International Journal of Hybrid Information Technology
Vol.8, No.12 (2015), pp. 97-116
http://dx.doi.org/10.14257/ijhit.2015.8.12.06

A Hybrid System Dynamics Modeling Method for Organizational Factors in Fully Automatic Operation System

Bobo Zhao[1] and Tao Tang[2]

[1]*National Engineering Research Center of Rail Transportation Operation and Control System, BeijingJiaotong University, Beijing 100044, China*
[2]*State Key Laboratory of Rail Traffic Control and Safety, BeijingJiaotong University, Beijing 100044, China*

Abstract

The Fully Automated Operation (FAO) system is the new developing trend in the railway domain in China. However, FAO poses an operational risk because the operator lacks the operational experiences of new system so that it is difficult to determine fault property and process of revenue service. The paper attempts to explore the nature of changing mechanisms of organization integrated with human factors as a process and to single out the latent causes of failure in FAO system. In order to analyze the organization's risk, a Viable System Model (VSM) is adopted to explore the control flaws of FAO system's organization from the Systems Theoretic Accident Model and Processes (STAMP). Meanwhile, with respect to detecting the causal relationship and revealing deeper reasons of the control flaws of organization, we propose a set of dynamic archetypes of pattern of organizational breakdown based on the system dynamics. The recursion of constrains and process inherited by STAMP provides the feasibility and vulnerability over prediction and recovery process of system operation and management. The hybrid system dynamics modeling method, combining VSM and system dynamics, can help to predict the organization risks, monitor the drifting safety boundary, analyze the boot cause in accident, and support the recovery of inappropriate feedback of organization in FAO system.

1 Introduction

The Fully Automated Operation (FAO) system poses an application trend in China as well as bringing out the new fault property and the process of FAO system's revenue service. Meantime, more and more studies propose the human and organizational factors may become the root cause of accident. The increasing complexity of system has led to human-organization-machine techniques integration focusing on the system theory to analyze system safety. The safety is not a response of barriers of several events but it needs proactive protections and adequate constrains for whole system including organization process in management. As a result, in view of system theory to analyze influence of human and organizational factors in socio-technique system is a developmental tendency in safety literature.

In order to coordinate key safety requirements of devices with human behavior and organization performance to assure high-quality engineering and operational management, it is significant to build a dynamic control model of human-organization to accommodate circumstances. The ultimate goal is to explore the nature of changing mechanisms of organization integrated human factors as a process in FAO system. Acquisition of the complex attributes changing in new system to understand the intrinsic characteristics clearly makes the possibility of controlling the risks of FAO system in a limited range. This paper attempts to find out the negative factors which lead in high risk in FAO system, and expose the key evolution of patterns of organizational breakdown which can be managed in an effective way.

ISSN: 1738-9968 IJHIT

The concept of system safety literature concludes two original ideas: a safety thought of a “control problem” and safety needs a “system theoretic” approach [1]. Modern safety analysis techniques have shifted from single component failure to system theoretic approach, such as Accimaps [2], FRAM [3], STAMP [4], which concentrate on the complex relationship and interaction between elements of the overall system. The Systems Theoretic Accident Model and Processes(STAMP) was presented to analyze the accident in a system view, which transfers the problem into safety constraint question in control model at each control hierarchical [4]. But the method of STAMP has a weak point at analysis of organization level, hence a more flexible method should be integrated and supplemented for the theoretical model of organization. Recently the study of organization's aspect is trending toward the 'prediction' and 'proactive or leading indicators' of safety performance in organization. The Viable System Model (VSM) was proposed to keep the organization's viability and balance itself with the environment [5]. Some accident study has used VSM to analyze organizational factors [6, 7]. In order to take a less gap between organizational models and techniques of investigation for an overall system perspective, Kontogiannis and Malakis [8] elaborated the method of STAMPbased on VSM and revealed several patterns of organizational breakdowns in a Helicopter Emergency Service. A perception has been proposed that the creation of system deficiencies and organizational vulnerabilities, rather than their eventual presence, should be considered into safety models. A further STAMP-VSMjoint framework has been presented which extends proactive assessment of breaches of safety constraints and causal organizational breakdowns in systemic safety approaches [9].

It is shown that accident happened when the risk has been drifting over several years toward a high state, but no change in usual behavior [10]. In order to trace risk over the dynamics system process, the system dynamics has been combined with STAMP to design a dynamic risk management model [11], and the model has been used to identify the increasing risk, create and test risk mitigation action. A further approaches of accident analysis and hazard analysis from system dynamics have been proposed, considering principles found in the human factors, organizational safety and system safety literature [12]. In the synthesis, system dynamics plays an important role in viable analysis of the device and organization in socio-technology system, and also can assist to settle nonlinear problem defective in traditional system theory. In the recent decade, the organizational factors plays a key role in all kinds of accident, and particularly it is a root cause in catastrophic accident sharp end. Another trend is the development of organization's resilience study across the life-cycle of operational management, in order to diagnose the dynamics feedback loop and casual relationship in the hazard identification to provide safety risk management. There have been general system behavioral and organizational behavior archetypes study with system dynamics [13, 14]. An initial set of six system safety archetypes modeling based on system dynamic has been proposed to explain common behaviors of dynamic organizational factors often led to accidents [15]. Furthermore, system dynamic archetypes have been studied as variants of two generic templates of ECOM and VSM, which explore many elements of complexity theory and system control [16]. All these archetypes only express general behaviors related system attitude and safety issue, but there is no available system approach to control organizational constraints and transfer the flaws to operational process toward a status of system safety in FAO system, particularly lack of archetypes related organizational dynamic mechanisms, which can obviously explain the latent interaction relationship of whole system and organizational risk drifting tendency.

It is difficult to explicitly define the human and organization interaction relationship and locate the final result in more complex system. We can hardly predict the terminal result but can trace the dynamic evolution of system safety boundary, and monitor the risk and prevent catastrophic accident. In this study, a VSM model applied in the special FAO system is raised to help the safety analysis of inadequate constraints of organization, and

the dynamics models of organizational safety process in the system are proposed to further reveal the deeper reasons of the control flaws of organization. Thehybrid system dynamics method combining system dynamics and VSM can help to predict the organization risks, monitor the drifting safety boundary, analyze the boot cause in accident, and support the recovery of inappropriate feedback of organization in FAO system.

The study focuses on the FAO system working in the grade of automation level 4, which has no attendant in train [17]. The ultimate aim of the research is to find out the intrinsic causal relationship and keep the reliance in operational management of the FAO system after the increase of automation level. In the second section, we understand and grasp the essential changing quality between FAO system and traditional system particular in organizational management and technique investment. In the third section, a VSM model of FAO system's organization is applied to identify control flaws based the basic classification, for the aim to analyze the reasons why result in the control flaws. In the last section, a set of archetypes is considered organizational factors of safety process in FAO system in detail. Five kinds of archetypes are presented to perceive the dynamics process formed in the new organization system, and they can be used to bring out how the FAO system will work toward a healthy direction and what organization should do in a new situation.

2. The FAO System and the Organization Model

As the socio-technical system becomes more complex along with integrated technology in urban rail transit system, the system confronts the difficulty with interactive mix application and adaption of combination between technological and organizational aspects to minimize the effect of risk.

2.1. The Technology and Organization System

In this section, we introduce FAO system and discuss apparent distinctions between traditional urban rail transit system and FAO system.

