Article

Hazard Analysis for Escalator Emergency Braking System via System Safety Analysis Method Based on STAMP

Zitong Zhou , Yanyang Zi *, Jinglong Chen and Tong An

State Key Laboratory for Manufacturing and Systems Engineering, Xi'an Jiaotong University, Xi'an 710049, China; tongzhou925@stu.xjtu.edu.cn (Z.Z.); jlstrive2008@163.com (J.C.); antong0531@stu.xjtu.edu.cn (T.A.)

* Correspondence: ziyi@mail.xjtu.edu.cn

Received: 19 September 2019; Accepted: 22 October 2019; Published: 25 October 2019

Abstract: Due to the complex mechanical structure and control process of escalator emergency braking systems (EEBS), traditional hazard analysis based on the event chain model have limitations in exploring component interaction failure in such a complex social-technical system. Therefore, a hazard analysis framework is proposed in this paper for hazard analysis of complex electromechanical systems based on system-theoretic accident model and process (STAMP). Firstly, basic principles of STAMP are introduced and comparison with other hazard analysis methods is conducted, then the safety analysis framework is proposed. Secondly, a study case is performed to identify unsafe control actions of EEBS from control structures, and a specific control diagram is organized to recognize potential example casual scenarios. Next, comparison between fault tree analysis and STAMP for escalator's overturned accident shows that hazards related to component damaged can be identified by both, while hazards that focus on components interaction can only be identified by STAMP. Besides, single control way and tandem operation process are found to be the obvious causal factors of accidents. Finally, some improvement measures like decibel detection or vibration monitoring of key components are suggested to help the current broken chain detection to trigger the anti-reversal device for a better safe EEBS.

Keywords: system safety; STAMP; escalator emergency braking system; hazard; unsafe control action; fault tree analysis

1. Introduction

Escalators, as an important part of modern life, plays a more and more significant role in our life. In China, the number of elevators and escalators continues to grow every year, and the growth rate ranks first in the world. With the increase in the number of escalators, accidents related to escalator have also shown an upward trend. Since 2005, China has experienced an average of about 40 elevator accidents per year and the death people is about 30. The number of serious escalator accidents from the year 2009 to 2014 is shown in Figure 1 and the injuries in Guangzhou Metro from the year 2013 to 2015 are shown in Table 1 [1]. Due to the huge number of bases, although the death rate of escalators is very low, the damage and social influence on the injured are very serious. Thus, the safety of escalators has also attracted more and more attention [2–5]. When accidents happened, hazard analysis techniques based on related safety theory can help technicians identify the cause of failure efficiently and the potential hazards that may cause the accident, then set up safety protection to avoid the recurrence of similar accidents according the causes and hazards.

Table 1. Overview of the injuries in Guangzhou Metro [1]. Reproduced with permission from [1], Elsevier, 2019.

Year	Passenger Flow Per Year (billion)	Total Injuries	Escalator-Related Injuries
2013	1.99	418	291
2014	2.28	477	314
2015	2.40	520	345

Figure 1. Trend of serious escalator-related accidents in China, 2009–2014 [1]. Reproduced with permission from [1], Elsevier, 2019.

As the base of the safety issue, accident or safety theory is used to clarify the cause, the process, the end and the consequences of the accident to make a clear analysis of the occurrence and development of the accident. Traditional accident theory started from almost 100 years ago, accident prone theory was proposed by Farmer and Chamb based on the research of statistical casualty distribution Greenwood and Woods [6]. After that, Traditional safety theory such as Heinrich Law and Energy Release Theory have been proposed successively [7,8]. All these theories focus on the instability and unsafety of human beings and their behavior in the system. However, the WASH-1400 report about nuclear reactor safety study established the framework of probabilistic risk assessment (PRA) technology and conducted safety assessment in the field of nuclear power, which greatly promoted the research and application of probabilistic risk models [9]. In 1997, Reason expressed the different levels of the system as slices of Swiss cheese. The “holes” on the slices represent defects at all levels of the system, which became the most famous “Swiss cheese” model in classical safety theory [10]. Since then, some descriptive theories based on the actual behavior of the system, such as normal accident theory (NAT) proposed by Charles Perrow, and highly reliable organization Theory (HRO) proposed by Karlene Roberts, have a profound impact on accident cause and system safety [11–13].

