Study on the Accident-causing Model Based on Safety Region and Applications in China Railway Transportation System

Qin yong Ma hui Jia limin
State Key Lab of Rail Traffic Control & Safety
Beijing Jiaotong University
Beijing, China
yqin@bjtu.edu.cn

Ma hui Du Miao
School of Traffic and Transportation
Beijing Jiaotong University
Beijing, China

Du miao
Tianjin metro operation company
Tianjin metro operation company
Tianjin, China

***Abstract*—In order to quantitatively and systematically explain the accident occur process and assess the risk for the complex system, this paper proposes a new accident-causing analysis model, i.e. perturbation-safety region (P-SR) model. In this model, the safety region definition is introduced for the quantitative description of the system safe status; also the change process of the system risk is analyzed. The four relative parts included in this model are described in details, such as the risk resource part, the perturbation part, the alarm and system change part, and the accident part. Finally, the proposed model is applied to railway transportation system, and the Wenzhou train collision is systematically analyzed, also the specified control measure for the train emergency dispatch is demonstrated.**

Keywords-accident-causing analysis ;complex system; perturbation; safety region; railway transportaion system;

I. INTRODUCTION

Accident-causing theory mainly studies why accident happens and the mechanism of its process [1]. In order to prevent future accidents, the relationship of the causation found out in each part of procedure is established by disclosing the interaction of the components in the system. Traditional accident-causing theory, like Domino theory proposed by Heinrich in the 1940s [2], takes single element such as human, equipment or other causes separately into consideration as a chain or sequence of events [3], which explains well accidents caused by physical components and relatively simple systems [4]. Whilst systems we build today are increasingly complex that linear model is no longer adequate to capture the interactions and coupling within the system; thus it requires us to analyze the accident causation systematically as a whole. To catch up with the complexity, the accident theories developed via previous linear causation theories to present-day systematic theories, such as: system theory, perturbation accident-causing theory, energy transfer theory and information theory [5].

The systems approach addresses the notion that safety is an emergent property, which arises from non-linear interactions between multiple components across complex system and the relationship of behaviors implicated in operation [6]. In systemic safety models, the accident process is described as a complex and interconnected network of events to model the dynamics of complex systems [7]. Rasmussen's hierarchical sociotechnical framework [8] and Leveson's system theoretic accident modeling and processes [4] are two notable approaches. Even though these accident models considered the joint effect of multi-factors in an accident with their dynamic interactions, the descriptions of them (human, equipment, environment and etc.) are mainly qualitative, and the outcome of those interactions of system components are described respectively without an uniform expression. On the one hand, these models are sufficient to help us learn from accidents that have already happened, and thereby preventing hazards from the similar kind. On the other, as they hardly reveal the course of the outcome of system change, they are inadequate to guide real-time emergency response to prevent accident when the system is disturbed and prone to accident. This is mainly because the consideration of system state as a whole is lacked of in these models. And the challenges we meet today to achieve safety is going beyond accident analysis to the extent of resilience engineering [9]. Hereby, the accident analysis should also be able to implement in the real-time field work to prevent accident not only after but during its process, by enhancing its resilience against disturbance.

To achieve this goal, the conception of safety region, which depict the safe state affected by different factors in a unified way, is introduced with the combination of perturbation accident-causing theory to establish the perturbation-safety region (P-SR) accident-causing theory. In this theory, in addition to analysis causality systemically, the safe state of the system after perturbation is described quantitatively with the changing course of it in P-SR model. And then by exploiting

This study is supported by 863 Program of China's Ministry of Science and Technology, and Specialized Research Fund for the Doctoral Program of National Ministry of Education.

DOI reference number: 10.18293/SEKE2015-160

the safe state as risk assessment, the monitoring and evaluation of system safe state as well as the corresponding control measures are brought into the model to enable its practicability in safety management of production activities.

In this paper, the P-SR accident theory is illustrated in section Ⅱ,with detailed description of safety region and accident causing process. And then the application of the model is presented in section Ⅲ: (1) the whole accident course and the crucial safety factors of railway system is extracted by the reconstruction of Wenzhou train collision; and (2) a specific emergency railway safe state restoration method-train rescheduling- follows to illustrate the process of how the safety control measure works in real operation.

II. THE ACCIDENT-CAUSING MODEL OF P-SR

Inevitable as perturbation is in production activities, Amalberti [10] argued that these 'noises' (e.g. equipment malfunction or human errors) jeopardize operation safety; conceptually they should be symmetrically assessed and then calculate the associated risks. With new safety methods and perspectives that keep up with the continuously increasing complexity of industry, accident models aiming at explaining events and guide risk assessment need to match this complexity [11]. Specific to the complex system, the P-SR model promotes a quantitative description of the safe state and risk boundary of the system, which will better instruct safety monitoring and relative control measures. The concept, perspectives and processes are defined and described in this section.

A. The Definition of Safety Region

Safety region analysis have been applied to monitor the safety and stability of power system [12].The concept of region quantitatively describes the safety boundary of a system so that it could dynamically and consecutively monitor the system state with its changing process, and evaluate the safe state to provide warning information.

