Using STAMP/STPA to Chinese High Speed Railway Train Control System

Liu Jintao，Ph.D. candidate
State Key Laboratory of Rail Traffic Control and Safety
Beijing Jiaotong University

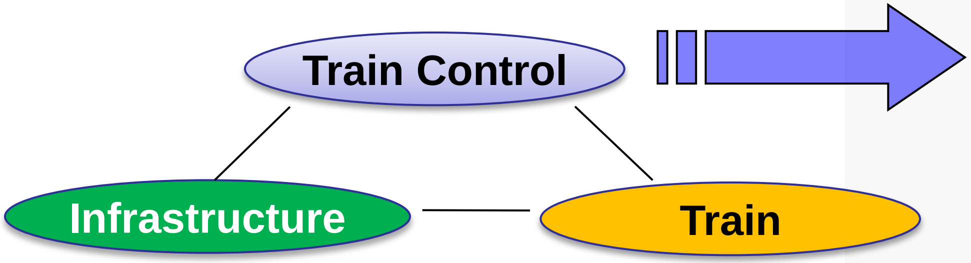
Outline

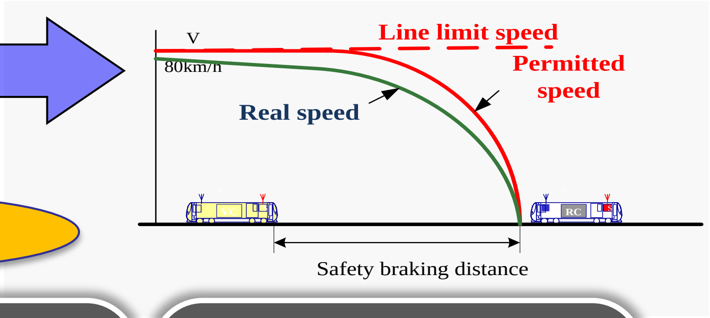
- Background and Motivation
  - Train control system in requirements phase
  - Hazard analysis on train control system
- Some ideas in using STPA in requirements phase
  - Internal Function Modules in Control Loops
  - Causal Factors
  - Formal model-based Causal Factors Analysis
- Case study : Chinese Train Control System
  - Chinese High Speed Railway Train Control System
  - Perform STPA on study case
- Conclusion

Background and Motivation

➢ What is train control system?

To separate and protect train against collision and derailment.





Se . 2006.German
de d, 10 injured.

Apr. 2008. China JiaoJi
injured.

Jul. 2011. China
dead, 200 injur d.

Train Control System is Safety-Critical

Background and Motivation

- **Main features of Train Control System in the Requirements Phase**

  In requirements phase of train control system lifecycle, the system is specified in system requirements specification (SRS).

  - Described in natural language

  - Refinement of functional requirements on technical level

    (A set of function modules and their inputs/outputs)

Background and Motivation

- **Hazard Analysis on Train Control System in the Requirements Phase**

  As the basis of system design and development, train control system depicted in SRS shall be analyzed to identify the hazardous factors that lead to the system hazard.

  According to these hazardous factors, we could further improve the SRS, and establish the safety requirements.

Background and Motivation

- **Why and How to use STAMP/STPA**
  - Event Chain can not effectively help to analyze the hazardous factors.
  - Specifically Not Repeat the Benefits of STPA
    - Step1: Identify unsafe control actions
    - Step2: Identify causal factors
      - ✓ Causal factors focused by STPA are related to the control algorithm, the process model and so on.
      - ✓ The system in requirements phase is described in natural language, for which the formal description is more accurate way.

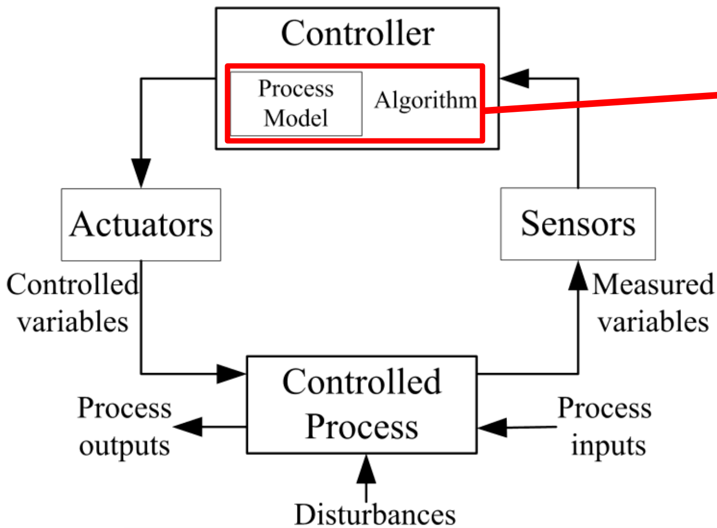
Considering such two aspects, we propose some ideas to customize the specific implementation of STPA .