In 1997, Rasmussen initiated the system safety analysis method based on cybernetics and systems theory, in which risk management was described as a control process and risk management must be established based on the classification for hazard sources of control requirements [14]. In 2004, Leveson established a system theoretic accident model and processes (STAMP) based on the system theory. The core idea of the model is that accident is the emergence of interactions between various elements in a complex system, and the lack of control actions that impose constraints on these interactions will lead to accidents [15]. The appearance of the STAMP model leads to the rapid development of modern safety theories based on systems theory. In 2008, Zahra Mohaghegh proposed the SoTeRia method using a combination of system dynamics, Bayesian networks, and other methods to quantitatively describe how influence factors are transferred from organizational factors to technical aspects [16,17]. In 2015, Cody proposed the system-theoretic early concept analysis (STECA) method

for safety analysis from the perspective of systems science and control science based on STAMP and hazard analysis technology [18]. Figure 2 shows the development of safety related theory based on the above-mentioned description.

Figure 2. Development of safety theory.

The classical safety theory based on the event chain model and probabilistic failure analysis focuses on the failure analysis of equipment and can effectively analysis the accidents caused by component failures or operational errors. However, the safety risk analysis based on the event chain model ignores the impact of the interaction between components on system safety. Meanwhile, the quantitative risk assessment based on probabilistic failure analysis is not suitable for solving the problem that people participate in the control of complex system safety evaluation issues, because it only considers the combination of single event failure probability and mutual exclusion event probability. The study of modern safety theory breaks through the shortcomings of the classical safety theory that only pays attention to the performance of components and recognizes the insufficiency of feedback or control from the perspective of system theory, making the STAMP more suitable for a complex system [19]. STAMP has been widely used in aerospace, petrochemical, transportation and other industries whose strong vitality lie in the fact that STAMP tries to help us to understand the system safety from the perspective of control, rather than being trapped in the constraints of traditional event chain model [20–23]. On the base of STAMP, system-theoretic process analysis (STPA) was proposed to be a new hazard analysis [19]. Besides, another important advantage of STAMP/STPA is its simple operability and broad applicability. Thus, the impact of task specificity on the safety analysis of man-machine-loop systems is reduced. The goal of STPA, which is to create a set of scenarios that can lead to a hazard, is the same as fault tree analysis (FTA) but STPA includes a broader set of potential scenarios including those in which no failures occur but the problems arise due to unsafe and unintended interactions among the system components.

As for the safety analysis of escalator, some research focused their attention on mathematical statistics analysis to find the relationship between various considerations and escalator-related accidents [24–26]. There are also some studies on behavior or state of passengers such as group trampling risk simulation [27], congestion risk simulation based on social force model [28], and pedestrian flows modeling [29]. Some traditional hazard analysis methods like FTA, hazard and operability analysis (HAZOP) are also applied in analysis of escalator-related accidents, but they paid more attention to component failure or causal relationship of human events, ignoring the interactions of components and other causes [30,31]. Therefore, STPA is introduced into the safety analysis of escalators in this paper, which can help to understand the connotation of escalator-related accidents systematically and comprehensively. On the other hand, based on the analysis results analyzed by the above safety analysis methods, many useful strategies and methods are used to improve system safety [32–36]. Similarly, the proposed method for safety analysis of escalator emergency braking systems (EEBS) in this paper also hopes to find some useful measures to improve the safety of EEBS.

The remainder of this paper is organized as follows. In Section 2, a brief introduction about System theoretic accident model and process is illustrated and comparison between FTA, failure mode

effects and criticality analysis (FMECA), HAZOP and STPA are carried out to show the superiority of STAMP in complex social-technical system, then a safety analysis framework is proposed in this paper for hazard analysis of complex electromechanical system based on system-theoretic accident model and process. In Section 3, a system safety analysis method based on STPA is introduced and a case study of escalator emergency braking system demonstrates the method. In Section 4, result comparison between FTA and STPA is discussed, and some targeted improvement measures are suggested to improve the safety of EEBS. Finally, conclusion is drawn in Section 5.