On the basis of the object studied in accident models, the safety region is defined as a changing space to describe the multifactor. Let $X=\{x_1,x_2,\cdots,x_n\}$ be the set of characteristic variables representing the characteristic state of the system, in which n is the number of the critical subsystem. The characteristic variables, derived from multifactor of human, equipment, environment, management or other factors, contain both discrete variables and continuous variables. Define space E as safety region: within the boundary of E is safe space; otherwise is accident space $\overline{E}$. The boundary is determined by the threshold of system safe state, i.e. the accepted risk level that can ensure system safety.

The safety region is determined as a n dimension space by the number of the characteristic variables n, in which the lower dimension spatial scope may vary with high dimension variables. Fig.1 gives an example of a 3-dimension safety region composed of $X=\{x_1,x_2,x_3\}$, in which x_3 is a discrete variable, representing two types of system state at this dimension: when $x_3=0$, the safety region is E_0; when $x_3=1$, it changes to E_1.

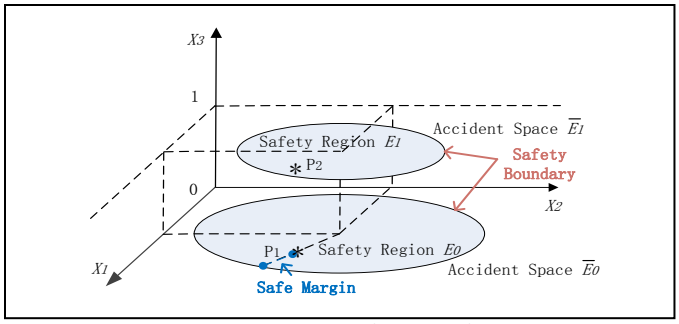


Figure 1. The change of system safety region

The boundary of the safety region is only determined specifically to a certain system. Usually, the state of the system located in safety region is called the balanced state. If the character point falls in the safe space, then the system is confirmed to be safe, with the distance between the point and boundary, called safe margin, to assess the safety level of the system. Otherwise, the point falls in the accident space when it breaks through the safety boundary, indicating that the safe state reaches an unacceptable level and then causes the accident.

In production activities, the system state continually deviates from safe space under the influence of perturbation. As it reaches a certain extent that beyond the safety boundary, the system enters the accident space. Fig. 2 show a safety region consists of 2 dimension variables $\{x_1,x_2\}$, in which P_1 and P_2 represent respectively system running safely and accident taking place. Obviously, the crucial task to use safety region to denote system safety is to obtain the safety boundary- a decision function returning a safe threshold that differentiate the state of safety and accident [13].

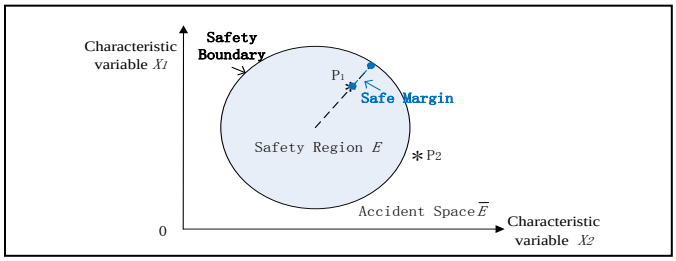


Figure 2. A schematic diagram of two-dimension safety region

B. The Analysis of Accident-causing Model Based on Perturbation-Safety Region

The P-SR accident-causing model (Fig.3) consists of four critical parts: the risk resource part, the perturbation part, the alarm and system change part, and the accident part.

To study the nature of accidents, in the first part, the risk resource is prominently analyzed in the perspective of energy carrier, followed by the analysis of the direct cause of perturbation. The moving device, electrified equipment, and containers loaded of hazardous chemicals constitute the energy carrier in the system, which is the material basis of an accident. And the severity of the accident is related to the types, quantity, property, status, and energy storage method of the energy carrier. Normally, the system maintains safety by effectively taking control of the energy. Only when the unsafe multifactor

