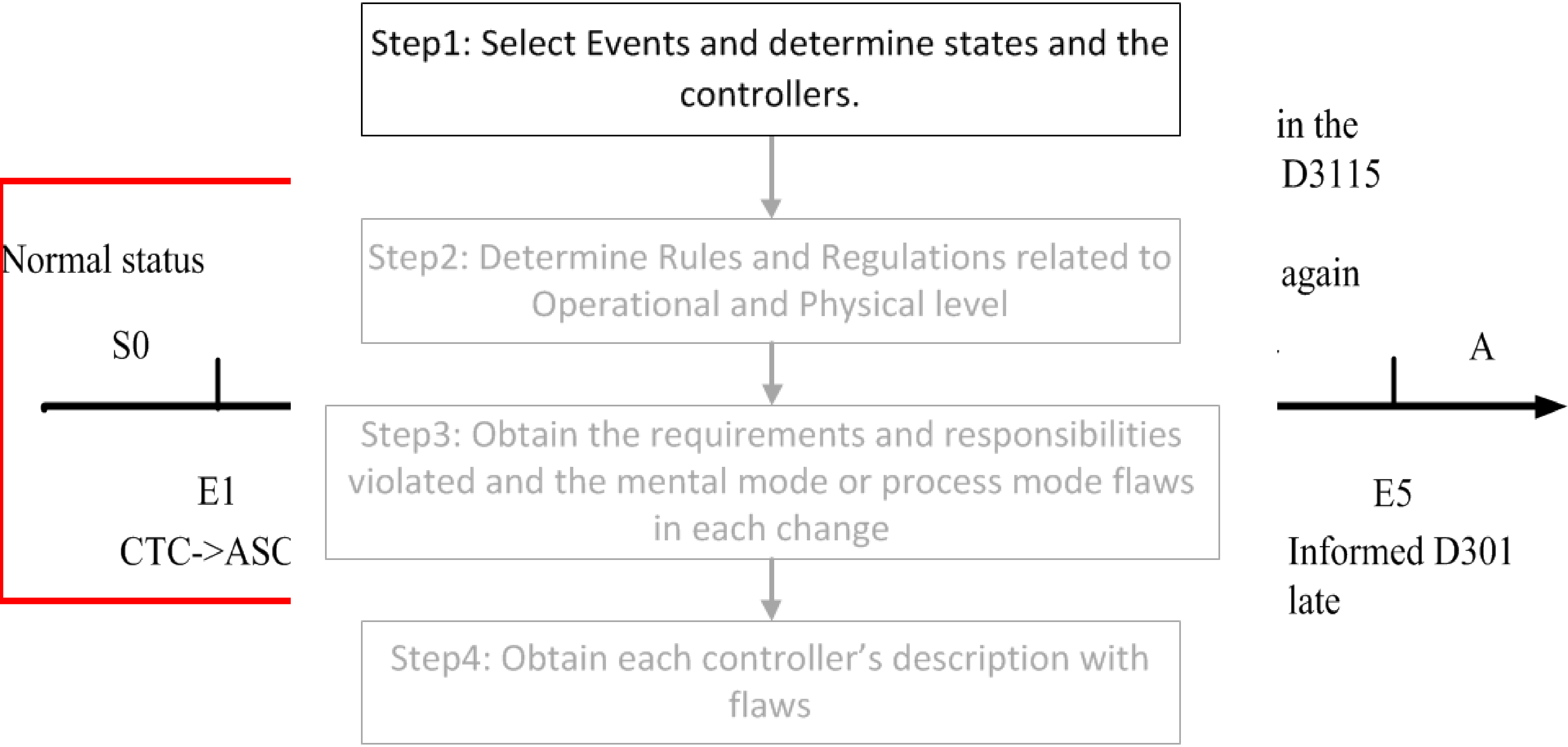
Step1: Select Events and determine states and the controllers.

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

Step1c:
Determine states



Step1: Select Events and determine states and the controllers.