2. Safety Analysis Framework for Complex Electromechanical Equipment System Based on STAMP

STAMP treats safety as a control problem, and the focus of system safety is changed from preventing failures in implementing safety constraints. It still contains component failures, but it extends the concept of accidental causes to include component interactions. It contains three main concepts: safety constraints, hierarchical control structures, and process models. The most basic concept in STAMP is not an event but a constraint. The main causes of safety issues in the new theory are component failures, system external disturbances, interactions between components, and component behaviors that lead to dangerous system states.

2.1. Principles of STAMP

The safety of a complex system is more than component failure or reliability decline. In STAMP, safety is an emergent or system property, rather than a component property. In system theory, complex systems are viewed as a hierarchy of organizational levels. A hierarchical multilevel model of stakeholders is posited in STAMP, like the model of Rasmussen [13], but more expanded. Another basic concept in STAMP is safety constraints. In system theory, safety can be regarded as an emergent which is originated from interactions between components. The method of controlling the emergent is to impose constraints on the behavior of the components and the interactions between the components. Meanwhile, due to the constraint property of hierarchical structure, the accidents will happen if the higher layers cannot provide enough constraints or the lower layers violate the safety constraints when the high-level constraints control the behavior of the lower layers. With the development of the equipment toward automation and intelligent, the system becomes more and more complex, and the difficulty in identifying and executing safety constraints in design and operation has been increased. Figure 3 shows a general socio-technical system control structure from STAMP, which does not represent any particular system. Each node in the graph is a human or machine component in a socio-technical system. Connecting lines show control actions used to enforce safety constraints on the system and feedback that provides information to the controlling entity.

Besides constraints and hierarchical models, a third basic concept in STAMP is that of process models. The process model is an important part of the control theory. A typical process model consists of the controller that issued the command and the controlled object that provided the feedback (controlled process), which is shown in Figure 4. Usually, the controller contains process model and control algorithm. When the controller sends a command to controlled process, the corresponding feedback which is generated by controlled process will be sent to controller to form a complete controlled process. Component interaction accidents can often be interpreted as process model errors. When the controller's process model does not match the controlled system or the controller issues an unsafe command, an accident will also happen.

Figure 3. General socio-technical system control structure from the system-theoretic accident model and process (STAMP) [15]. Reproduced with permission from [15], Elsevier, 2019.

Based on three basic concepts of STAMP, the basic casual factors of a standard control loop under the STAMP framework was concluded in Figure 5 [19].

Figure 4. Multi-level control process.

Figure 5. Basic causes of unsafe control. Reproduced with permission from [15], Elsevier, 2019

2.2. Comparison between FTA, FMECA, HAZOP, and STAMP

Traditional risk analysis theory considers hazards as the result of the action of a series of events. The considered events usually involve several types of component failures or human errors, mainly adopting the forward sequence method (such as failure mode and impact analysis) or the backward sequence method (Such as the fault tree directly describes the linear relationship between the failure and the influencing factors and is suitable for analyzing the hazard caused by the failure of a physical component or a simple system.) Three hazard analysis techniques are suggested in the functional safety standard (ISO26262): fault tree

analysis (FTA), failure modes and effects analysis (FMEA), and hazard and operability (HAZOP) analysis. Table 2 summaries and compares three general hazard analysis techniques with STAMP.

Table 2. Comparison of safety analysis techniques.