The FAO system needs to add the following functions based traditional system: (1) awake trains which are in stabling locations (in depot, sidings or in the line) before they enter service by remote action from the Operating Control Center (OCC);(2) set the trains to sleep in stabling locations (in depot, sidings or in the line) after they leave service by remote action from the OCC; (3) drive train automatically in main line and depot. In order to accomplish the automatic functions and ensure the management system to provide reliable and safe revenue service, the system should consist of three subsystems: the FAO train control system, the FAO station passenger management system, and the FAO train management system as shown in Figure 1. The architecture of FAO system has the hierarchical control functions of the entities: passenger, train and revenue service, which are controlled and supervised by a socio-technique system including operators, group and device. Operators work in an integrated process and the work team must cooperate and interact with each other for the effective and safe operation. Meanwhile, the system has no attendant in train; therefore, feedbacks are necessary to monitor the whole system status. There are three feedback loops: FAO train control system, FAO station system (passengers), and FAO operation system (operators). It is obvious that feedback loops of three subsystems can compensate the flaws when no attendant is in train, and the aim is to make operators in a well-known status of the whole system.

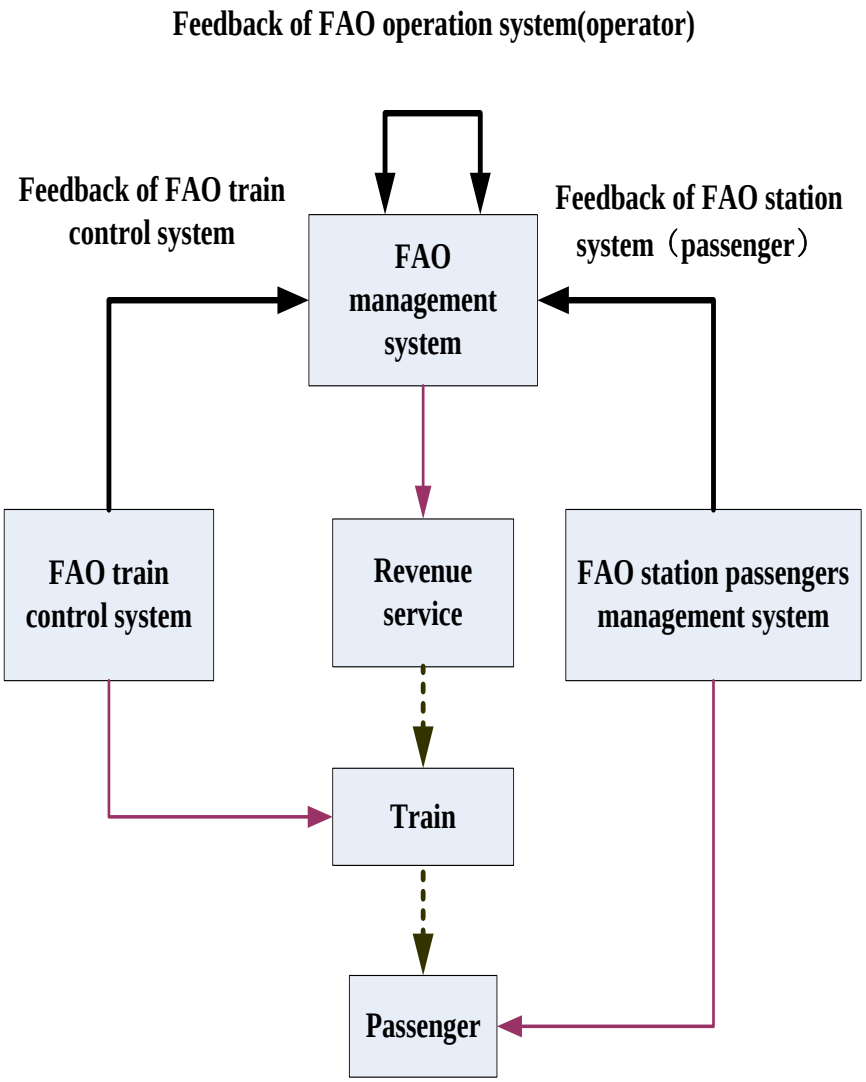

Figure 1. The Architecture of FAO Operational System

In the past decade, designers have focused on the task what devices can do and reduced driver's workload as much as possible, so driverless operation of urban rail transit system is realized. But it also causes side-effect ignored in practical operation over time. In automatic system such as FAO system, the system can't be separated alone for its complete automation, but should consider the aggregation reflection of interior interaction of system, organizational modality in new system and safety culture of organization. From the view of concept, new FAO system with the improvement of automation system faces the following problems: (1) constraints of practical operation understanding in new FAO system and influence of old experience in traditional system; (2) unknown status of system operation; (3) reduction of safety consciousness with technological progress;(4) re-allocation of team responsibility; (4) excessive confidence of system' safety; (5) inadequate feedback to human and organization.

Besides the axis of technology revolution in rail transit driverless system, a new organizational approach of automatic metro line is necessary to be combined with FAO system. Job assignment should include new responsibility, and the OCC takes the duty of central decision-making. The conflicting coordination of different work team in traditional system have been dissolved and shifted by internal reconstruction. Likewise, the absence of driver needs an appropriate organizational design that complements directly operation

of the service, and raises deep thinking of safety and operational questions in the condition of emergency incident. This can be a complex challenge for the new FAO system's operation followed with the organization construction and functions.

The upgrade of existing metro lines also makes significant changes within the operational models, characterized by an improvement and re-assignment in job profiles. For example, the instant contact between customer and operator should be added in system to provide the real-time service to facilitate passenger. An appropriate organization model, integrated with technology system, opens up the opportunity to overcome the disturbance and offers a remote service to passenger. For this purpose, processes of FAO system's organization should be redefined. It is believed that a good reconstruction for new organization will make the enough flexibility in train operation and passenger management in balance with the residence of safety.

In the following section, an operational model of FAO system's organization is proposed based on VSM and FAO's safety control structure.

2.2. A Organization Model of FAO System

The STAMP method takes the system theory to analyze accident, and the main thinking of accident causality is the inadequate enforcement of safety constraints. It takes a drift from linear representation of event sequence to resilient analysis of whole system. This method has three elements: safety constraints (SC); hierarchical control structures; process models and control loops [4]. Safety constraint addresses a control problem shifted from the concept of an event sequence in a hierarchical structure, by a process model in which the safety can be controlled.

This study attempts to extend the STAMP about safety analysis with organization of FAO system focused on the safety constrains and process models. From Figure 2, the hierarchical control structure of FAO system shows the system-level constrains of organization:

SC1: The FAO's operational management and organizational procedure should control and manage the trains and passengers safely

SC2: An effective measure and respond must be taken by the organization when an emergency or failure incident appears.

SC3: The operation company management should keep a safe oversight and has an enough feedback.