Outline

- Background and Motivation
  - Train control system in requirements phase
  - Hazard analysis on train control system
- Some ideas in using STPA in requirements phase
  - Internal Function Modules in Control Loops
  - Causal Factors
  - Formal model-based Causal Factors Analysis
- Case study : Chinese Train Control System
  - Chinese High Speed Railway Train Control System
  - Perform STPA on study case
- Conclusion

Some ideas in using STPA in requirements phase

- **Internal Function Modules in Control Loops**

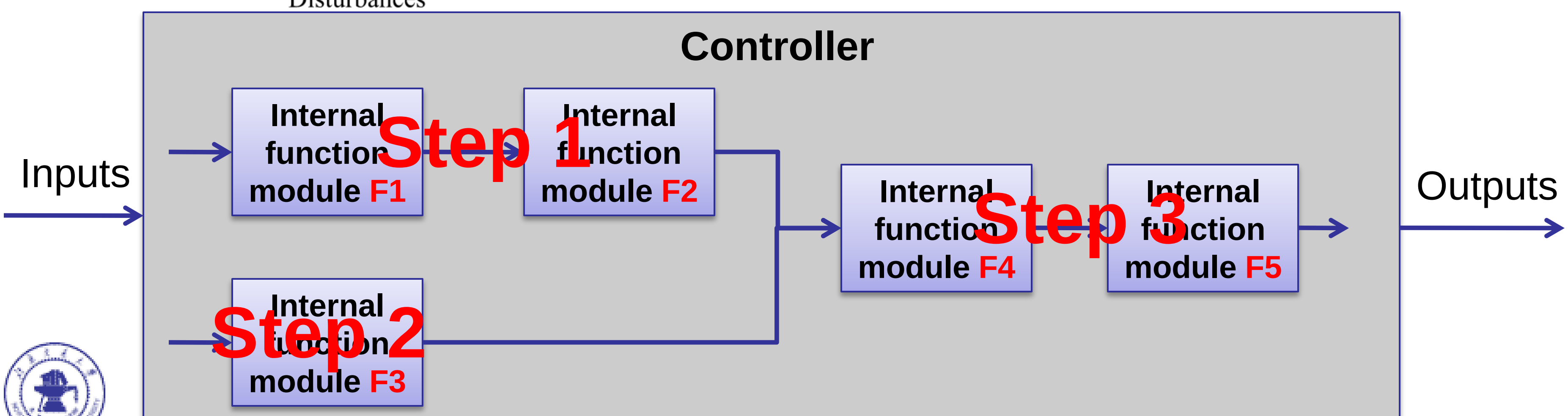


Step 1: F1 *a*, F2 *b*;

Step 2: F3 *c*;

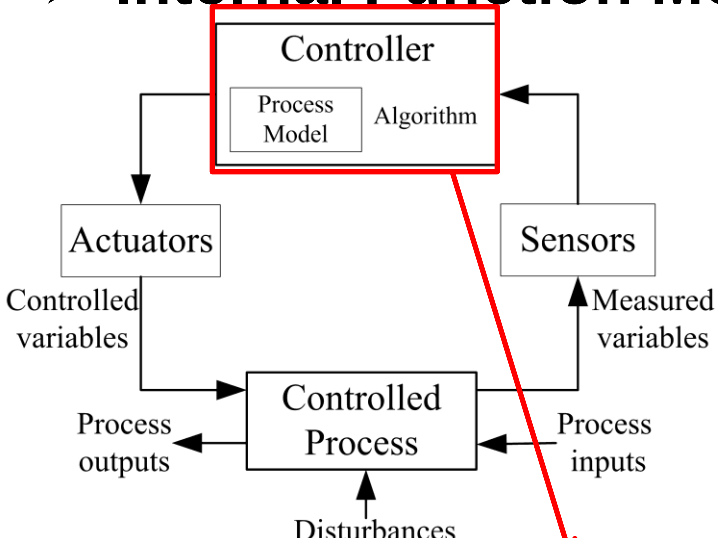
Step 3: F4 *d*, F5 *e*;

...