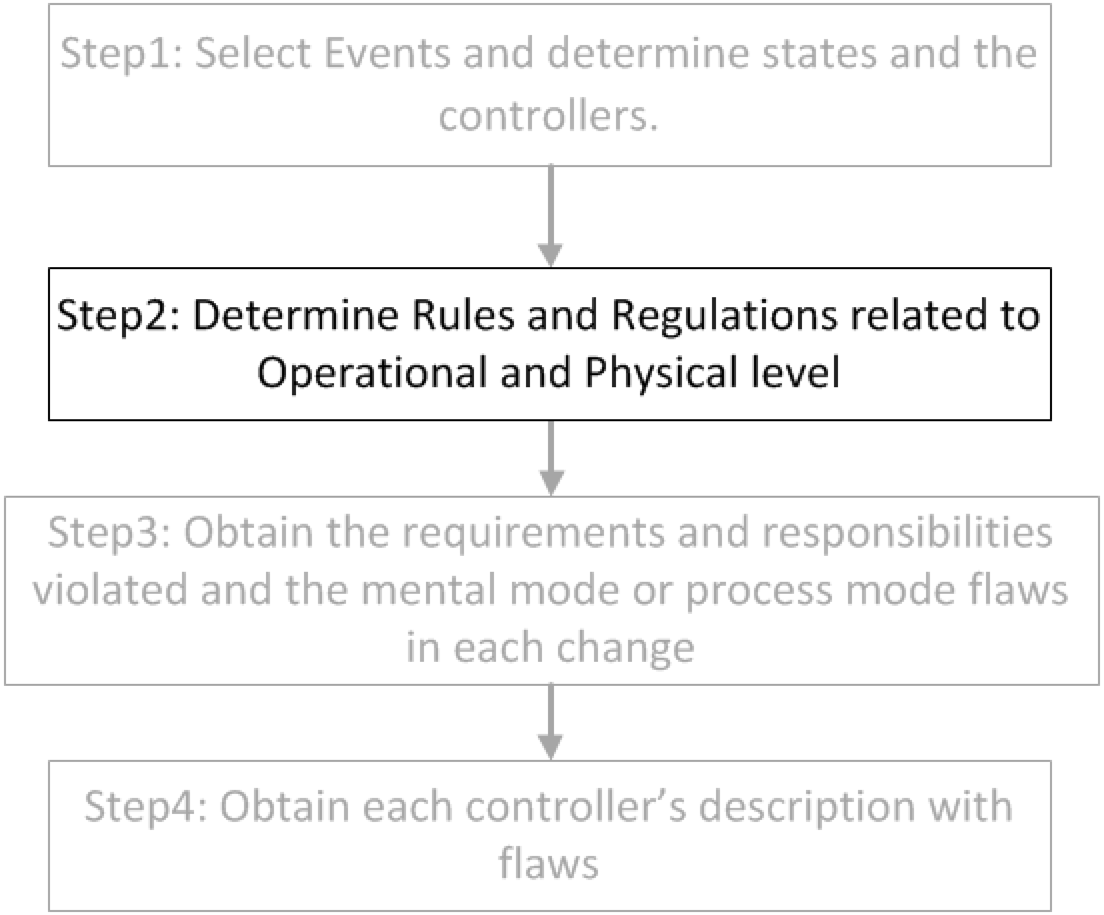
Step2: Determine Rules and Regulations related to Operational and Physical level

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

Steps2:Related Rules and Regulations

1. Reg n[2007]
2. Rai 2008]
3. Me ıy
   pas
4. Hig)9]
5. Sha
   rule
6. Joi ɔn
   woı



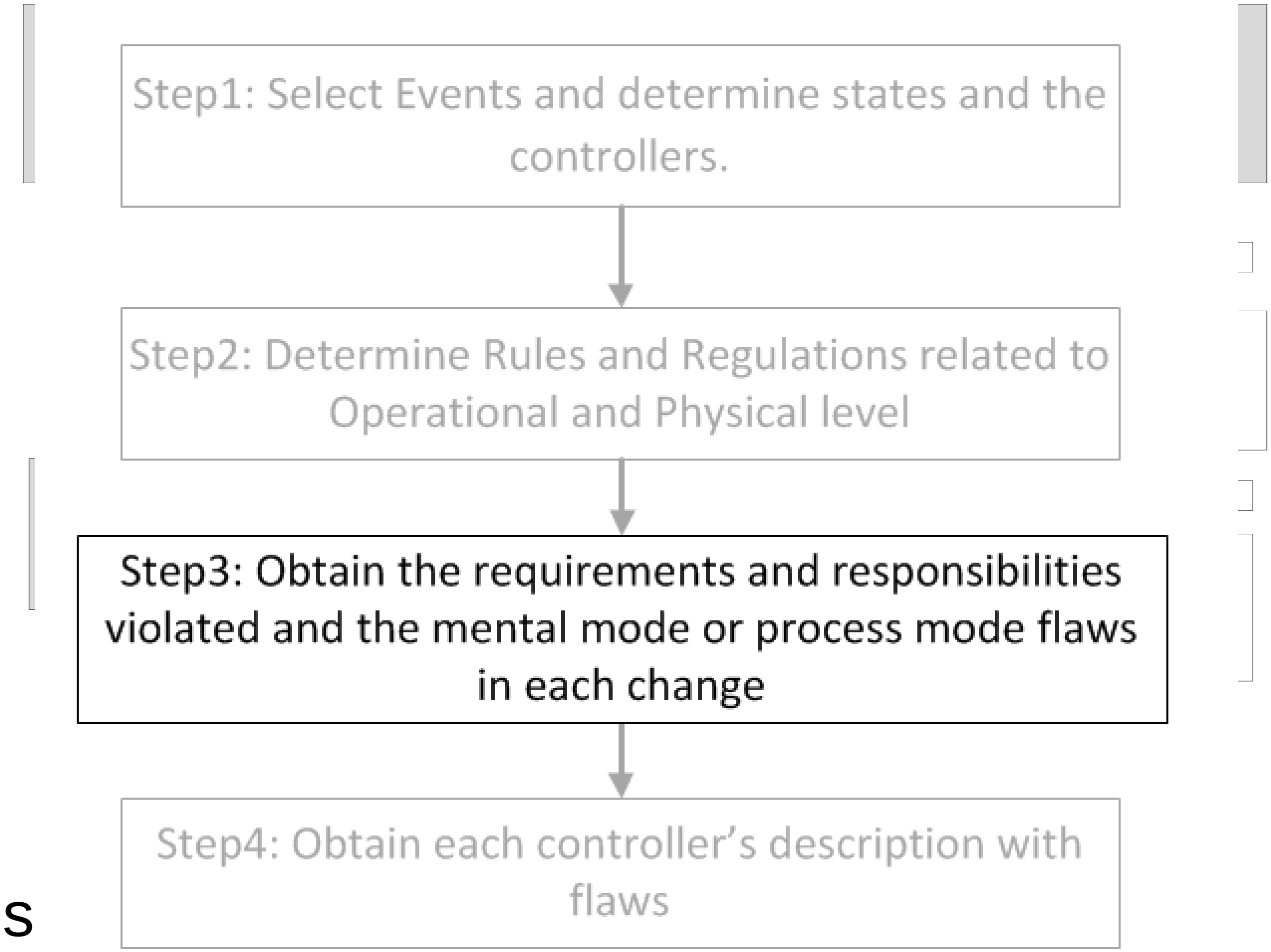
Step1: Select Events and determine states and the controllers.