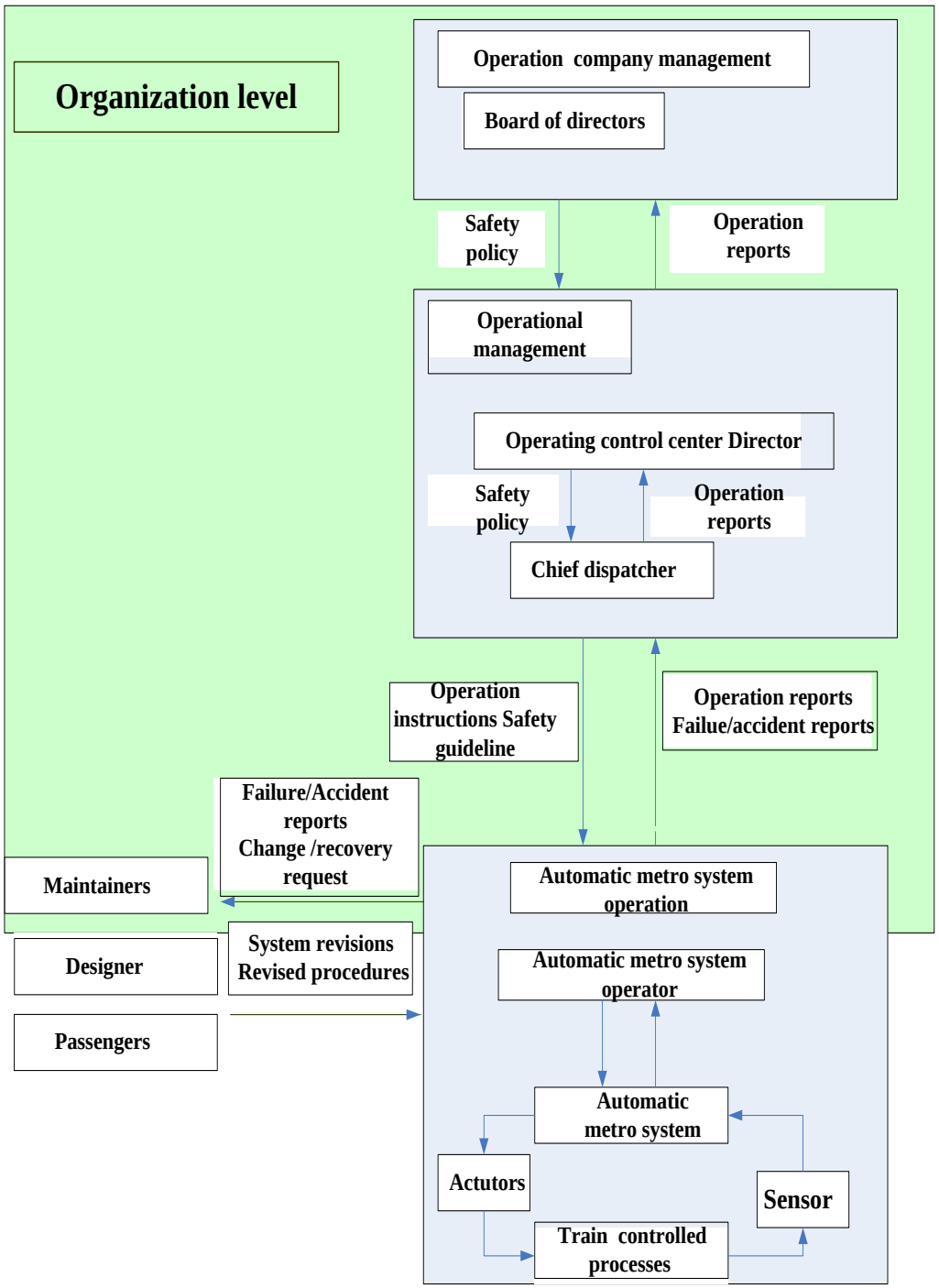

Figure 2. The Safety Control Structure of FAO System

From the aforementioned sections, the STAMP is neutral in organization analysis. To further analyze the aspect of the organizational characteristics, the VSM is employed to design, analyze the organization and to achieve a viable system in a cybernetic eyes. By the "whole systems" theory, VSM reveals the inextricable characteristic linked with a myriad factors. It is based on fundamental cybernetic principles of communication and control in complex organizations, which offers a way of providing true autonomy and recursive subsystem together with the necessary supporting links between the individual parts. In short, the VSM provides a cybernetic model to seek the source of effective organization in the cybernetics of natural processes like the brain itself [5].

It is believed that FAO system's organization should keep the viable safety management system as recursive system. The recursive property means autonomy and self-regulation at each level of FAO system' organization, and burrows the organization from the most global to the most local level to adapt the increasing pace of change. The VSM model of FAO system's organization is shown in Figure 3: system 1 (S1) actually do the basic activities of the operational procedure, manage the fleet of trains, awake the train in given location, set the train to sleep, supervise passenger flow, and provide passenger service.S1processes the basic units to keep a stable dynamic status in safety management of trains and passengers, and it can be seen as a lower level of relative autonomy which regulates with itself to adapt the scale of complexity in the five functions of VSM models. The meta-systems including systems 2 (S2) to system 5 (S5) coordinate the whole organization system with each other to get the viability and balance with the environment which is constituted of trains, passengers and infrastructures in metro, to facilitate all the management units working together in an integrated, harmonious mode [18].

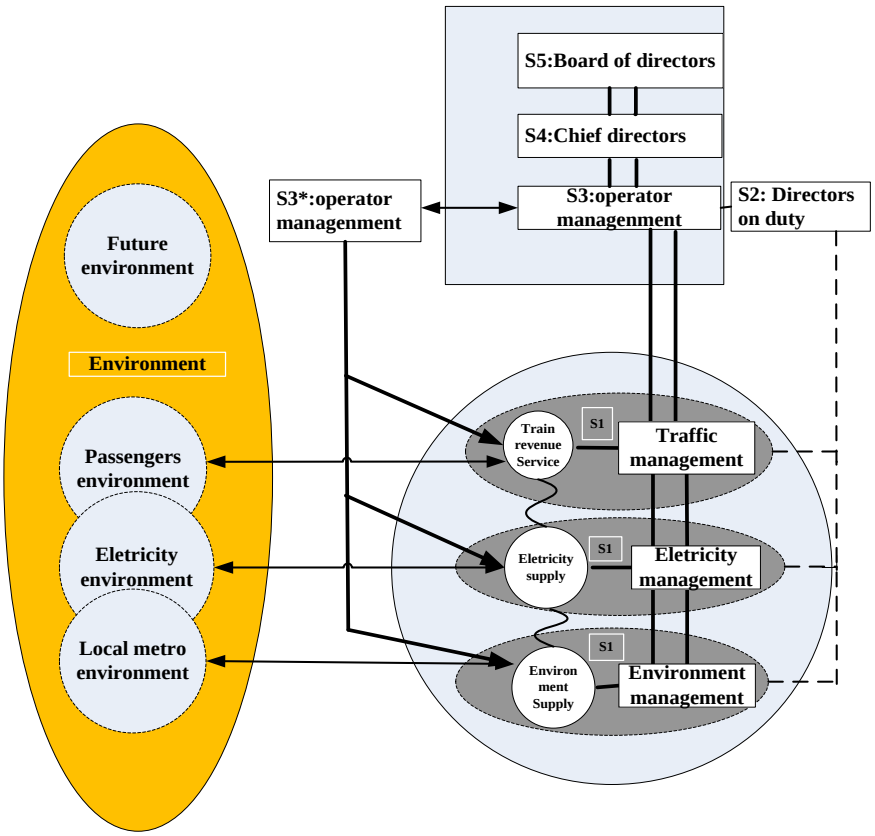

Figure 3. The Viable System Model of FAO System

Extended description of the five safety functions of the VSM model in FAO system is adapted from the models proposed by Kontogiannis and Malakis [8], and an case is studied to reveal the organization process of FAO system associated with “safety management”.