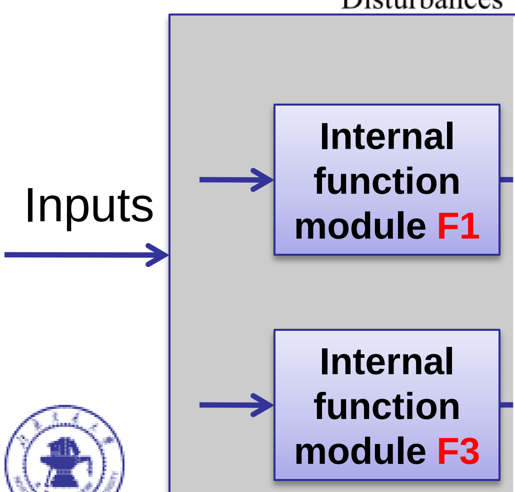


Some ideas in using STPA in requirements phase

- **Internal Function Modules in Control Loops**



We describe the internal function modules and their inputs/outputs in the controller using the form of lists.



Internal Function Modules in Controller	Inputs/Outputs
F1	Input: Output:
F2	Input: Output:
F3	Input: Output:

Some ideas in using STPA in requirements phase

➢ Causal Factors

1. Inadequate Enforcement of Constraints (Control Actions)
- 1.1 Unidentified hazards
- 1.2 Inappropriate, ineffective, or missing control actions for identified hazards
  - 1.2.1. Design of control algorithm (process) does not enforce constraints
    - —Flaw(s) in creation process
    - —Process changes without appropriate change in control algorithm (asynchronous evolution)
    - —Incorrect modification or adaptation
  - 1.2.2 Process models inconsistent, incomplete, or incorrect (lack of linkup)
    - —Flaw(s) in creation process
    - —Flaws(s) in updating process (asynchronous evolution)
    - —Time lags and measurement inaccuracies not accounted for
  - 1.2.3 Inadequate coordination among controllers and decision makers (boundary and overlap areas)

2. Inadequate Execution of Control Action
- 2.1 Communication flaw
- 2.2 Inadequate actuator operation
- 2.3 Time lag

3. Inadequate or missing feedback
- 3.1 Not provided in system design
- 3.2 Communication flaw
- 3.3 Time lag
- 3.4 Inadequate sensor operation (incorrect or no information provided)

◆Map the control algorithm-related and process model-related issues into the layer of function modules and their inputs.

Inputs of internal function modules in controller is incorrect, missing, or not updated in time
- — Flaw(s) in engineering process
- — Flaw(s) in updating process
- — Incorrect data entered by human

Internal function modules in controller fail
- — Flaw(s) in creation process
- — Incorrect modification

a) We identify the inputs-related causal factors with manual analysis.

b) We identify the function module-related issues with formal method.

Some ideas in using STPA in requirements phase

- **Formal model-based Causal Factors Analysis**

Behavior Model

Functional Failure Model

– **Step1:** Find all possible internal functional failures according to the list of

ormal behavior with

onal

els

tion

with the

Definition 1
the represen

1) *C* refers to a
2) *M* refers to a ... M_i
is the failure d
3) *F*
com
4) *D*
func
5) *S*
whe
6) *f*
f={f_1
7) *A*
influ
failures on the

```
IntegrateModel (fmodel, nmodel)          // Integrate functional failure model (fmodel) and
{                                        //  normal behavior model (nmodel)
  affec = FindAffection (fmodel);        // Traverse failure model and find affection (affec)
  Parse (affec);                         // Parse affection which describes the influences of failures
  For each keyword of affec              // For each keyword in the result of last Parse function
     if the keyword is 'goto' and both origin state and target state aren't true simultaneously
           AddNewTransition(failure);    // Add one transition caused by failure between the origin
                                         //state and target state
     else   guard=AddConstraint('&'failure); // Otherwise modify the constraint which exists in the
...
                                         //state with failure by using logical connective
           ReplaceConstraint( nmodel, guard);
}
Main ()
{
     Get (fmodel, nmodel); // Get the failure model and normal model of system
     IntegrateModel (fmodel, nmodel) // Integrate functional failure model and normal  behavior model
}
```