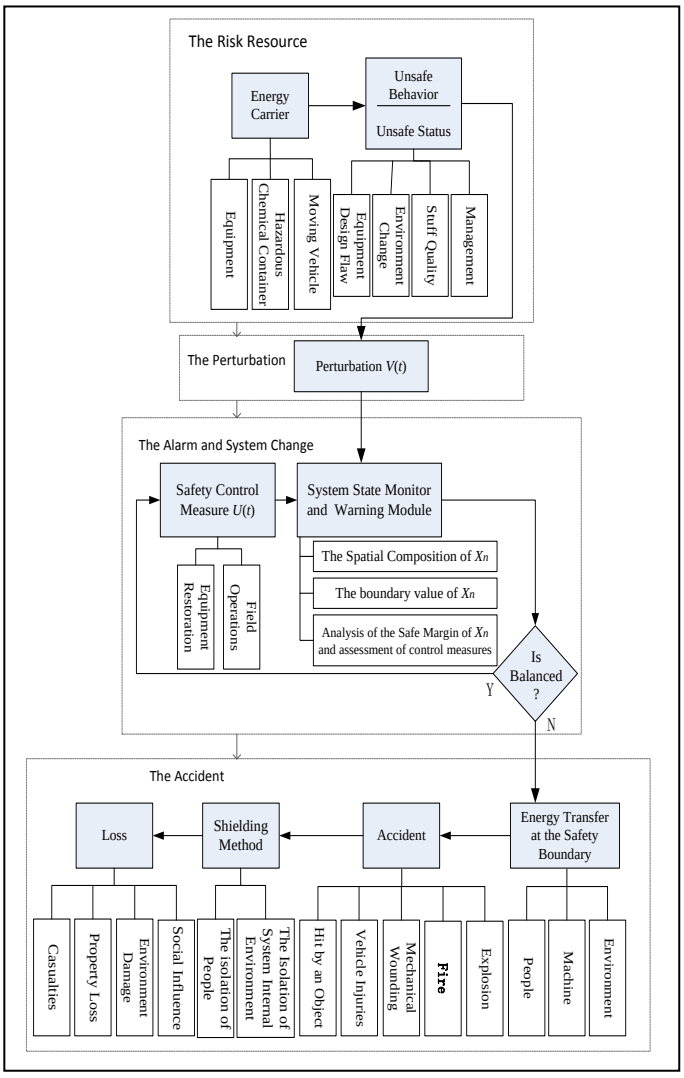


Figure 3. The Perturbation-Safety Region accident-causing model

disturbs the system will it result in failure of energy control- mainly because of the unsafe status and unsafe behavior:

- Unsafe status includes environment change and the defect of the equipment itself. First, natural disasters and extreme weather, e.g. lightning, earthquake, typhoon, debris flow and blizzard, are uncontrollable stochastic factors, which will influence the equipment and energy transmission in the system by causing the perturbation to the balanced state and further the accidental release of energy. Second, the equipment has problems of wear, deformation, and metal fatigue due to the long time use, thereby increasing the probability of mechanical fault. And the device itself may also have design flaws. Meanwhile, with the increasing complexity of the system, the dynamic interaction of each part is more complicated that the fault of single equipment may affect the whole system. Thus, the system is vulnerable to the unsafe state.
- Unsafe behavior mainly refers to the unsafe operation and management of human. The role people play in the system mainly includes: design personnel, operation staff, maintenance staff and management personnel. They together determine the reliability, stability and safety of a system. Yet each person is an individual with different quality, characteristic, education and etc. In the process of production, man's operation ability, management level and experience are closely related to system safety. Unsafe behaviors such as sneaking off in work, illegal operation, the decision-making mistakes, and loose management are the possible causes of an accident.

The effect of the unsafe state and behavior engenders the perturbation $V(t)$, shown in the perturbation part of the model in Fig.3, which is the direct cause that deviate the safe state from balanced state. The perturbation should be further analyzed in term of the specific system and situations.

As the controllers or decision makers are highly dependent on feedbacks to take action after perturbation, the necessary information about the actual state of the process is crucial to avoid accidents [4]. The question then arises about how we express and present the actual safe state. In the next stage, the alarm and system change part, the concept of safety region we introduced is the solution to this problem. At the beginning, the initial balanced state is expressed as $X(t)=\{x_1(t),x_2(t),\cdots,x_n(t)\big|x\in E\}$. After the perturbation, it changes to $X(t+1)=AX(t)+V(t),x\in E$, in which A is the system parameter. In order to ensure the system to still be in balanced after the disturbance, the changes of state in safety region need to be monitored so that the safe margin can be calculated. Then, according to the safe margin, corresponding prevention and control measures should be taken to rebalance the system. If the adopted measures are inadequate, the system will break the safety boundary and into the accident space. Herein, a system state monitor and warning module based on safety region is included in this part. As $X(t+1)$ moves to the safety boundary, the safe margin decreases; then the warning system generates alarm information; based on the alarm information, safety control measure $U(t)$ should be applied on the system, which is expressed as $X(t+1)=AX(t)+BU(t)+V(t),x\in E$ (B is the safety control parameter). If the system restores balance, it continues to monitor the change of safe margin and assess the control measures, so that the safety control measures module responds appropriately; if the system state broke the balanced state, it means undesired energy transfer has occurred and resulted in an accident.

Fig. 4 depicts the rebalance or accident procedure after perturbation under the action of system state monitor and early warning module (the arrows are the state locus, and the blue lines show the safe margin at each time).

The system is in balanced state before t_1. At t_1 the safe state begins to move toward the safety boundary under the effect of perturbation $V(t)$ .Then the warning module detects the reduction of the safe margin and raises alarm. Afterwards, the countermeasure $U(t)$ is applied at t_2 to slow down the decrease of safe margin. Later, the safe margin decreases slower at t_3, indicating that the system tends to restore the balanced state. Still, appropriate safety measures continue to be implemented

at t_3 . Finally the safe margin begins to move toward the internal safe space at t_4 , which means the system state has been effectively controlled, thereby avoiding the accident.