S1: Safety Policy Implementation in FAO system. It refers to the operational and manageable units of FAO system and offers interactions with passengers, trains and kinds of devices to implement revenue service in normality. It monitor and control the risk created in unstable situation. The system implements the safety policy and safety plans to keep the safety at the sharp end depending various techniques such as train control technique and operational management technique.

S2: Safety Coordination in FAO system. It is to coordinate operations in multi-domains

such as dispatch of passengers, trains and electricity, and it regulates the safety plans and resource assignment to avoid conflicting situation for providing safe, convenient and rapid trip service. We located the responsibility into director on duty in OCC to coordinate such conflicting interactions.

S3: Safety Functional in FAO system (management of operators). The management of operators in FAO system is theS3 which is responsible for maintaining safety within an acceptable range and ensuring all operational sharp end and management procedure to implement the organization's safety policy. The management of operators receives strategy and normative safety plans and standards from high-level system, and it makes work plan of S1 and assigns resource into S1.For this reason of safe control in FAO system, S3 also needs to monitor and conduct audits continuously through the feedback of the operations of S1, obviously as a constructor of safety functions in meta-unit of FAO system. It offers effective control of operational component and receives enough feedback to complete audit function. If the safety policy has changed, it will has a complete adaption and monitor the feedback of operational units after the assignment of resource. The vertical relationship is bidirectional, which is inactive up and alert down status.

S4: Safety Development and Adaptation in FAO system. It plays an intelligent function as it scans the environment for threats and opportunities while looking inside for internal strengths and weakness for the continual adaptation and anticipation of the whole system [9]. From the view, chief director has the responsibility of S4to provide safety assessment of organization's performance in FAO system. S4 should catch the real status of current system, grasp the relationships among the system variables, and understand the current state of the system which provides the sufficient information of the whole S1 toS5.

S5: Safety Policy in FAO system. S5 is responsible for formulating the safety policy and making normative decisions [9]. The board of directors in FAO system takes the functions of the S5, which is responsible for guiding the metro company's sustainable development, promoting the safety culture throughout the organization, and maintaining the safety consciousness of the whole system. Another responsibility of S5 should also achieve a balance between exploitation of existing safety rules and exploration of new safety concepts [9], and thus board of directors also should balance the gap between the extension of safety rules from the traditional system and the innovation of recognition of safety problem in FAO system.

3. The Potential Control Flaws in the Organization in FAO System

From a system control view, Leveson [4] proposed the key thought of safety constraints to protect the system safety which was specified as a 'control problem', and inadequate control is the leading factor violating the safety constraints. The method of STAMP is to facilitate safety analysis particular in the technique field, whilst VSM is a cybernetics model to analyze the structure, communication and control functions of viable organization. A further study of combination of STAMP and VSM is to solve the problem of safety management in a systematic approach, and a set of organizational control flaws has been proposed by the analysis of violation of the organizational safety requirements [9].

A classification of organizational control flaws is shown in Table 1 [9]:

Table 1. Control Flaws Identified at Organizational Level in FAO Organization

Control Flaws	Causes	Detailed description
(1)Inadequate formulation of safety policy and goals (Inadequate S5).	(a) Ambiguous safety policy or lack of safety policy.	The FAO organization may provide an ambiguous safety policy about the operation and management of driverless train, including emergency level, plan and scheme. The FAO system may not provide a clear safety goal which can be used to assess the operational process and emergency recovery. For example, the incident respond time, which can indicate the new performance of FAO system, is provided.
	(b) Trapped in the unnoticed loop between formulating goals and monitoring.	The FAO system's organization may focus on higher capacity and greater flexibility from the sophisticated technology, but safety awareness is reduced when operator monitors more smooth service related with passengers, and the gap between the application of operation and the aim of safety awareness will lead to unsafe system boundary.
	(c) Eroding safety goals.	The number of accident of FAO system is less than that of the traditional system so that the pressure, for decades, will make the organization of FAO system reduce the safety consciousness, and finally erode the safety goals.
(2)Inadequate adaptation to changes (Inadequate S4).	(a) Open loop	Facing the new change, the FAO organization is always in a numb status for lacking appropriate feedback, and it usually uses old patterns and plans of management.
	(b) Lack of double loop learning.	For the reason of decreasing accident rate, operator is not able to learn rich experience of FAO system, and the FAO organization can't formulate the experienced work team until several sorts of emergency incidents happen.
(3) Inadequate assignment of control authority and responsibilities (Inadequate S3).	(a) Imbalance between autonomy versus centralized control	The FAO organization needs a centralization mode for the global management and it needs the viability in relation to passengers' calmed, emergent situation and rescue operation.
	(b) Gaps and overlaps of responsibilities.	It happens in emergent situation. When a violation of normal operation or an emergency need blended methods including electricity, signaling, dispatching, maintaining and vehicle service, the gap of responsibilities between the job profiles and overlap among the work group will lead to a chaotic situation. The work teams of different majors in OCC have monitored the process independently to get the system failure with single cause, but with mixed causes which need the deep coordination.
(4) Inadequate design and ineffective implementation of safety	(a) Mismatch between the safety plans and the strategy of managinguncertai	Lack of emergency process regulation but the aim of safety is needed.

plans(Inadequate mapping of S5 to S1 and S2).	nty	
	(b) Lack of coordination	Lack of coordination between the traffic dispatcher, electricity dispatcher and maintenance worker. Lack of coordination between the chief director and the local rescue worker, which will worsen the implementation of safety plans when the emergency situation.
	(c) Inconsistency between plans and routines in practice.	The safety plan is so ambiguous that process in practice implementsbased on the old safety plans.
	(d) Plans are not following the changes in the system, stagnant plans	The safety plans haven't been changed according to the new distinction among the new operational services to passengers. In case of changes in the operation, such as the ATC subsystem down, the downgrade of system, train failure, and organization reconstruction of FAO system and *etc*., the safety plans haven't be adjusted from all these changes.
	(e) Lack of resources	Lack of a work team, which can process the emergency incident, including calming passengers, rescuing if needed, driving the train into the next station, and *etc*. Lack of tools supporting the operation's decision, and predicting future conflicts long before they occur. Lack of measures implementing optimum recovery quickly from major failures. Lack of deep training for understanding the intrinsic mechanisms of FAO system's organization.
	(f) Ineffective training procedures	In efficient training for the chief director in OCC with management experience in FAO system and for the operators with skilled task implementation. In efficient training for rescue worker in the situation of chaos emergency.
(5) Inadequate modeling of the state of the safety performance (Inadequate) mapping of S4 to S1 and S2).	(a) Inadequate feedback control.	The information particularly in the failure situation is not adequately provided to OCC. Lack of improvement of FAO system's organization and training for new staff in OCC after a small number of incidents happens. The real status of the whole FAO system is not adequately provided to the operators in OCC.
	(b) Lack of management of changes, inadequate risk analysis. Lack of leading safety indicators.	Risk analysis can't guide an efficient improvement in safety plans, design and implement of engineering. Risk analysis is not enough because of the experience absence from the new system, e.g., in case of system failure, fire in tunnel, disturbance events and so on.