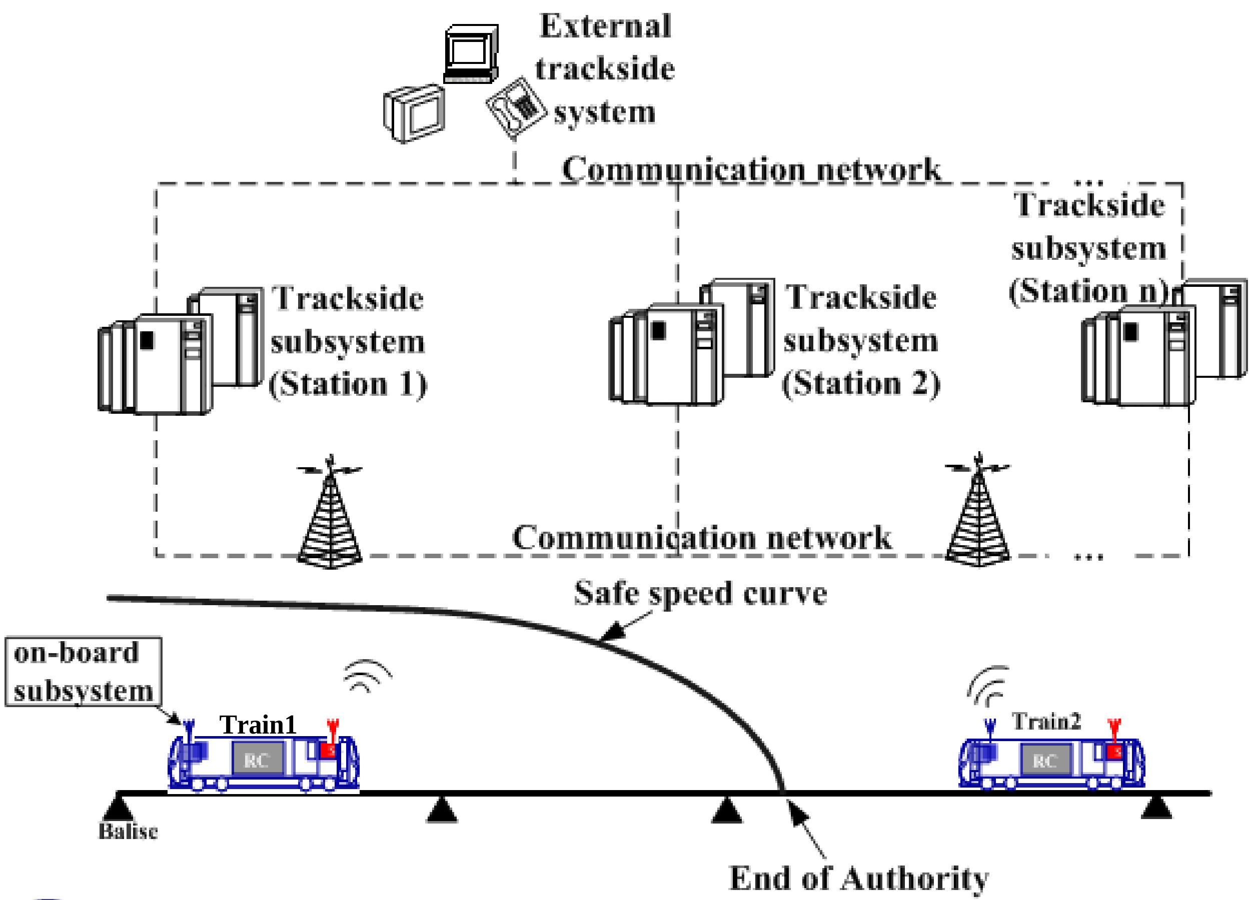
Definition 2 (*Monitor*). The fault events monitor is a structure $M=(S, A, f, Init)$, where, $S=\{s_1, s_2 \ldots s_n\}$ is the sets of states of the monitor, $A=\{a_1, a_2 \ldots a_n\}$ is the sets of fault events in the PHAVer model, $f: A \rightarrow S$ is the mapping function from A to S, $Init=S_0$ is the sets of initial states of the fault events monitor.