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

Step3 S0:Normal state



Step1: Select Events and determine states and the controllers.

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

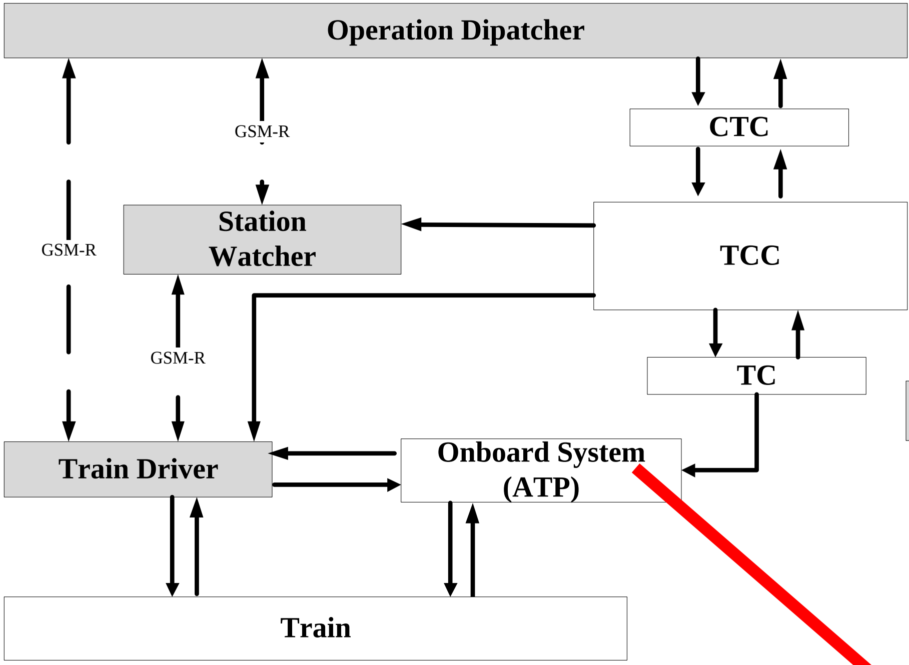
Step3: Obtain the requirements and responsibilities violated and the mental mode or process mode flaws in each change