The classification of control flaws of organization level can be used to analyze the potential hazards in the organization statically. A research goes a further step how these hazards are drifting over time especially in the FAO system. The emphasis is on how to describe the dynamics evolution process of organization, and to find out the essential

pattern and influence factors of organization which may guide the accident finally in FAO system. A set of dynamic organizational failure archetypes is corresponding with the models of control flaws in Table 2, which extends the VSM-STAMP joint framework to further safety assessment. The archetypes indicate the process which affirms the root reasons may be beyond the safety boundary of FAO system across so much safety constrains in several time stages, and find out the boundary condition that leads to unsafe status of system. The extension of the work process of organization gives a dynamic supplementary to the static inspection of the organization role described in VSM-STAMP joint method.

Table 2. Corresponding Reflection of Dynamic Organizational Failure Archetypes

Control flaws	Dynamics archetypes
Inadequate formulation of safety policy and goals (Inadequate S5)	Weakening of safety awareness with advanced technology
Inadequate adaptation to changes (Inadequate S4)	Unknown of system real status
Inadequate assignment of control authority and responsibilities(Inadequate S3)	Increasing integrated “mental” pressure
Inadequate design and ineffective implementation of safety plans(Inadequate mapping of System 5 to Systems 1 and 2).	Weakening team cooperation and communication
Inadequate modeling of the state of the safety performance (Inadequate） mapping of S4 to S 1 and 2)	Incomplete understanding of system risk

Based on the classification of organizational control flaws in FAO system, the following section extends the dynamics tracing on root causes into the pattern of breakdown of organizational processes, and finds out the reasons for the control flaws of FAO system. It is considered that the dynamics modeling of the control flaws (at the operational process) of organization (at the organizational level) will provide essential guidance to reveal how and why an accident may occur.

4. Dynamics Archetypes Model of Control Flaws

A set of dynamic organizational failure archetypes integrated with human factors are presented to achieve supervision of risk and protection of safety in FAO system. These archetypes include a discussion of dynamic mechanism, in which latent organizational factors in FAO system result in a loss or maintaining whole safety of system. This study shows system dynamics is an effective way to scratch the influence of organizational factors in FAO system. It can indicate what the organization need to do and how human can make a correct and positive decision at safety edge and in emergency situation.

4.1. Weakening of Safety Awareness with Advanced Technology

The advantage of FAO system is to control train automatic operation which greatly reduces the staff's workload. Operator assigns train task and sets train in revenue service, while train is responsible for automatic driving according to the timetable. There is no attendant and their task will be executed by Automatic Train Operation (ATO) on board. When the system works in normal status, the major task of OCC is to monitor the train's tracking through the screen of track layout displaying in OCC. It appears to play a positive role in staff's satisfaction for less workload. However, from investigation of line 10 in Shanghai, the operator has the thought that monitoring the train automatic tracking

between stations is boring and repetitive, and the operator likes to deem FAO system working in an overall automatic status of full safety.

It is actual the system is drifting toward the boundary of safe behavior when operator immerses in a numb status [19]. We will discuss why it is in a threatening status that operator considers FAO system always running under a state of ‘‘safety’’ in the following section. Figure 4 will explain why FAO system with advanced technology gets high safety in the beginning, and after a period of time, the system will cause a decline in safety becauseof operator's numb status. This structure consists of one reinforcing loop (*R_advance_technology*) and two balancing loops (*B_complacent and B_safety_awareness*).The both balancing loops have substantial delay; therefore, the balancing loops change to the main loops instead of the reinforcing loop(*R_advance_technology*).

4.1.1. Individual Staff Complacent

If system achieves more success, staff is followed with perceived success which will increase the staff's complacent, affecting system safety efficacy, and eventually lead to a situation of high risk which will bring system in accident [11]. Even if lack of service experience related to FAO system, the operator will consider that the system is enough successful because various complex technologies have been integrated into the system. The perfect automation degree is the main root cause of the operator complacent, which will guide the system into a state of mute when emergency incident happens(*B_complacent)*. For example, in 7.23 China Yong-Tai-Wen railway accident, dispatcher noticed the red light strip and announced worker to maintain the track circuit. When the train D3115 located in the track circuit 5829 with failure, the dispatcher allowed the next train D301 to leave from Yongjia station to Wenzhounan station. At the same time, dispatcher also believed the ATP on aboard would protect train D301 against the correct movement authority, and it was too late when he called the train D301 to notice the D3115 in front of cab [20]. If the dispatcher keeps the mind in an alert state, the system will not get out of the safety boundary.

Operant conditioning theory addresses that people learn to get something they want or to avoid something they don't want. The behavior of operator is influenced by the reinforcement or lack of reinforcement brought about by its consequences [21]. FAO system's service condition is creating a complacent consequence to make operator follow specific forms of behavior, and is raising the frequency of the similar behavior. Operators in OCC will become complacent or form mental models that they are at risk of controlling disaster while the system is running at higher automatic level. Thus, this behavior will allow negative stimuli in a relatively numb manner. The status is also an inadequate control from the theory of STAMP that operator is not alert enough to monitor FAO system, and therefore, complacent will become one of main root causes in FAO system with a decade of time delay.

4.1.2. Safety Awareness

It is designed with reduction of manual operation associated with the new system to avoid human error. The focus on safe behavior of driver will weaken gradually if the number of action is decreased. The technology of FAO system satisfies the higher objective to decrease the frequency of manual action. However, it has resulted in a corresponding decline in human cognition to system safety of intrinsic environment. It also has weakened the staff's safety awareness in the working situation and increased the vulnerability of safety consciousness (*B_safety_awareness*).

Over-optimization of a particular safety measure will decrease system awareness and adversely affect system safety [13]. Many methods are considered in FAO system to protect train safety driving. Onboard and wayside Automatic train protection(ATP) system

is used to protect the max speed of train and termination permitted, and Automatic train protection (ATC) system makes the operator believe that it could always protect train safety operation according to the failure-safety principle, which can prevent catastrophic consequences from failure. A further step, a variety of complex technologies are integrated in FAO system to replace human to do more and more work. Nevertheless, the device is not a substitute in aspect of human safety awareness, which is subjective but plays a crucial role in safety sharp-edged situation. Although large amounts of academic research are carried in device's anti-disturbance and system self-diagnosis, it is ambiguous and hardly used in the engineering design. The characteristic of self-operation is hard to be scratched accurately, whereas human can observe it and mitigate high risk from unsafe boundary, and therefore, the operator should always keep safety consciousness with the system while the FAO system is giving significant changes in human behavior.

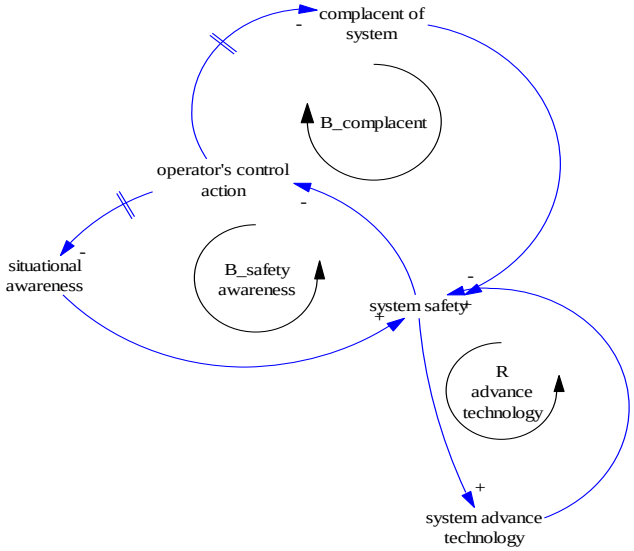

Figure 4. Weakening of Safety Awareness with Advanced Technology

4.2. Unknown Real Status of System

Physical isolation in automatic operation of FAO system reduces the workload of staff, but the increase is always accompanied by a form of mental isolation [22]. The safety critical characteristics of FAO system make operator take a new challenge to identify the system status which is determined with automatic device supervision and tracing on train. The problem is that mental isolation will result in high risk for the unknown of system's real status. Figure5 shows how operator's actions of fault diagnosis and fault recovery may initially promise safety in FAO system but eventually reach a point in which system failure may cause an accident. The safe goal in mental models will erode overtime which has the negative reflection from the following archetype.