Outline

- Background and Motivation
  - Train control system in requirements phase
  - Hazard analysis on train control system
- Some ideas in using STPA in requirements phase
  - Internal Function Modules in Control Loops
  - Causal Factors
  - Formal model-based Causal Factors Analysis
- Case study : Chinese Train Control System
  - Chinese High Speed Railway Train Control System
  - Perform STPA on study case
- Conclusion

Case Study

➢ Chinese High Speed Railway Train Control System



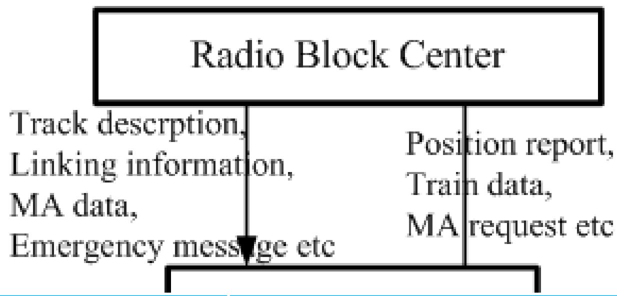
Reference structure of the system

◆One typical hazard of the system is considered: *The train control system does not protect the train against exceedance of the safe speed limits*.

◆The hazard can be traced to one system-level safety constraint that mitigates the hazard: *The train control system shall make impossible the violation of the safe speed limits.*

Case Study

➢ Control Structure



We take vital computer as example to illustrate the list containing internal function modules and inputs/outputs.

Internal Function Modules in Vital Computer	Inputs/Outputs
1 Supervision and protection	Input: Track description, Train data, System data, Location data, MA data, Emergency stop location, Session status Output: Train order, MA request
2 Train properties handling	Input: Driver input, Location data Output: Train data, Train integrity status, Position report
3 Data provision	Input: Track description, MA data, System data Output: Track description, MA data, System data
4 Emergency handling	Input: Emergency message, Revocation of emergency message Output: Emergency stop location, Acknowledgement of emergency stop

the
acks.
sent

Case Study

Step1: Unsafe Control Actions (UCAs)

Type	UCAs	Scenarios	Refined safety constraints
A required control action is not provided or is inadequately executed	UCA1.1 The train in over-speed doesn't receive the brake command from the VC.	The speed of train have been exceeded the speed limitation.	The train shall receive the brake command when the speed of train have been exceeded the speed limitation.
	UCA1.2 The VC doesn't receive the emergency message from the RBC.	The emergency situations happened.	The VC shall receive the emergency message in emergency situations.
	UCA1.3 The VC doesn't receive the route information or the speed restriction.	The route has the fixed speed limit.	The VC shall receive the route information and the speed restriction
			t MA
			e ed
			data
			e train
A potentially correct or adequate control action is provided at the wrong time	command to the train too late.	exceeded the speed limitation.	mand to the train in time.
	UCA3.2 The RBC shortens a given MA too late when necessary.	When the route has been changed in some situations.	The RBC shall shorten a given MA in time.
	UCA3.3 The driver releases the emergency brake too early.	The train has not been stopped completely.	The driver shall release the emergency brake when the train has stopped.

Type	UCAs	Scenarios	Refined safety constraints
A required control action is not provided or is inadequately executed	**UCA1.1** The train in over-speed doesn't receive the brake command from the VC.	The speed of train have been exceeded the speed limitation.	The train shall receive the brake command when the speed of train have been exceeded the speed limitation.

Hazard: The train exceeds the safe speed limits.