Method	Time&. by	Advantages	Disadvantages
FTA	1961 By American Telephone & Telegraph Company	Concise expression of causality and logic; Predict and Prevent accident; Qualitative and quantitative analysis	Not for analysis of a process or equipment system; More steps and computational complexity for a complex system; The probability of all basic events needs to know for quantitative analysis etc.
FMECA	1950s By United States Air Force	The whole process of product development; Principle and operation are simple; The base of other failure analysis	Heavy workload, time-consuming; Univariate analysis; Limited by environmental conditions; Poor generality of the conclusion, etc.
HAZOP	1974 By Imperial Chemical Industries	Detailed analysis of process engineering; Design evaluation and operation evaluation;	Need professional groups to work; Ignore the interaction between subsystems
STAMP	2004 By Massachusetts Institute of Technology	Understanding accidents from the perspective of system theory and cybernetics; Fully consider the interaction between systems;	Emphasize social factors; Mostly used for qualitative analysis and need to be combined with other methods for quantitative analysis

FTA, FMECA, and HAZOP are proposed before the 1980s in which industrial automation and intelligence are still not highly dependent. Only giant companies and some research institutes like the nuclear industry, aerospace, and universities have enough human and material resources to carry out relevant technology research. Although some detail can be found by these three methods, the limitation of methods shown in Table 2 is clear. These traditional safety analysis methods based on the event chain model are unable to do as much as they can when dealing with computer-oriented automated control system. However, due to the particularity understanding of safety in STAMP, the connotation of safety has been substantially improved from the introduction of concepts such as hierarchical models, process models, and safety constraints.

2.3. System-Theretical Process Analysis (STPA)

STPA is a new hazard analysis technique based on system safety theory. According to the above-mentioned description, an accident is defined as the result of a complex process in which the system behavior goes against the safety constraints. The main steps of STPA can be shown as follows:

Step 1: Identify improper control actions of the system that may cause danger,

Step 2: Determine how potential hazard controls may occur in step 1.

The goal of STPA is to find comprehensive causes of accidents, and those actions which can happen or exist to affect safety are unsafe control actions (UCA). UCAs fall into four general types in STPA:

- (1) An unsafe control action is provided that creates a hazard,
- (2) A required control action is not provided to avoid a hazard,
- (3) A potentially safe control action is provided too late, too early, or in the wrong order,
- (4) A continuous safe control action is provided too long or is stopped too soon.

2.4. A Safety Analysis Framework for Complex Electromechanical System Based on STAMP

The electromechanical equipment system is the most common part of an integrated system, in which humans can operate control system consisting of computer or programmable logic controller (PLC). The cooperation of various parts such as electronic components, mechanical parts, and industrial control algorithms can guarantee system safety of the electromechanical equipment system. Due to the

complex mechanical components and control process, traditional hazard analysis methods based on event chain model have limitations in exploring component interaction failure and process unmatched in such a complex social-technical system. Therefore, a hazard analysis framework for complex electromechanical equipment based on STAMP is proposed in this paper. Figure 6 shows the main diagram of the framework.

Figure 6. Hazard analysis framework for electromechanical equipment system based on STAMP.

Figure 6 can be divided into four parts: (1) Firstly, safety requirements of an electromechanical equipment system can be determined on the basis of system understanding and accident case collection, then hierarchy structure model of equipment and process model of operation should be established. (2) Secondly, safety constraints can be defined by hierarchy structure model and process model combined with safety requirements; Then, safety control structure and safety control process are established. Iterative STPA are performed with the help of basic unsafe control principles to identify unsafe control constraints and example casual scenarios. (3) Specific hazards (such as component failure, components interaction failure, external disturbance, dangerous behavior of the system and so on) for accident can be identified based on the analysis of STPA. (4) Finally, some targeted improvement measures can be added according to some key hazards such as components failure and components interaction failure.

3. Hazard Analysis for Breaking System of Escalator

Emergency braking system is an important part of an escalator, which is crucial for ensuring the safe operation of equipment. The escalator relies on the normal operation of the brake when the operation needs to be stopped or an emergency occurs. In this section, STPA is introduced in the escalator emergency braking system to demonstrate the superiority of the method in a complex social-technical system.