Automation degree is followed with more complex system structure, complete functions and interaction types. Discipline, standard and instruction of operation and management are necessary for operator to adapt automatic system and recognize procedure of operation. Operator, who can learn what happens by the man-machine interface when a failure occurs, has the responsibility to identify the root causes of incidents before it deviates to an accident, and to find the correction process with time pressure (*R_actual_fix*). However, accident in FAO system is not caused by a single fault, but a collection of several unexpected and hidden faults under special environment and the aggregation of kinds of faults will present to staff only an obscure phenomenon. Nevertheless, operator generally locates cause of failure phenomenon to a single device

failure because of various factors (time, pressure, complexity, staff satisfaction, and *etc*.,) makes a surface processing solution which neither solves the root problem nor applies the correct application, and finally will guide to an inevitable accident (*R_problem_drift*).

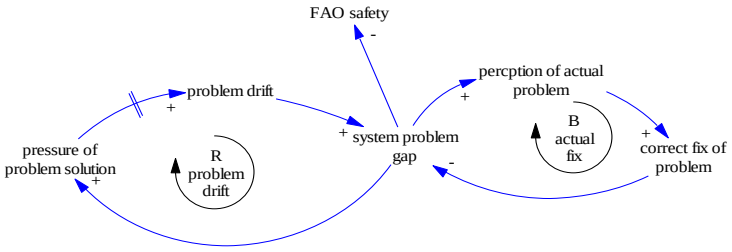

Figure 5. Unknown of System Real Status

4.3. Incomplete Understanding of System Risk

It is considered that risk-related behavior produces ‘risk compensation’ at several hierarchical levels with different mechanisms [23]. Before defining the risk-related behavior, we should have a deep-depth risk analysis in system, particularly in a high integrated system. From the view of system design, FAO system needs to use a resilient method to become appropriate for system’s work process, which enhances the ability of avoidance, survival and recovery. One important method to keep the preliminary protection is safety risk analysis integrated into system design phase across the work process of FAO system. For example, ATC system replaces driver's all operation such as train awakening automatically to realize the main control function of train. It means that ATC system must implement the functions instead of the driver's operation as well as driver's responsibilities. In fact, ATC system is designed to replace the driver actions, but can't understand the risk of train operation’s process completely into the design phase. Safety will be compromised when the advantages of ATC system's automatic technology are not accompanied by corresponding understanding of the risk associated with human's responsibility (*B_understanding_risk_driver*). In the actual FAO system, operator in OCC tends to further understand the function of high technology system, but perceive neither the risk changed in automatic technology system nor hazard hidden in the back of the system.

In case that random disturbance or emergency incident happens in the system, the FAO's device can't be completely consider random events to its automatic operation. At the same time, the device can only identify characteristics of significance event (such as train fire warning), but can't single out tiny change in event (for example, the switch in front of train, but the system thinks switch is set at the right position) for avoiding to spread the influence, while the driver can find the subtle changes, analyze the change and evaluate risk to make safe operation of train. Hence, it is necessary to understand how the subtle changes will result in qualitative change in risk completely when replacing driver's operation, and it needs to add the real-time monitoring and processing of random events when the device performs the train driver's operation (*B_understanding_risk1*). It is shown in Figure6why FAO system with high automatic grade can get the instant safety but can't control safety over the whole procedure of revenue service. In case of an ultra-safe system which has continuous elimination of errors and incidents, breakdowns may paradoxically decrease safety [24]. Loop *B_decresing_accident* shows that understanding of FAO with advanced technology will weaken if the number of incident of FAO system is decreasing. From Figure 6, we propose the following note (*R_preliminaryhazard_analysis*):

（1） Understanding the risk which is perceived by driver.
（2） Addingthesystem risk into the process of FAO organization.
（3） Monitoring the risk migration profile of FAO system to mitigate risk.

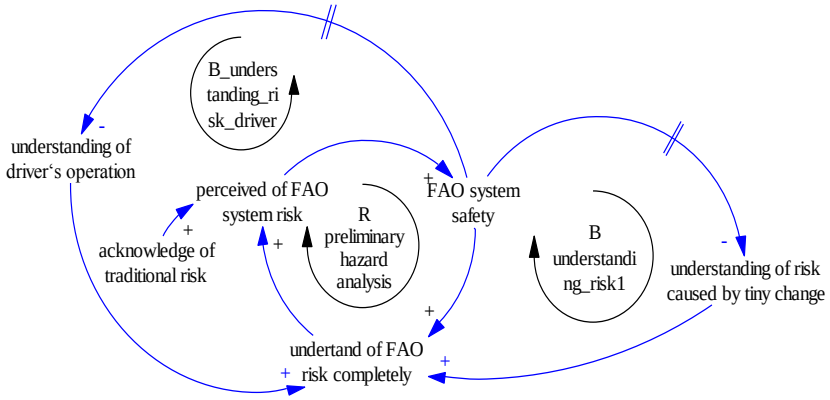

Figure 6. Incomplete Understanding of System Risk

4.4. Increase of the Integrated “Mental” Pressure

The error of driver operation caused by emotion resulted in many accident. For example: at 9:19 am on April 25 in 2005, an EMU from the Fukuchiyama Line of JR West derailed near Osaka killing 106 passengers and injuring 562. At a previous station, the train overran by 70 meters causing a one minute delay. The driver was explaining to the conductor at the time when the train entered the 304-meter-radius curve at 116km/h, against a 70km/h speed limit. The first car tilted to the left, causing derailment [25]. The result of accident shows that emotion is closely linked in human mental activity, and will affect the human's physical activity. It is difficult to avoid driver's error particular caused by the problem of driver's psychology in changing situation. Figure7 will explain the reason that the mental model of driver can be hardly replaced and will result in a decline in FAO system in case of inappropriate aggregation to operator's pressure workload in OCC.

From the model of operation risk slowly addressed by Karen Marais, we extend the model about application for the FAO system, and Figure 7 explains why safety will tend to decline after it reaches a certain degree. It includes two loops: Loop *R_monitor_normal* illustrates how equipment's automatic level improves the FAO system's performance and capacity, and Loop *R_mental_emergency* addresses why safety decreases when continuous optimization methods is used in safety because of lifting pressure.

It seems like that FAO system presents a fully automatic operation system from the definition of system requirement, and ‘‘physical’’ actions related to driver are carried out automatically by equipment because of the clear definition for manual operation, which can be diverted into the specific component of hardware and software in the design phase. For example, the driver's responsibility of ‘‘manipulating control handle’’ is replaced by the physical hardware interface and software process. System designer can clearly describe the type, process, range and boundary to perform system functions. It also can test the functions to prevent error-design of equipment and validate the function at the early stage of the system design with simulating process (*R_monitor_normal*).