Case Study

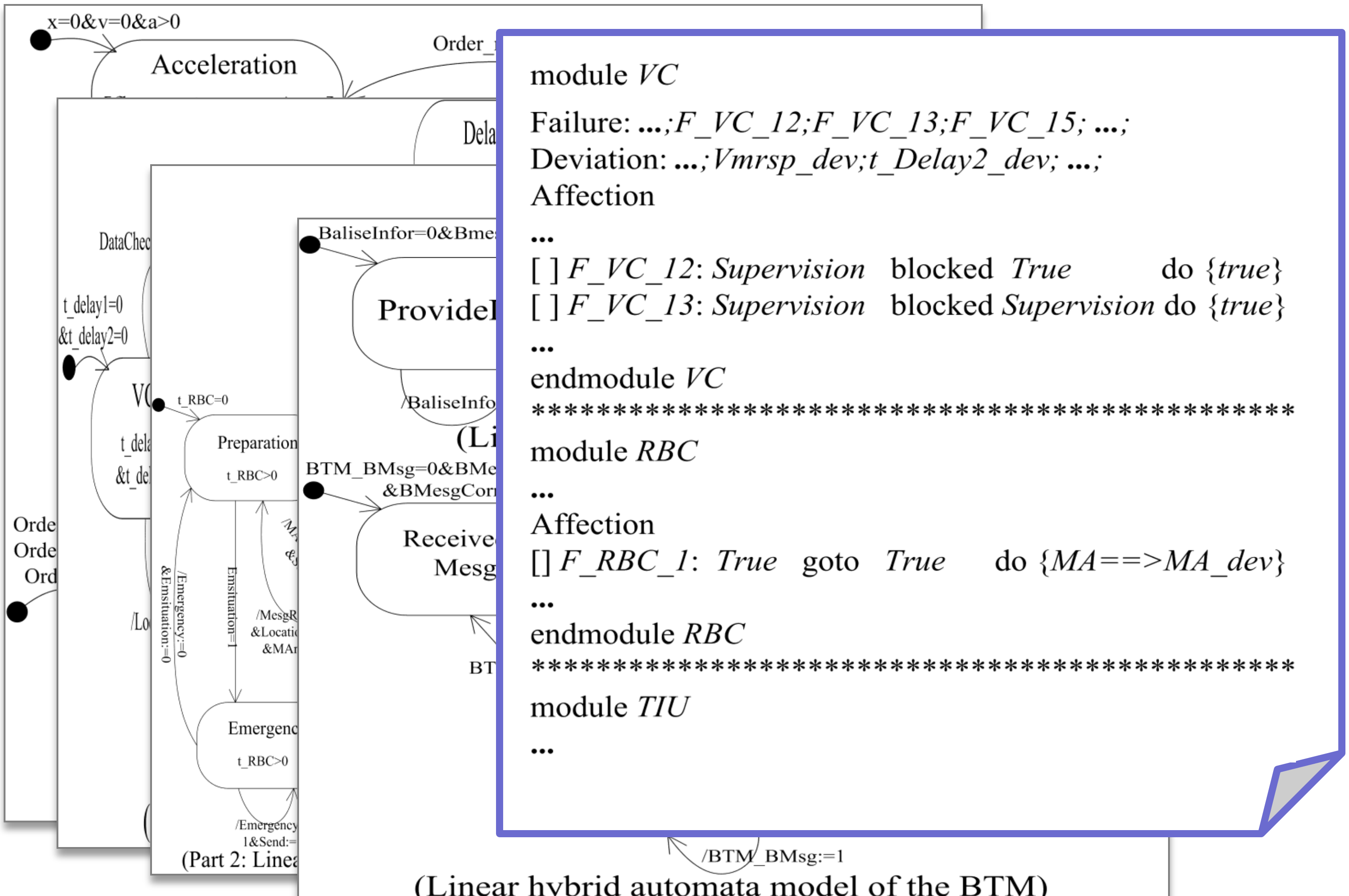
➢ Step2A: Inputs-related Causal Factors

Unsafe control actions (UCA)	Inputs-related causal factors(ICF)leading to unsafe control actions
UCA1.1 The train in over-speed doesn't receive the brake command from the VC.	ICF1.1.1: The actual speed used to compare with the speed restriction in the VC is incorrect. ICF1.1.2: The train data (e.g. train category, braking model, etc.) used for speed profile is incorrect. ICF1.1.3: The system data used to select brake commands in the VC is incorrect. ICF1.1.4: The emergency stop location in the VC is missing.
UCA1.2 The VC doesn't receive the emergency message from the RBC.	ICF1.2.1: The emergency situation which shall be known by the RBC is incorrect or missing. ICF1.2.2: The end of authority (EOA) used to evaluate emergency in the RBC is incorrect. ICF1.2.3: The location data received by the RBC is incorrect.
UCA1.3 The VC doesn't receive the route	ICF1.3.1: The route information and the speed restriction stored in both balise and RBC are missing.
UCA3.2 The RBC shortens a given MA too late when necessary.	ICF3.2.1: The route information in the RBC is not updated in time. ICF3.2.2: The location data in the RBC is not updated in time.
UCA3.3 The driver releases the emergency brake too early.	ICF3.3.1: The current speed provided by the DMI is incorrect.