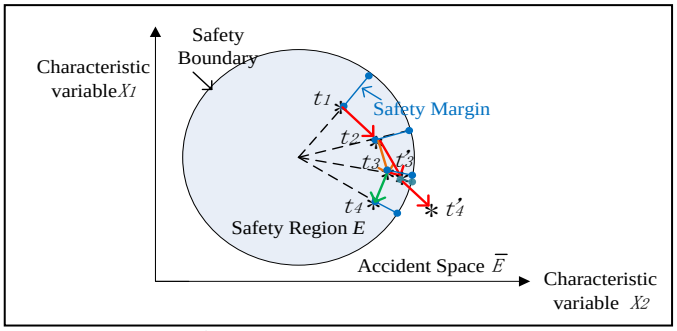


Figure 4. The trace of system state retrieving equilibrium state or heading to accident after perpurbation

Another trace in Fig.4 shows an opposite situation where the safety measure $U(t)$ fails to work. The difference is that the countermeasure taken at t_2 is far enough to slow down the decreasing speed of the safe margin. Thus, at $t_3^{'}$, the system state is already close to the safety boundary and keeps approaching it. Ultimately, the system state breaks through the boundary, with the energy (chemical energy, mechanical energy, kinetic energy, or electric energy) transferring to people, equipment, and environment.

According to the previous analysis, the safety control measure based on the monitor and warning module is critical to restore system safety after perturbation, as it decides the trend as well as the speed of the system state change. Therefore, in the accident prevention and control procedure, we should establish corresponding emergency plans specific to the object; and strengthen its disturbance control measures to reduce the probability of accidents, eventually avoiding the accidents.

Nevertheless, when the accident happens, there's still shielding method-the isolation of people, environment and energy carrier -we can take to control the damage degree of the energy release. If the shielding measure fails or not timely, the accident may cause severe direct loss like casualties and property loss, as well as the indirect loss such as damage of the environment, the social influence and the production stagnation, which is described in the accident part in Fig.3.

To sum up, the key of P-SR model is to extract the characteristic state variables of safety critical subsystem to build the safety region; and then determine the safety threshold to establish the safety boundary. That's when the system state can be quantitatively calculated as safe margin.

III. THE APPLICATION OF P-SR MODEL ON RAILWAY TRANSPORTATION SYSTEM

As China's railway transportation system thrives, the train speed is increasingly faster, train numbers are much denser, power supply capacity is bigger, and the multi-factors coupling is higher. With a lot of risk sources, the railway system is both an ultra-safe system and a typical complex system, confronted with enormous challenges of accident prevention and control. The P-SR model herein provides a solution to solve these problems as the following one accident analysis example and one emergency control example confirm.

A. The Wenzhou Train collision Accident Analysis

According to the accident investigation report established by State Council of China [14], the P-SR model is employed to analyze and reconstruct the Wenzhou train collision process so as to provide decision support for future accident prevention and the improvement of safety measures.

On 23 July 2011, high speed train D301 from Beijing to FuZhou collided with the high speed train D3115 from Hangzhou to FuZhou on Yongwen railway line, Wenzhou, Zhejiang province, China. The analysis of the accident based on P-SR model is established in Table Ⅰ.

As the relative speed and positon of a train with adjacent trains is the essence to control safety, this system safety-critical state space is defined as three-dimensional: train running control mode, train speed and train interval. So the safety region is also three-dimension, in which the train running control mode is discrete variable with the value of automatic block control or manual control; the train speed is continuous variable ranging from 0~350 km/h; the train interval is discrete variable indicating the number of blocks between two trains running on the same rail at same direction. To facilitate the graphical display of the safety region, the traffic control mode is set as a third dimension, thus we can describe the changing of the system's safe state in two-dimensional space.

Previously we introduced that the special extent of the safety region in dimensionality reduction space is possible to vary with the value of high-dimension variables. In this example, along with the change of train running control mode, the boundary of the two-dimensional safety region made up by the train speed and train interval changes as well (see Fig.5). In automatic block control mode, also the normal operation mode, the safety space is in a large range as shown in area E_0 ; while in manual control mode, the spatial extent of safety region reduces to E_1 , as Automatic Train Protection (ATP) requires the speed to be lower than 20 km/h and the train interval is required to be as the distance between adjacent stations.

The system safety region composes of the velocity v (km/h) of the first train running onto the section and the interval of the subsequent train *n* (the number of the blocks between two successive trains). In automatic train control mode, the safety boundary is made up by the safety threshold of the train running speed of 250 km/h and the minimum safe interval of 2 blocks, as $E_0(v,n)=\{v\le 250, n\ge 2\}$. In the manual mode, the safety threshold of the speed changes to 20 km/h and the minimum safety interval increases to 3 blocks, as $E_1(v,n)=\{v\le 20, n\ge 3\}$, for sufficiently stopping the train before any collision.

The safety region is E_0 at t_1 , when D3115 set off from Yongjia station at a normal speed onto the section under automatic train control mode. However, the control mode changed into manual mode at t_2 , with the safety region narrowed down to E_1 . Soon after, D3115 was stopped by the ATP when running onto the track 5829AG with faulted track circuit. At the time of t_3 , D301 entered the same section