3.1. Overview of Escalator Emergency Braking System

At present, most of the emergency brakes use electromagnetic triggers. The electromagnets keep pulling during normal operation, and the brake turns on when the electromagnets lose power. When the escalator is overspeed or reversed, the emergency brake and the working brake act simultaneously. Based on the above basic logic, when the brake is operating, the operating state of the escalator is first judged based on the measurement result of the proximity switch (speed sensor). If the escalator speed exceeds a certain threshold, the corresponding brake operates. Figure 7 shows the mechanical structure of the escalator brake.

Figure 7. Mechanical structure of escalator emergency brake: (a) Mechanical structure diagram of escalator emergency braking systems (EEBS), (b) Actual ratchet structure.

The emergency brake is set under the following conditions according to national standard: (1) The working brake and the elevator system are connected by the transmission chain, (2) The working brake is not the electromechanical brake, (3) The public transport escalator. The escalator or moving walkway should be stopped at a deceleration with obvious feeling and be kept still under the braking force of emergency brake. In general situation, the emergency brake shall act in either of the following two cases: (1) before the speed exceeds 40% of the rated speed, (2) when the travel direction suddenly changes. Figure 8 shows the speed sensors (a) and overspeed protection switch (b). On the basis of above-mentioned description, the working principle of escalator braking system can be shown in Figure 9.

Figure 8. Speed sensors and overspeed protection switch: (a) The speed sensors, (b) Overspeed protection switch.

Figure 9. The working principle of the escalator braking system.

3.2. Control Structure of EEBS

Braking system is one of the most important equipment for escalators to ensure safety in emergency situations. When the escalator speed monitoring system finds that the speed is abnormal, the control system adopts different protection measures according to different speed thresholds. At the same time, an emergency stop switch is installed on the upper and lower sides of the escalator to facilitate the manual operation of passengers or operators in the event of an emergency. In order to reduce the complexity of the control structure diagram, when the accident occurs, the braking process is divided into two levels: the perspective of the overall operation of the escalator and the perspective of the escalator braking system. Level 1 in Figure 10a is the control chart of the escalator operation, which mainly includes seven parts: designer and manufacturer, operator, passenger, escalator power equipment, escalator control system, brake and emergency stop switch. When an accident occurs, the monitoring module in the escalator power equipment will send a control command to the escalator control system to control the brake action, or the operator and the passenger may also send the brake operation control command to the escalator control system through the emergency stop switch.

Figure 10b shows the control structure of Level 2. Speed sensors, PLC and overspeed judgment algorithm are the core of the controller, and electromagnetic switches can be regarded as the actuator of control structure. Then, the speed of the transmission system is the controlled process of Level 2.

(a)

Figure 10. Cont.

Figure 10. Control structure of escalator operation in two levels: (a) Control structure of escalator operation in Level 1, (b) Control Structure of the braking system in Level 2.

3.3. STPA for Escalator Braking System

After establishing the control structure of the brake-oriented process for escalator operation, control actions can be summarized to further analysis. Tables 3 and 4 list important control process around the time of the brake operation through control structures of two levels. There are seven main control processes in Level 1, and five control process in Level 2. The primary problem is to understand the relationship between controller and controlled process. Then in STPA, with the guidance of basic casual factors of a standard control loop shown in Figure 5, every control process contains potentially unsafe control actions can be organized and concluded in Tables 5 and 6. Unsafe control actions (UCAs) involved in control structure of two levels can be summarized as complete as possible. STPA for Level 2 is similar to the above-mentioned description steps. Meanwhile, some specific UCAs can also be further analyzed. For example, UCA29 can also be the consequence of many causes like workers' lack expertise, wrong installation instructions and limited installation space and so on. That means a new controlled process of UCA29 can be further established, if it is necessary, and the continuous use of STPA at different levels is exactly the advantage of STPA.

Table 3. Control process in Level 1.

#	Control Process	From	to
1	C1 Design or manufacture	Designer or manufacturer	Brake system
2	C2 Running escalator	Operators	Control system
3	C3 Taking escalator	Passengers	escalator
4	C4 Control system running	Control system	Power system
5	C5 issue brake command	Control System	Brake
6	C6 Braking Process	Brake	Power system
7	C7 Emergency Stop	Operators or passengers	Control system

Table 4. Control process in Level 2.