Step4: Obtain each controller's description with flaws

➢ Des

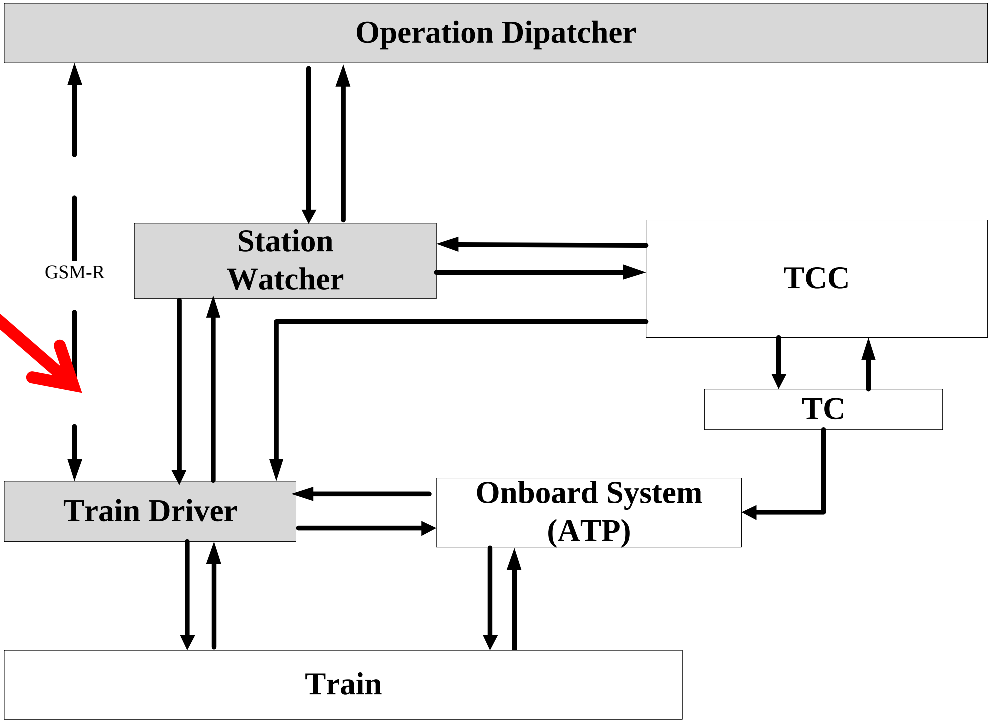
Monitor stations status (Route Status)[From CTC system]

Step3 Control structure change

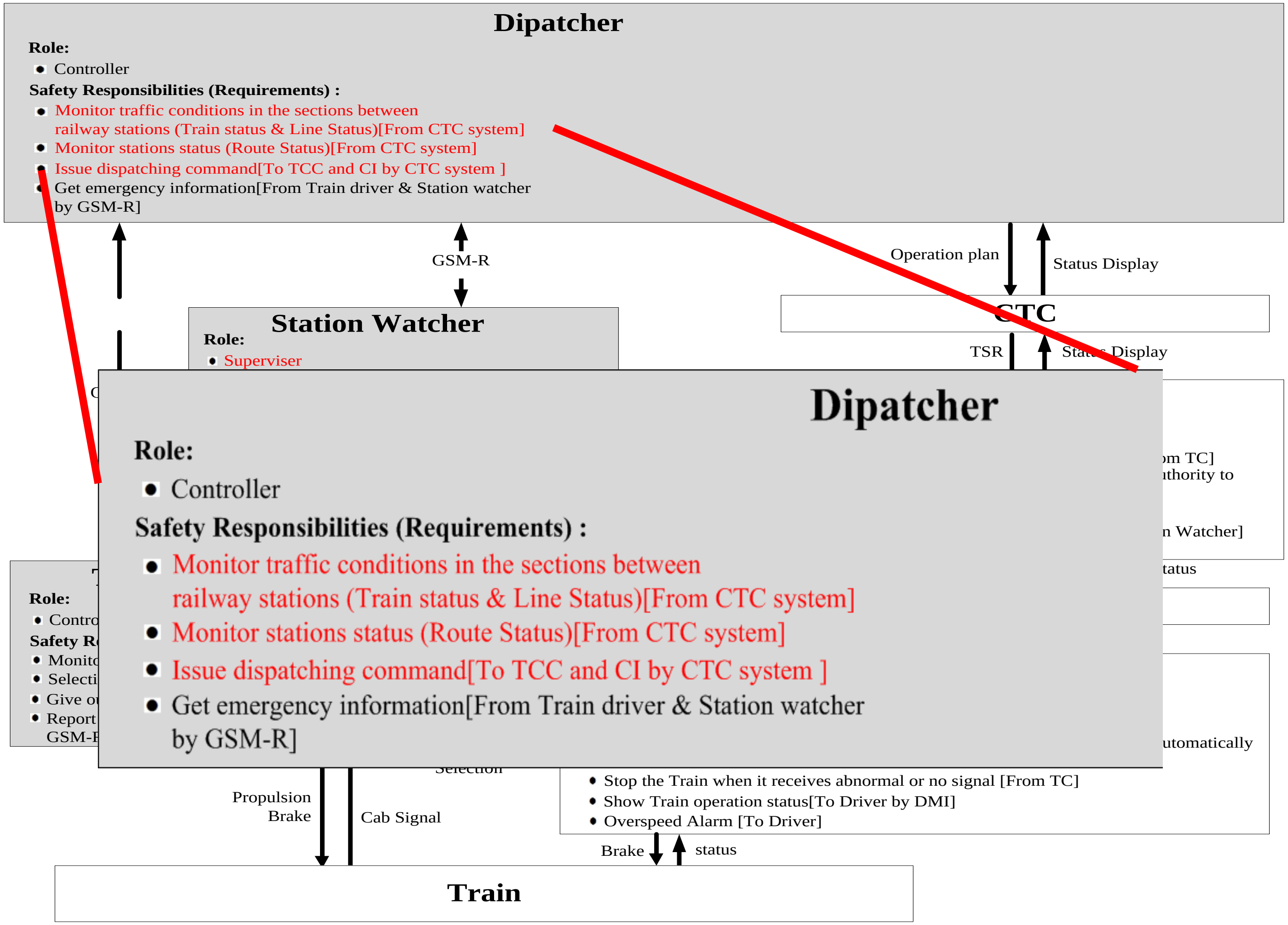


Normal

ASC(Regulation Req.)