TABLE I. THE ACCIDENT-CAUSING ANALYSIS OF WENZHOU TRAIN COLLISION

Items			Content
Energy Carrier			Moving motor train unit
Trigger Factors	***Unsafe Status***		1. The lightning activity was unusually intensive alone the Wenzhou-Yongjia and Wenzhou-Ouhai railway line; 2. The host in the train control center only transfer the fault message received the from track circuit to the monitor and maintenance terminal, while continuing outputting the signal control message according to the occupancy of track at the last moment before malfunction (the track was free so the control center authorized green signal). 3. The integrated wireless communication devices in D3115 lost its signal, so the driver couldn't connect to train dispatcher in time.
	Unsafe Behavior	Management	1. The equipment design company had severe defects in the design process and quality control of control center equipment 2. The project director ministry had a series of management failures on equipment bidding, technical examination and inspection for service for newly developed signaling equipment 3. The field work company had loopholes and deficiencies in safety management and failed to adequately respond to equipment malfunction caused by lightning.
		Operation	1. The field stuff didn't perform joint interaction control of train running and track ocuppancy under manual mode. 2. The D315 was authorized onto the section at automatic control mode without confirmation that the D3115 had arrived at the next station or the equipment had restored to work normally.
The perturbation			1. The lightning struck a trackside signal assembly, burning out its fuses F2, while the transmitter in track circuit 5829AG lost connection with the control center. 2. The control center gave an incorrect indication, based on the state before the fault when the track was free, that the track section containing train D3115 was unoccupied, thereby allowing the signal instruction staying green. 3. Due to the communication error between 5829AG track circuit and control center, 5829AG track circuit began to send messy code, causing the computer interlocking system in Wenzhou south station displayed red bond on the corresponding section. 4. As D3115 run onto the malfunctioned track 5829AG, the messy code transmitted to the train triggered automatic braking of ATP, so that D3115 came to a halt with 3 times failure to override the system into visual driving mode.
The monitor and warning			1. The computer interlocking system in Wenzhou south station appeared 'red band'. 2. The frequency shift track circuit terminal at mechanical room in Wenzhou south station displayed red alarm light 3. The last two communication boards in the track circuit interface unit in Wenzhou south station indicated red warning light. 4. The computer interlocking system in Wenzhou south station appeared 'red band', while the Centralized Traffic Control System (CTC) in dispatching station didn't.
Safety measures			1. The track maintenance workers walked alone the Wenzhou-Ouhai and Yongjia-Wenzhou railway line to check the occupancy of track. 2. The railway electricity workers attempted to restore the faulted equipment. 3. The train control mode was change from automatic control into manual control mode in Yongjia station, Wenzhou south station and Ouhai station. 4. The dispatcher instructed the driver of D3115 driving under visual mode at a speed lower than 20 km/h, when encountering red light in the section.
Accident Space			
Energy Transfer			Train D301 ran at 99 km/h crashed into the rear-end of the D3115 run at 16 km/h.
Accident			The 15th and 16th coaches at the rear of D3115 and the front five coaches of D301 were derailed.
Shielding			The driver of D301 pulled on emergency brake at the sight of D3115.
Loss			40 people were killed and 172 injured; 7 motor train set vehicles was scrapped, 2 broken heavily, 5 broken at medium, 15 broken slightly; the network of Overhead Contact System in accident section collapsed; the railway line at accident section shut down for 32 hours and 35 minutes.

TABLE II. THE MONITOR AND WARNING INFORMATION IN WENZHOU COLLISION AND CORRESPONDING EVALUATION

Time	The monitor and warning of equilibrium state	Safety measures	Safety Region	Safety Margin	Evaluation of safety measures
t_1	None	None	E_0	equilibrium state	—
t_2	The inconformity of the display in CTC and train control center	The train control mode was change to manual control mode in Yongjia station, Wenzhou south station .	E_1	Increasing	Effective
	Track circuit sent messy code	D3115 was stopped by the Automatic Train Protection (ATP)	E_1	Increasing	Effective
	None	The driver of train D3115 overrode the ATP and drove at visual mode.	E_1	Decreasing	Failed
t_3	None	The following train D301 approached onto the section of track where D3115 had been stopped at automatic mode	E_1	Decreasing dramatically	Dangerous
t_4	None	Emergency brake of D301	E_1	Enter accident space	Slight

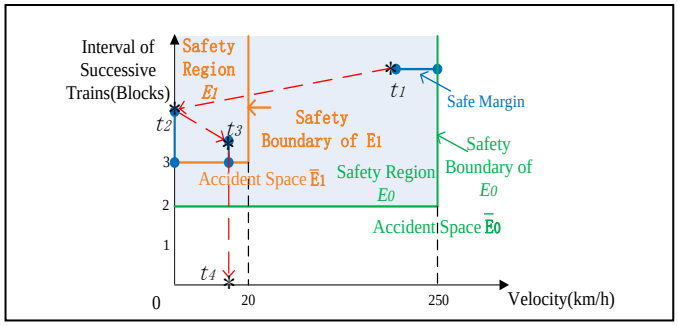


Figure 5. The evolution of system state in Wenzhou train collision based on safety region

occupied by D3115 as a way of the automatic mode, which it shouldn't. Two minutes later, D3115 finally overrode the ATP to start the visual driving mode. Nonetheless, the interval between these two trains decreased sharply at this time. As there was no effective warning, no imperative safety measure was taken. Thus the safe margin diminished dramatically. Eventually, D301 collided with D3115 at t_4 that the system state broke through the safety boundary, with energy transfer, causing the accident. The course of the accident is shown in Fig.5 as red arrow lines. The warning and monitor information with relative safety measures at each time is evaluated according to safe margin in Table Ⅱ.