Unsafe control actions (UCA)	Inputs-related causal factors leading to unsafe control actions
UCA1.1 The train in over-speed doesn't receive the brake command from the VC.	ICF1.1.1: The actual speed used to compare with the speed restriction in the VC is incorrect. ICF1.1.2: The train data (e.g. train category, braking model, etc.) used for speed profile is incorrect. ICF1.1.3: The system data used to select brake commands in the VC is incorrect. ICF1.1.4: The emergency stop location in the VC is missing.

Case Study

➢ Step2B: Formal Model-based Causal Factors Analysis



Case Study

➢ Step2B: Formal Model-based Causal Factors Analysis

Unsafe control actions (UCA)	Function module-related causal factors leading to unsafe control actions
UCA1.1V>Vmrsp+dv_sbi&Order_reqSB=0 or Lc>EOA&Order_reqSB=0	{F_SDU_3, F_VC_11},{F_VC_3},{F_VC_8}, {F_VC_9},{F_VC_12},{F_VC_14},{F_VC_15},

Unsafe control actions (UCA)	Inputs-related causal factors(ICF)leading to unsafe control actions
UCA1.1 The train in over-speed doesn't receive the brake command from the VC.	ICF1.1.1: The actual speed used to compare with the speed restriction in the VC is incorrect. ICF1.1.2: The train data (e.g. train category, braking model, etc.) used for speed profile is incorrect. ICF1.1.3: The system data used to select brake commands in the VC is incorrect. ICF1.1.4: The emergency stop location in the VC is missing.
UCA1.2 The VC doesn't receive the emergency message from the RBC.	ICF1.2.1: The emergency situation which shall be known by the RBC is incorrect or missing. ICF1.2.2: The end of authority (EOA) used to evaluate emergency in the RBC is incorrect. ICF1.2.3: The location data received by the RBC is incorrect.
UCA1.3 The VC doesn't receive the route information or the speed restriction.	ICF1.3.1: The route information and the speed restriction stored in both balise and RBC are missing.
UCA2.1 The RBC provides an incorrect MA for the VC.	ICF2.1.1: The location data used to generate the MA is incorrect. ICF2.1.2: The route information used to generate the MA is incorrect. ICF2.1.3: The train data received by the RBC is incorrect.
UCA2.2 Both RBC and balise provide incorrect route information and speed restriction.	ICF2.2.1: The route information and the speed restriction in both balise and RBC are incorrect.
UCA2.3 The driver inputs incorrect train data into the VC.	ICF2.3.1: The train data known by the driver is incorrect.
UCA2.4 The driver accelerates the train.	ICF2.4.1: The permit speed and the target speed displayed to the driver are incorrect. ICF2.4.2: The actual speed or the location data displayed to the driver is incorrect.

Case Study

➢ Comparison with traditional analysis

Analysis using FTA	Analysis using STPA
Inputs-related issues leading to the hazard are hard to analyze in detail. For example, *incorrect data to trackside constituents*	Inputs-related control flaws identified with the STPA method are more detailed, (missing, incorrect or not updating in time)
Some failures identified are mistaken for the single points of failures. For example, *SDU fail to determine the distance {F_SDU_3}*	Results are more complete. For example, {*F_SDU_3*, *F_VC_11*}
Once the hazard changes, the analysis needs to be performed all over again from the beginning to the end	Hierarchical control structure and the behavior models can be reused for analyzing another hazard as long as the system remains unchanged

Outline

- Background and Motivation
  - Train control system in requirements phase
  - Hazard analysis on train control system
- Some ideas in using STPA in requirements phase
  - Internal Function Modules in Control Loops
  - Causal Factors
  - Formal model-based Causal Factors Analysis
- Case study : Chinese Train Control System
  - Chinese High Speed Railway Train Control System
  - Perform STPA on study case
- Conclusion

Conclusion

- We found that STAMP/STPA is extremely useful for the train control system.
- We showed the specific implementation of STPA in the hazard analysis of train control system in requirements phase.
- Future work is suggested that more study should be carried out on identification of inputs-related causal factors with the formal methods.

Q&A
Thank you!

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