Step3 Roles and responsibilities change



Dipatcher

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:

- Superviser

Dipatcher

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]

- Stop the Train when it receives abnormal or no signal [From TC]
- Show Train operation status[To Driver by DMI]
- Overspeed Alarm [To Driver]

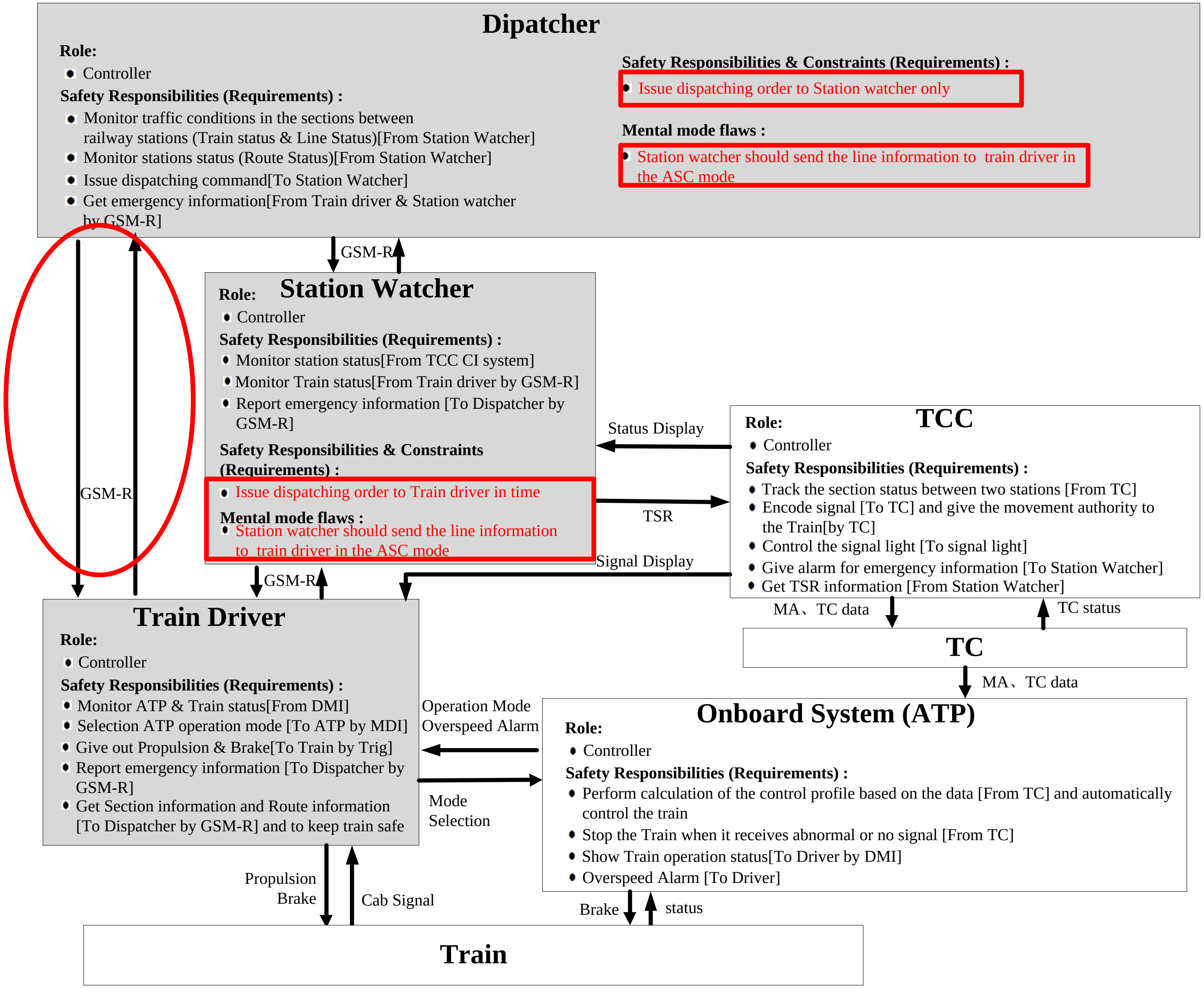
Train

Step3 Controllers actions after change

- ➢ Controllers’ actual actions
  - ✓ Dispatcher gives orders to D3115 train Driver