According to the analysis of the P-SR accident-causing model, it is the joint efforts and the interaction between multiple factors that put the system at risk of accident. However, it is the control measures that finally decide whether an accident will happen or not. In Wenzhou train collision accident, the safety measures adopted according to the early warning has somewhat maintained system safe margin. But when the system neither obtained the early warning information in the field, nor did any imperative human or equipment safety control measures are taken, the system safe margin began to drop dramatically until the accident happened.

B. Specified Application of the Safety Control Measures

This section focuses on the system safety control measures to restore the order of the system. Specific to the railway system, train dispatching and rescheduling is the imperative method to ensure both the operation safety and transportation capability of the whole system, as essentially they avoid the time and space conflicts between different trains, which is the decisive factor to the range of safety region. Therefore, a train rescheduling method is specially proposed in this part.

1) The principle and strategy of train rescheduling

When the railway system is in unbalanced state, strategies to restore the system need to follow certain principles.

a) Principles of train rescheduling

- Schedule the train in the original path and avoid detour and outage to the greatest extent;
- When detour is necessary, check the train and the line conform or not and choose the shortest one;
- Higher grade Trains can't be overtaken by lower ones;
- Passenger trains can't be overtaken by freight trains;
- The punctual trains have a higher priority.
- Passenger trains can arrival in advance but can't departure in advance.

b) Strategies for train rescheduling

- Detour, outage, reconnection and turn-back can be adopted when necessary;
- Change the section running time;
- Change the dwelling time in station;
- Change the overtaking station or time.

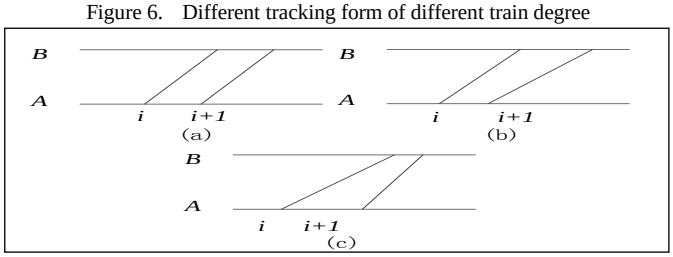
2) Rescheduling method

The process of train operation is discretized, so the rescheduling can be got one section by one section.

Paper [15] summarizes 3 rules for the events dispatching. A first-to-start dispatcher selects the next train to be moved based on the earliest start time. A first-to-finish dispatcher selects the next train to be moved based on the earliest finish time on its next segment. Other possible dispatchers can be created by setting the dispatch decision time for train i as $t_i = (1-\delta)u_i + \delta v_i$, where u_i is the start time for train i and v_i is its expected finish time on its next immediate segment and $\delta \in [0,1]$.

While the trains' grades are not considered in the dispatching rules mentioned before. As the grades are different between the neighbouring trains, there will be 3 situations: the neighbouring trains have the same grades (Fig.6(a)), higher grades train run after the lower grade train (Fig.6(b)), and lower grade train run after the higher grade train (Fig.6(c)).

Figure 6. Different tracking form of different train degree



When the actual start time of trains (AST) in each section is obtained, the timetable is got too. So the calculation of AST is the key of the problem. In this paper, AST is calculated by the formulas in Table III.

TABLE III. FORMULAS FOR THE ACTUAL START TIME

(a)	If $s''_{i+1} - s_i \geq I$	then $s_{i+1} = s''_{i+1}$, $s_i = s_i$
	If $s''_{i+1} - s_i < I$	Then $s_{i+1} = s_i + I$, $s_i = s_i$
(b)	If $s''_{i+1} - s_i \geq I$	Then $s_{i+1} = s''_{i+1}$, $s_i = s_i$
	If $s''_{i+1} - s_i < I$	Then $s_{i+1} = s_i + I$, $s_i = s_i$
(c)	If $s''_{i+1} - s_i \geq I + t_i - t_{i+1}$	Then $s_{i+1} = s''_{i+1}$, $s_i = s_i$
	If $s''_{i+1} - s_i < I + t_i - t_{i+1}$	Then $s_{i+1} = s''_{i+1}, s_i = s_{i+1} + I$

In Tab. III, s_i stands for AST, while $s_i^{"}$ stands for the earliest start time (EST). The two concepts can be distinguished that AST is EST considering constrains between trains. EST can be got by two factors, a) the reckoning time according to AST and section running time in last section and the operation time in last station, b) the start time in the original timetable. We choose the bigger one as the result. It can be seen in (1).

$$s_k^{"} = \max(s_{k-1} + t_{k-1} + t_j, s_k^*) \tag{1}$$

Where, $s_k^{"}$ stands for EST in section k, s_{k-1} stands for AST in section k-1, t_{k-1} stands for the running time in section k-1, and t_j stands for the operation time in station j.

On account of factors such as weather, track condition, equipment condition and etc., the velocity of trains is not constant. So we consider the pure running time as a variable number. The section running is depicted in (2).

$$t_p = \alpha_{p-1}\tau_q + \alpha_{p+1}\tau_t + t_p + \delta \tag{2}$$

Where, α is a 0-1variable representing whether train stops in station or not, τ_q and τ_t stand for the addition time of start and stop, t_p stands for the pure running time, δ is a stochastic number.