However, the designers of FAO system hardly include driver's ‘‘mental’’ behaviors in the design of the equipment, and the main reasons are that it is difficult to define the ‘‘mental’’ action process and final result explicitly. For example, in the traditional system, a driver can continuously surveille at distance in the process of driving the train, ensures train stopping against obstacles (red light signal) on the track, and drives the train from

the corresponding movement authority. In such process, the driver ‘‘observes’’ in front of the track as well as the track information, ‘‘perceives’’ information to decide train driving mode and state, and finally output ‘‘decision’’ how train can be controlled by inputting the ‘‘mental’’ model of human. Fully automatic operation of train takes another problem, which is the aggregation of all driver's mental model processes into OCC's staff.

The Studies try to divide the execution process of driver's ‘‘mental’’ behaviors into a series of stages, and it is possible to represent the characteristics of key processes. Requirement is also reflected in hardware and software system. For example, the function of ‘‘observation’’ of track and signal information in front of cab, is replaced by the closed circuit television supervisory system (CCTV), but CCTV can't support individual's cognition-decision and only provide video input instead of driver's eye. Hence, CCTV is used to replace driver's monitoring of track information in front of cab, but neglect ‘‘cognition’’ and ‘‘decision’’ after the monitoring function. It is necessary to have agent to replace the driver individual's ‘‘cognition-decision’’ model, and to simulate the individual's cognition, judgment and feedback. Although it is feasible that execution of the process is shifted to operator in OCC, the operator's ‘‘mental’’ model will be added by multiple driver ‘‘mental’’ models. It will have the opposite effect with motivation and time pressure (*B_mental_emergency*).

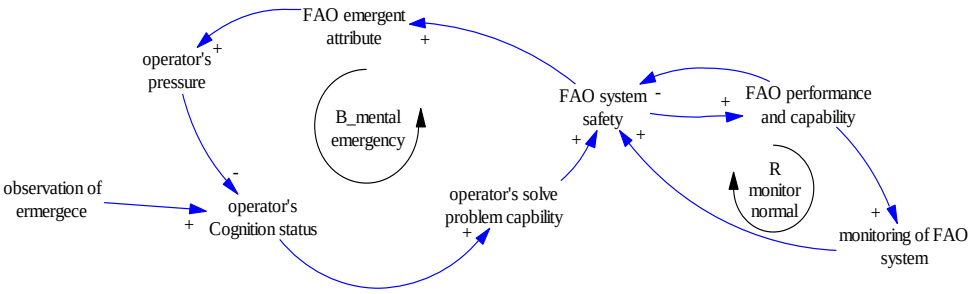

Figure 7. Increasing Integrated “Mental” Pressure

4.5. Weakening Team Cooperation and Communication

To achieve the system's success, team's early task is relatively simple. Naturally, new team for new system often deals with the easiest problem. And the team has formed an established pattern of activity to face more difficult problems while the environment changes, and its members are not willing to change their ‘‘perfect system’’. The new problem makes the increase of the conflict in the team but communication between the members is weak [26]. For example, the dispatcher announced the driver in D301 is too lately to notice the D3115 in 7.23 china Yong-Tai-Wen railway accident.

Individual's mental model can't be properly changed immediately and be resistant to change because inadequate training, poor system design and time pressure [14]. Although training and corresponding operation instruction of the FAO system are provided to the work team for actual activity, individual cognition in work team is based on experience of the traditional system. New content of task is mapped to the changeable responsibility of original work. In the beginning, the application of new technology in FAO system makes accidents rarely exposure to individual, and thus, individual of the work team is always imperfect in the process of handling incident in new system context because low incident rate and low team cooperation experience. On the other hand, the more task FAO device takes, the less visibility FAO system represents to individual who only recognizes the whole system's status. In particular that inadequate feedback may lead to difficulties for the human controllers [27]. The individual can't locate the root cause when failure happens in the system, assuming that effort of environment exceeds the capability of the

automatic equipment. Poor Individual's mental model lacks of sufficient understanding and training in new systems, which will result in weak team cooperation multiplying a negative influence over FAO system's safety (*B_visibility_system*).

The FAO system's reconstruction of work team is based on original pattern of activity, traditional CBTC management mode and the knowledge of task requirements. It is consisted of train dispatching work group, electricity dispatching work group, local maintenance work group, and vehicle maintenance work group. System with these different responsibilities for work group has a clear division: train dispatching work group is responsible for operation and management of train, power dispatching work group is responsible for the supply and maintenance of power in the whole metro system, vehicle maintenance work group is responsible for maintenance of vehicle, and the local maintenance workgroup is responsible for on-site inspection of track and the emergency operation. Reconstruction of FAO team makes that it is difficult to achieve enough communication between members, which will induce hover around safety margin of FAO system (*B_team_communication*). The work team accomplishes task under its own ‘‘perfect system’’ with the upgrade engineering for automation degree, and works in a simple and independent pattern. Members in the team only know individual responsibility but don't understand the cooperation of team deeply. Along with this, it is crucial to achieve steady safety in condition that needs enough communication and close cooperation, which will grow in high risk of FAO system. It is proposed that the poor and presentational understanding of team communication forms the potential hazards in FAO system. For example, the ‘‘appearance’’ lived mental model of work team will bring disastrous consequences to the FAO system if the environment changes in a rapid speed, and neither individual can scratch the essence of what happened, nor the team can guide the adaptation in a positive and interactive way. It will be difficult to agree with the solution once the problem appears to need close communication between members.

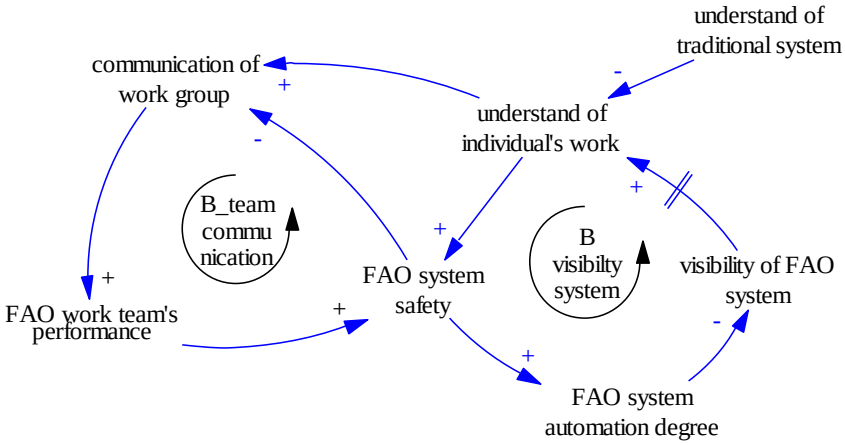

Figure 8. Weakening Team Cooperation and Communication

The independence of members in work team is strengthened with the complexity of task. In FAO system, the degree of complexity is closely related the situation when system works in abnormality. In Figure8, we propose a concept of multi-functional team to adapt the change of new team. Directive leadership leads to greater satisfaction when tasks are ambiguous or stressful when they are highly structured and well laid out [26], particularly

in situation of interference and emergency, and supportive leadership will result in high performance and staff satisfaction. Hence in FAO system, master dispatcher will give more enhanced leadership of whole system than traditional system, and any other staff will change the pattern of communication to improve passenger service. Local maintenance worker will be available to act as passenger contacts along the line, and to soothe the emotion of passenger in case of emergency incident. Vehicle maintenance worker will give service when train has a fault, and look after the passenger. Operational dispatcher and power dispatcher should exchange and cooperate with local maintenance worker and vehicle maintenance worker to find out the real status of FAO system when emergency, and assess the emergency incident and provide sufficient information to master dispatcher who will gives the dominant opinion. The groups will lead to increased acceptance of a solution by this bidirectional communication, and generate more complete information and knowledge to make decision [26]. Although the master has a guiding decision, the strengthened communication will activate more effective group decision-making by aggregating the resources of several individuals than individual decision making in traditional system.