#	Control Action	From	to
1	C8. Speed Measurement	sensors	escalator
2	C9. State judgment by PLC	PLC control system	escalator
3	C10. Issue command by PLC	PLC control system	Brake system
4	C11. brake start	Electromagnetic switch	Pawl of brake
5	C12. Braking Process	Brake	Power system (Driving spindle)

The failure of the escalator equipment may lead to an overturned accident. Once escalator overturned, it would cause serious casualties. According to Table 6, we further analyzed the cause of the brake malfunction (related to UCA42). First, system constraints and sub-system constraints of two levels should be defined as follows:

- (1) System constraints: When the escalator overturned, the brake can start effectively,
- (2) Sub-system constraints: When the brake is turned on, the escalator can effectively slow down.

As for the basic system constraint of the effective start of the brake, if it is regarded as a controlled process, then the brake design and manufacturing department can be considered as the controller of the process, and the escalator operator can be considered as the actuator, and the maintenance personnel can be considered as the sensors of the control process. At this macro level, a basic process model is established. With the help of the lack of control in STAMP, the unsafe constraints that may lead to accidents are shown in Figure 11. Besides the unsafe control factors of each part in Level 1, some other unsafe control factors caused by the interaction failure between parts and some related external causes can also be identified.

In view of the failure of the brake to start the process effectively, we construct a more specific process model from the perspective of the brake operation principle. Taking the escalator PLC control system as the controller, the brake itself as the actuator, and the drive spindle that needs to be decelerated in the event of an accident as the controlled object, a process model is established. Figure 12a shows the mechanical structure of the drive chain protection device and Figure 12b shows the basic working principle of the escalator emergency brake.

Figure 11. Unsafe control action identification of Level 1.

Table 5. Potentially hazardous control actions in Level 1.

#	Control Action	Not Provided	Incorrect Provided	Wrong Time or Wrong Sequence	Incorrect Duration
1	C1 Design or manufacture brake	UCA1 Lack verification	UCA2 original design flaw UCA4 unqualified processing		UCA3 development lifecycle (D & M) is too long
2	C2 Escalator Running	UCA5 Lack effective means of supervision UCA6 No safety hints are set	UCA7 Keep running when escalator breakdown		UCA8 negligent management and maintenance for a long time
3	C3 Taking escalator		UCA9 unsafe behavior or mental of passengers	UCA10 taking escalator when escalator break down	
4	C4 Control system running	UCA11 out of control because of inherent fault	UCA12 wrong control command from staff	UCA13 Unreasonable design of control system	UCA14 control command delay
5	C5 issue brake command	UCA15 No brake command issued in emergency situation		UCA16 Brake command issued when escalator in normal operation	UCA17 Brake command delay when emergency
6	C6 Braking Process	UCA18 Brake is not started	UCA19 Unsuccessful braking	UCA20 Brake when escalator in normal operation	UCA21 Escalator does not stop because of short brake time; UCA22 Serious wear because of long brake time
7	C7 Emergency Stop	UCA23 No operation in an emergency	UCA24 Wrong operation in an emergency	UCA25 operation in normal running	

Table 6. Potentially hazardous control actions in Level 2.

#	Control Action	Not Provided	Incorrect Provided	Wrong Time or Wrong Sequence	Incorrect Duration
1	C8 Speed Measurement using sensors	UCA26 Non installed sensor UCA27 Sensor damaged	UCA28 Measurement Error of sensor UCA29 improper installation position UCA30 signals from sensor are disturbed		UCA31 Resolution or sample rate is low
2	C9 state judgment by PLC		UCA32 incorrect state judgment algorithm	UCA33 wrong state judgment	UCA34 state judgment required time is too long
3	C10 Issue command by PLC	UCA35 No brake command issued by PLC		UCA36 Wrong brake command issued by PLC	
4	C11 brake start	UCA37 The electromagnetic switch failed to start normally	UCA38 The contact fault of electronic components was not detected	UCA39 Electromagnetic switch starting in normal operation	UCA40 The action time of the electromagnetic switch is too long; UCA41 The response time of the brake is too long
5	C12 Braking Process	UCA42 Pawl is not working	UCA43 No effective deceleration of brake operation	UCA44 rake when escalator in normal operation	UCA45 short brake time; UCA46 Serious wear because of long brake time

Figure 12. Structure diagram of EEBS: (a) Mechanical structure of drive chain protection device, (b) Working principle of the brake.