The variation of section running time enriches the problem space, and we can find a better solution. The value of δ is vital to the quality of the result. R. Albrecht [16] made many experiment to obtain a more proper value in his doctoral dissertation, finding that when distributed normally (that is $\delta \in N(0, \alpha_T)$ and $\alpha_T = m/2$ [15], the result could be better. m stands for the section running time. The conclusion is still applied in this paper.

The algorithm is depicted in the following.

Step1: Choose all the events in section I,

Step2: Calculate the earliest start time of section *i* according to formula (1),

Step3: Calculate the actual start time of the section event according to table III,

Step4: Do i=i+1 until the last section,

Step5: Repeat step 1 to step 5 N times (N is determined by decision maker, it can be 100 or another), thus we have N feasible schemes, and find the best solution according to the object function among the N feasible schemes,

Step6: Draw the adjusted train diagram.

3) An experimental example of the method

The results of using the method before are discussed here for a representative example on Jin-qin passenger railway (approximately 260km with 9 stations), China. The case is based on real data and a scene with disorder is assumed.

The assumed scene: the section Junliangcheng north station to Binhai station suffered heavy rainfall during the period 13:00 to 17:00. And the allowed speed of the trains passed by then is 100 km/h. Because of the bad weather, 11 trains are late. So a quick adjustment of train timetable is needed.

We take the minimum deviation between the original timetable and the adjusted timetable as objective, then carry out the algorithm before with related data and the output objective distribution is shown in Fig.7. The results are normal distributed. The result with minimum deviation time is an ideal scheme and the rescheduled timetable is shown in Fig.8.

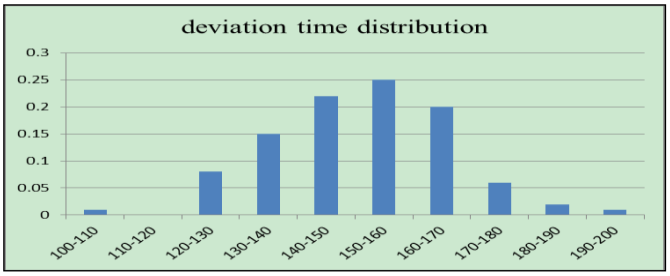


Figure 7. Objective distribution with variable running time

We can see that in Fig.9, D6795 is a train with lower grade compared to others and in order to cause larger deviation it is overtaken by train G1253 in Binhai station only. In this case the objective number is 109.3672 and the result can be got in an acceptable time. The method has also been applied with success to a range of test problems with various network sizes, number of trains and works well.

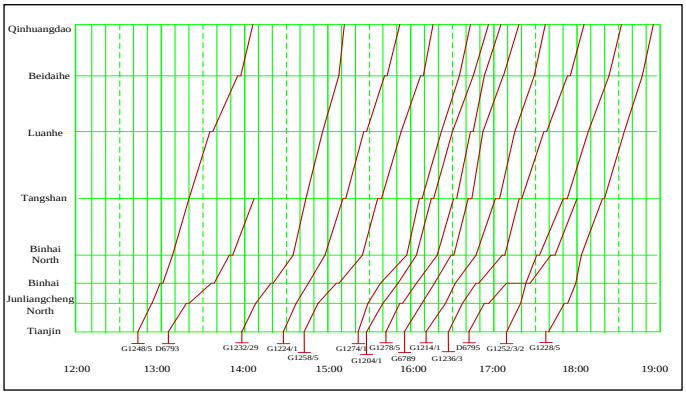


Figure 8. Train timetable with variable running time

IV. THE CORRESPONDING PREVENTION MEASURES

Besides the control measures, on the basis of the theory and analytical method of the P-SR accident model, we can further conclude the following preventive measures against accidents:

(1) Strengthen the implement of technical engineering in the system changes and control measures parts. As the external disturbance is almost inevitable, to maintain system balanced state is the critical process to prevent an accident.

(2) Strengthen the monitoring of the system running state and quantitative analysis of safety region, so as to timely reflect the safe state of the system. And then offer the safe state analysis and early warning information to provide basis for adopting corresponding control measures;

(3) Take comprehensive and effective safety control measures based on safe state and early warning information,

and at the same time constantly monitor the system state to assess the effectiveness of safety measures to adjust inappropriate control measures in time.

(4) Strengthen the construction of emergency management and human emergency response. As human bears huge psychological pressure when the system works out of order after disturbance, they are likely to make inappropriate decisions or take unsuitable actions that may aggravate the reduction of system safety margin.

V. CONCLUSION

This paper presents a new accident model, perturbation-safety region accident-causing theory model, to analyze complex system, based on perturbation occurs theory and system theory. The model we proposed focuses particular attention on how to measure safe state of the system as a feedback to control measures and how the relative control measures are taken according to that feedback. Instead of analyzing safety in the context of preventing component failure, it addresses the continuous monitor and control task after perturbation. Accidents are seen as resulting from inadequate or inappropriate control measure during system design, daily operation and emergency response. The process of an accident is captured from (1) intrinsic nature of the dangerous resource in the system, and then (2) the perturbation brought up by the unsafe state and behavior that deviates system from safe space, to (3) the alarm and monitor part that uses safe margin to guide corresponding control measure with assessment of it. Ultimately, the accident can be understood in terms of why the control measure enforced in a disturbed system fails to stop the progress of it. Specifically in the model, the system safe state depict by safety region visualizes the course of an accident by safe margin, which evaluates how close the system is near to accident space. This allows controllers or decision makers to have the crucial feedback to adopt appropriate measures.