5. Conclusion and Discussion

FAO system requires significant changes to the job profile of staff to make adaptive services. It is no longer necessary for routine driving work, and organization of FAO system needs to deploy service along the line and to provide direct service with passenger. It is a critical challenge to adapt the significant changes to keep the whole FAO system's organizational balance and viability with the environment.

The method of VSM is good at describing the organization structure and coordination behavior with interior and exterior elements and the VSM model is adopted to find out the organizational risks of FAO system in a cybernetics eyes from STAMP, so the supplement of control flaws of FAO system organization reveals the inadequate safety constrains caused by the organization, and form the basis for further dynamics causal analysis over time. A reflection of the control flaws and dynamics causal mechanism is acquired to connect the inherent relationship, which makes up the hybrid system dynamics method with extension of VSM-STAMP model.

It is argued that ‘‘over automation’’ has brought out the evolution of society, but degeneration of organizational perception of safety is followed with operational management. The imbalance between advanced technology and organization will guide a paradoxical growth in development for the nonlinearity and complexity of new FAO system. For this reason, five generic models of system dynamics have been proposed to explain nonlinear relationship of organization in FAO system and make their operation and management more practical.

The recursion of constrains and process inherited by STAMP provides the feasibility and vulnerability over prediction and recovery process of operation and management of system. The control flaws combined with all these archetypes can be used to further design dynamic behavior models at organizational level, which is integrated with individual recognition process for specific accident analysis in FAO system. They can explain why high automatic metro needs more complex and critical operation rule, high level of awareness in safety, and efficient training to form high reliability organization.

The current study is trying to find out inherent interaction relationship and influence mechanisms between device, human and organization, and to explore the dynamic characteristics and process of risk drifting to a fatal status in FAO system. The final objective is to mitigate the risk to an acceptable level. In future study, we will focus on the quantitative analysis of the archetypes in FAO system, prediction of the leading factors to support the system strategy and decision-making, particularly incase of emergency incidents.

Acknowledgments

This work was supported by the International Science & Technology Cooperation Program of China (No. 2012DFG81600), the Beijing Laboratory of Urban Rail Transit and Beijing Key Laboratory of Urban Rail Transit Automation and Control.

Reference

[1] J. H. Saleh, K. B. Marais, E. R. Bakolas and V. Cowlagi, "Highlights from the literature on accident causation and system safety", Review of major ideas, recent contributions, and challenges, Reliability Engineering & Sys-tem Safety, vol. 95, no. 11, **(2010)**, pp. 1105-1116.
[2] I. Svedung and J. Rasmussen, "Graphic representation of accident scenarios: mapping system structure and the causation of accidents", Safety Science, vol. 40, no. 5, **(2002)**, pp. 397-417.
[3] E. Hollnagel, "Barriers and accident prevention", Ashgate Aldershot, **(2004)**.
[4] N. Leveson, "A new accident model for engineering safer systems", Safety science, vol. 42, no. 4, **(2004)**, pp. 237-270.
[5] S. Beer, *et al.*, "Diagnosing the system for organizations", John Willey, **(1966)**.
[6] J. Santos-Reyes and A. N. Beard, "A systemic analysis of the padding on railway accident", Proceedings of the Institution of Mechanical Engineers, Part F: Journal of rail and rapid transit, vol. 220, no. 2, **(2006)**, pp. 121-151.
[7] J. Santos-Reyes and A. N. Beard, "A systemic approach to managing safety", Journal of Loss Prevention in the process industries, vol. 21, no. 1, **(2008)**, pp. 15-28.
[8] T. Kontogiannis and S. Malakis, "A systemic analysis of patterns of organizational breakdowns in accidents", A case from helicopter emergency medical service (hems) operations, Reliability Engineering & System Safety, vol. 99, **(2012)**, pp. 193-208.
[9] K. Kazaras, T. Kontogiannis and K. Kirytopoulos, "Proactive assessment of breaches of safety constraints and causal organizational breakdowns in complex systems", A joint stamp-vsm framework for safety assessment, Safety Science, vol. 62, **(2014)**, pp. 233-247.
[10] N. G. Leveson, "Safeware: system safety and computers", ACM, **(1995)**.
[11] N. Dulac, "A framework for dynamic safety and risk management modeling in complex engineering systems", Ph.D. thesis, Massachusetts Institute of Technology, **(2007)**.
[12] M. V. Stringfellow, "Accident analysis and hazard analysis for human and organizational factors, Ph.D. thesis", Massachusetts Institute of Technology, **(2010)**.
[13] W. Braun, "The system archetypes", The systems modeling workbook, **(2002)**, Available from: <http://www.uni-klu.ac.at/~gossimit/pap/sd/wb.
[14] M. Masuch, "Vicious circles in organizations", Administrative Science Quarterly, **(1985)**, pp. 14-33.
[15] K. Marais, J. H. Saleh and N. G. Leveson, "Archetypes for organizational safety", Safety science, vol. 44, no. 7, **(2006)**, pp. 565-582.
[16] T. Kontogiannis, "Modeling patterns of breakdown (or archetypes) of human and organizational processes in accidents using system dynamics", Safety Science, vol. 50, no. 4, **(2012)**, pp. 931-944.
[17] "International Electrotechnical Commission and others", IEC 62290-1: Railway applications: Urban guided transport management and command/control systems, **(2011)**.
[18] J. Walker, "An introduction to the viable system model as a diagnostic and design tool for co-operatives and federations", ESRAD eclectic systems. Downloaded from http://www. esrad. org. uk/resources/vsmg 3/screen. php.
[19] J. Rasmussen, "Information processing and human-machine interaction", An approach to cognitive engineering, North-Holland, **(1987)**.
[20] "The State Council's work team of "7.23" Yongwen Railway accident", investigation report of the "7.23" yongwen railway accident, Tech. rep., **(2011)**.
[21] B. F. Skinner, "Contingencies of reinforcement: a theoretical analysis", Prentice-Hall, **(1969)**.
[22] S. Zuboff, "In the age of the smart machine: The future of work and power", The Academy of Management Executive, vol. 3, no. 1, **(1989)**, pp. 76-77.
[23] H. Summala, "Accident risk and driver behavior", Safety Science, vol. 22, no. 1, **(1996)**, pp. 103-117.
[24] R. Amalberti, "The paradoxes of almost totally safe transportation systems", Safety science, vol. 37, o. 2, **(2001)**, pp. 109-126.
[25] H. Fukurai, "Japan's prosecutorial review commissions", Lay oversight of the government's discretion of prosecution, **(2011)**.
[26] S. P. Robbins, "Organizational Behavior", 14/e, Pearson Education India, **(2001)**.
[27] D. A. Norman, "The 'problem' with automation: inappropriate feedback and interaction", not' over-automation', Philosophical Transactions of the Royal Society of London. B, Biological Sciences, vol. 327, no. 1241, **(1990)**, pp. 585-593.