Step3 S1: Actual ASC

Dispatcher gives orders to D3115 train Driver [DA1]



Dipatcher

Role:

- Controller

Safety Responsibilities (Requirements) :

- Monitor traffic conditions in the sections between railway stations (Train status & Line Status)[From Station Watcher]
- Monitor stations status (Route Status)[From Station Watcher]
- Issue dispatching command[To Station Watcher]
- Get emergency information[From Train driver & Station watcher 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

Mental mode flaws :

- Station watcher should send the line information to train driver in the ASC mode

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]

TC

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

Onboard System (ATP)

Role:

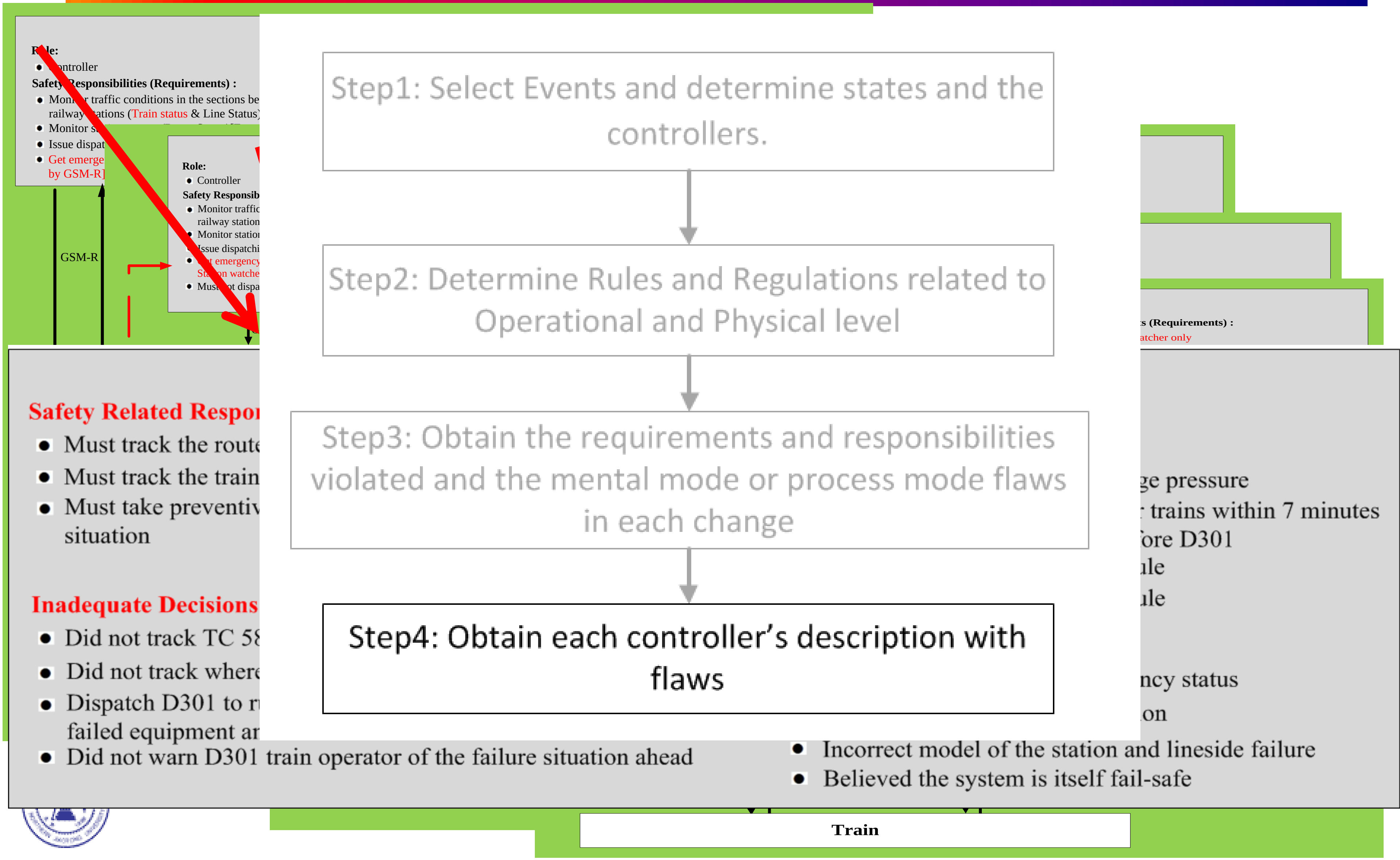
- Controller

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

Step4: Obtain each controller's description with flaws



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

Safety Related Respon

- Must track the route
- Must track the train
- Must take preventiv situation

Inadequate Decisions

- Did not track TC 58
- Did not track where
- Dispatch D301 to r failed equipment ar
- Did not warn D301 train operator of the failure situation ahead

ge pressure
trains within 7 minutes
ore D301
ule
ule
ncy status
on

- 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]