Hence, the P-SR model also overcomes the limitation that most accident models do not apply in real-time work. The results of the analysis not only contains static charts or figures, but also a dynamic system state diagram that monitors the system continuously, which could be implemented in real work to maintain safety. Through learning the progress of an accident, the notion of the model changes from the passive analysis after accident to the initiative safety restoration before accident. The necessity of this change lies in that the potential interactions between components in a system is rather complex that they are hard to understand and anticipate. So the common accident models, chain events or dynamic networks, focusing on how to prevent accident by exposing flaws in physic parts and behaviors with their interrelations, is not enough to keep up with the safety management needed in different kinds of system and perturbation. And yet the model we present builds a unified mathematical expression frame to describe the change brought up by multiple factors, which elevates the quantitative analysis ability for complex systems.

The validity of the model has been proved as the analysis and reconstruction of a typical railway accident in China case shows. To further illustrate the role that control measures take in a disturbed system, a railway emergency command method is proposed in this paper to back up the safety restoration with respect to the perturbation in daily operation.

The concept of P-SR model is suitable to improve performance in safety management. But there are still problems to be solved before the application, like (1) the safety region of each different system should be specified; (2) the characteristic state variables are crucial to the whole analysis that omitted variable may also increase the risk of accidents; (3) massive amounts of data are needed to be collected and analyzed.

ACKNOWLEDGMENT

This study is sponsored by the 863 Program (2012AA112001) of China's Ministry of Science and Technology, and Specialized Research Fund for the Doctoral Program (20120009110035) of National Ministry of Education. The support of State Key Lab of Rail Traffic Control & Safety of Beijing Jiaotong University is also gratefully acknowledged.

REFERENCES

[1] A. Kuhlmann, An Introduction to Safety Science,Germany, 1981.

[2] Heinrich, H.W., Petersen, D., Roos, N., Industrial accident prevention: a safety management approach, fifth ed, The U.S.:Mcgraw-Hill,1980.

[3] H. Xueqiu, Safety Engineering, China: China University of Mining and Technology,2000.

[4] Nancy Leveson, "A New Accident Model for Engineering Safer Systems," Safety sciecnce, vol.42, No.4,pp.237-270, April,2004

[5] China higher education committee in Safety Engineering Guidancs, Security System Engineering, China:China Coal Industry, 2002.

[6] Paul M. Salmon, Natassia Goode,Frank Archer, Caroline Spencer,Dudley McArdle, Roderick J. McClure,"A System approach to examining disaster response: Using Accimap to describe the factors influencing bushfire response," Safety sciecnce, vol.70, ,pp.114-122, December,2014.

[7] YunXiao Fan, Zhi Li, JingJing Pei, Hongyu Li, Jiang Sun, "Applying system thinking approach to accident analysis in China: Case study of "7.23" Yong-Tia-Wen High-speed train accident," Safety Science, vol. 76, pp. 190-201, July 2015.

[8] Rasmussen, J., "Risk management in a dynamic society: a modelling problem," Safety Science. Vol. 27, pp. 183–213 1997.

[9] Hollnagel, E.,Investigation as an impediment to learning. In: Hollnagel, E.,Nemeth, C., Dekker, S. (Eds.), Remaining Sensitive to the Possibility of Failure,Resilience Engineering Series. The U.K.: Ashgate, Aldershot,2008 .

[10] R Amalberti, "The paradoxes of almost totally safe transportation systems," Safety Science, vol. 37, pp. 109-126, March 2001.

[11] Rogier Woltjer, Ella Pinska-Chauvin, Tom Laursen, Billy Josefsson, "Towards understanding work-as-done in air traffic management safety assessment and design," Reliability Engineering & System Safety, March 2015.[Online]. Available: Elsevier, http://www.sciencedirect.com.

[12] X. Ancheng, Wu, F., F., L. Qiang, M. Shengwei,"Power system dynamic security region and its approximations," IEEE Transactions on Circuits and Systems I: Regular Papers, vol.53, pp.2849-2859, December 2006.

[13] Q. Yong,S. Jingxuan,Z. Yuan,Z. Shengzhi,J.Limin, "Online Security Assessment of Rail Vehicles in Service Status based on Safety Region Estimation," Journal of Central South University(Science and Technology), vol.44, pp .195-200,July 2013.

[14] The State Council of China, Yongwen Railway Line Major Traffic Accident Investigation Report ,China, December 2011.

[15] Albrecht A R, Panton D M, Lee D H., "Rescheduling rail networks with maintenance disruptions using Problem Space Search," Computers & Operations Research, vol. 40, pp. 703-712, September 2013.

[16] Amie R. Albrecht, "Integrating railway track maintenance and train timetables",University of South Australia,2009.