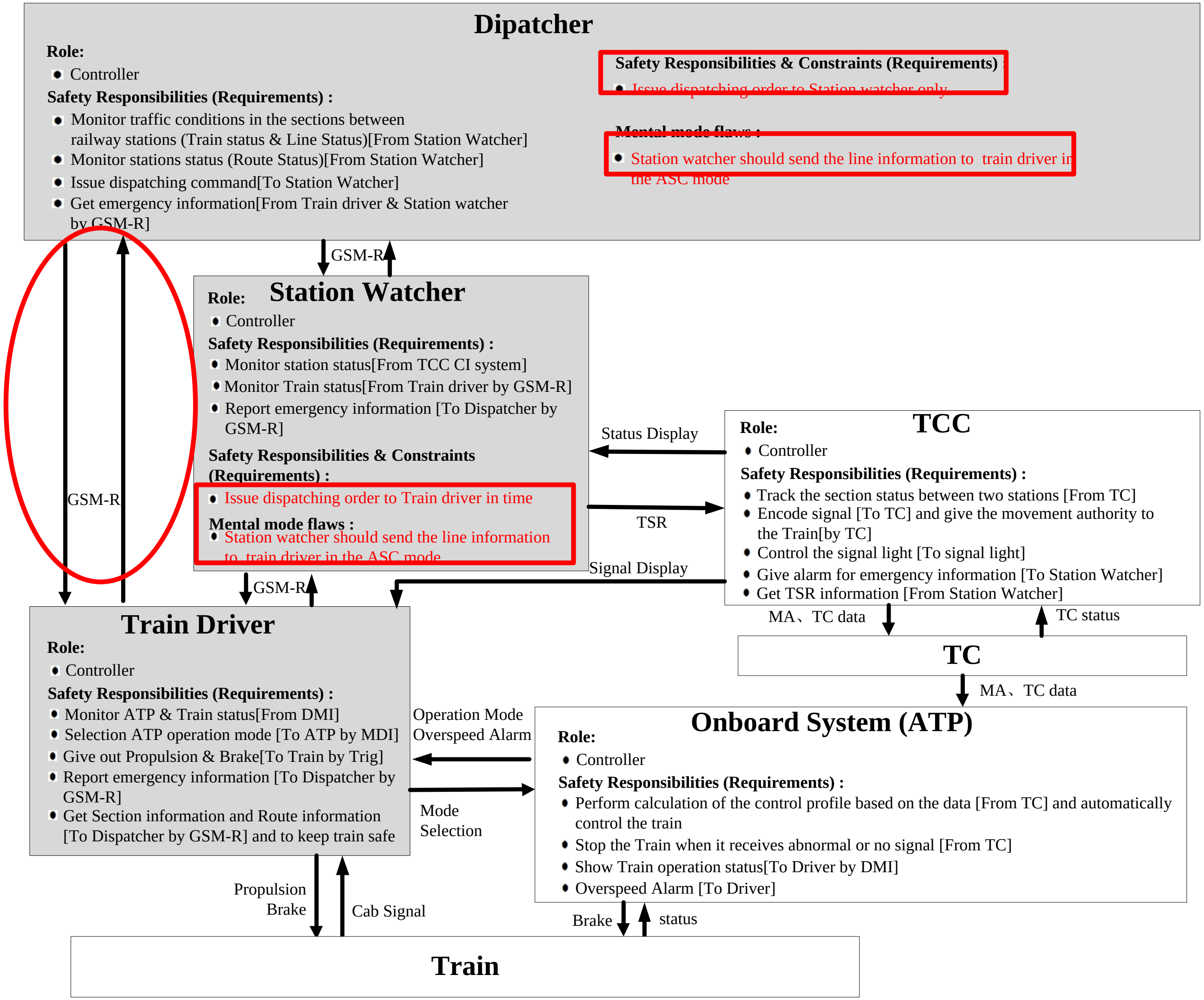
- Dispatcher order in ASC mode & the incompletion Rules& Regulations. [Limit the flexibility of the driver, Increase the risk]

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

First flaw

S1: Actual ASC

Dispatcher gives orders to D3115 train Driver [DA1]



Dipatcher

Role:

- Controller

Safety Responsibilities (Requirements) :

- Monitor traffic conditions in the sections between railway stations (Train status & Line Status)[From Station Watcher]
- Monitor stations status (Route Status)[From Station Watcher]
- Issue dispatching command[To Station Watcher]
- Get emergency information[From Train driver & Station watcher 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

Mental mode flaws :

- Station watcher should send the line information to train driver in the ASC mode

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]

TC

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

Onboard System (ATP)

Role:

- Controller

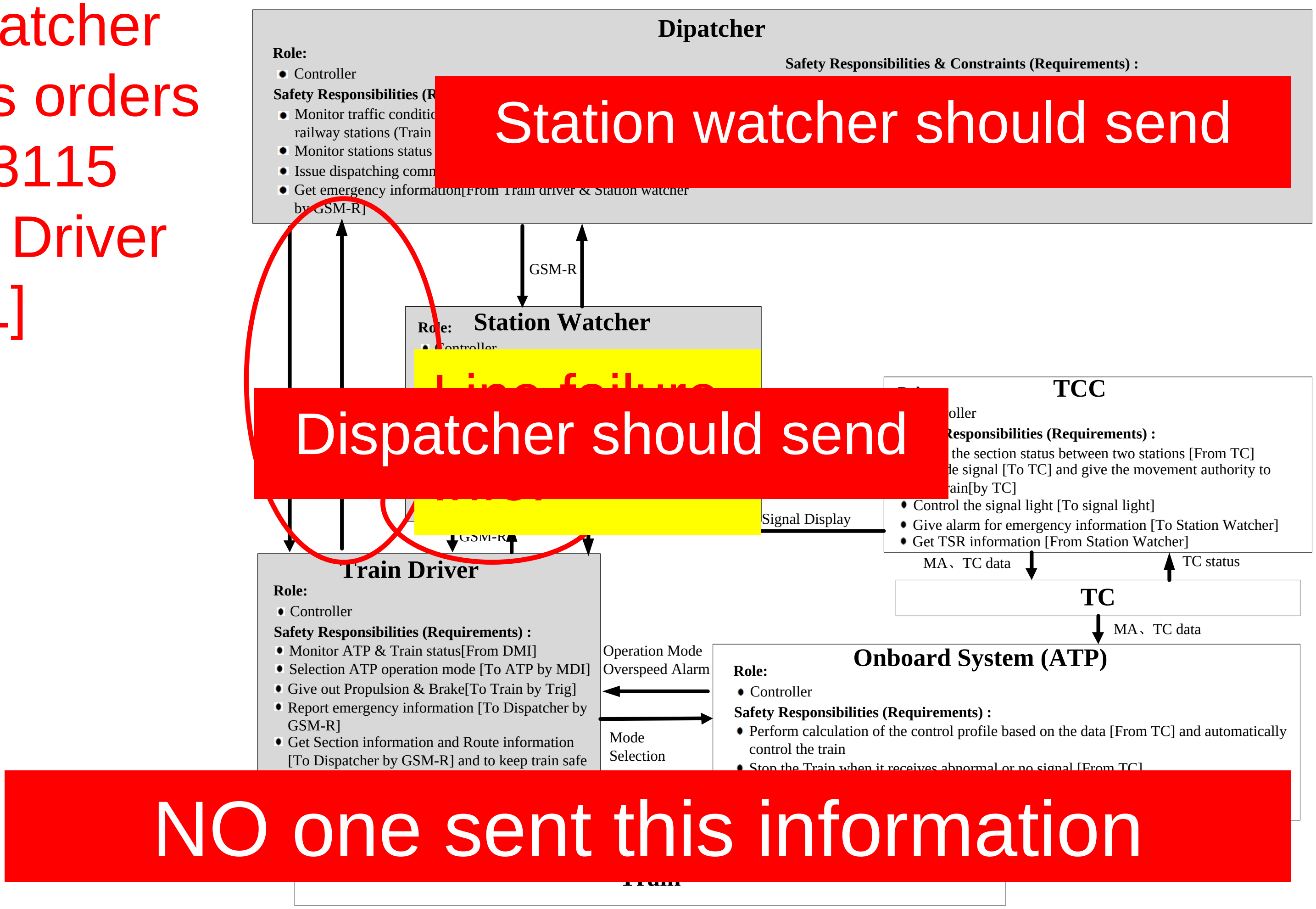
Safety Responsibilities (Requirements) :

- 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

First flaw   Created Problems

Dispatcher gives orders to D3115 train Driver [DA1]



Station watcher should send

Dispatcher should send

NO one sent this information

Dipatcher

Role:

- Controller

Safety Responsibilities (R

- Monitor traffic conditio
railway stations (Train
- Monitor stations status
- Issue dispatching comm
- Get emergency information[From Train driver & Station watcher by GSM-R]

Safety Responsibilities & Constraints (Requirements) :

GSM-R

Station Watcher

Role:

- Controller

Line failure

infor

GSM-R

TCC

oller

Responsibilities (Requirements) :

the section status between two stations [From TC]
le signal [To TC] and give the movement authority to
ain[by TC]

- Control the signal light [To signal light]
- Give alarm for emergency information [To Station Watcher]
- Get TSR information [From Station Watcher]

Signal Display

MA、TC data

TC status

TC

MA、TC data

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

Mode
Selection

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]

Train

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