Then on the basis of Tables 5 and 6, in conjunction with the operating context scenario, the causes of the unsafe controls that lead to the danger are identified. Figure 13 concludes the unsafe control actions from Level 2 to form a specific control diagram by using the working principle process shown in Figure 12b. The red segments in this diagram show the potential casual factors that may cause accidents.

According to some unsafe control from Figure 13, some specific example scenarios that violate safety constraints are summarized in the following Table 7. Those example scenarios are simulated to give a specific safety warning of escalator overturned accidents.

Figure 13. Hazardous unsafe control action of the braking process.

In the example scenario, based on the process model, the incentives for breaching safety constraints are summarized from different perspectives of the control structure. It can be seen that although the process model is based on equipment, in addition to component failures that violate safety constraints, it still contains the unsafe constraints that arise from interactions between many hardware and software. For example, in the determination of the escalator's overspeed status, it involves not only the reliability of the sensor signal but also the algorithm itself may be in error or the threshold for starting overspeed status is unreasonable. Too large or too small is not conducive to the brakes playing their due role in critical moments.

Table 7. Specific example Scenarios of hazardous unsafe control.

Unsafe Control (Incentives)	Example Scenario
Unreasonable installation location; Signal from sensor is disturbed; sensor damaged	The sensor does not measure the change effectively when overspeed occurs, which resulting in the PLC not making correct overspeed judgments.
Component of PLC damaged	Velocity judgment can be wrong and command mistake because of the component of PLC damaged.
Unreasonable overspeed judgment algorithm; Trigger threshold of overspeed judgment is too high or too low	The misjudgment of overspeed can lead to frequent starts of emergency brake system, which would influence the operation of escalator and aggravating the wear of mechanical components.
Command mistake from PLC	The brake command is sent during normal operation or the command is not sent when the speed exceed the safe threshold, or there is a delay in the command, increasing the response time of brake system.
Component of brake damaged	The mechanical component of brake system can't afford the instantly impact force and energy when it needs to work.
Component of Driving spindle damaged	The risk of losing power would be increased when components of driving spindle are damaged
High traffic flow	(1) the escalator is running under a heavy load, which would increase the wear of components and risk of component damage; (2) high traffic flow can easily lead to chain reaction and butterfly effect of unsafe behavior
Unsafe behavior and mental state of passenger	The passengers did not grasp the handrails. When an accident occurred, it caused panic, stampede, and increased brake load.
Response time of brake system is too long when accident occurs	When the accident occurs, the overspeed judgment time is long, the PLC does not issue the instruction in time, or the braking time is too short, or the passengers have a long reaction time, all of which cause the time course of the brake action process to be longer than the time course of the accident

4. Result Analysis and Comparison with FTA

In order to show the difference between STPA and FTA, a comparison is performed in this section. Some basic principles of FTA are introduced and fault tree analysis which had been performed on the escalator reversion accident is cited to show the result. Some improvement measures are given to form a better safe brake system.

4.1. FTA of Escalator Breaking System

As mentioned earlier, FTA is a typical top-down risk analysis method. It adopts a logical method and carries out hazard analysis work vividly. Its features are intuitive, clear, clear-cut, and logical, and can be used for qualitative analysis and quantitative analysis. In general, the development of safety system engineering is also based on fault tree analysis. In 1974, the US Atomic Energy Commission published a report on the risk assessment of nuclear power plants, the "Rasmussen Report (WASH-1400 report)", which effectively and extensively applied the FTA, thereby rapidly promoting its development of the FTA [8]. The fault tree is composed of various event symbols and logic gates. The relationship between events is represented by logic gates. Based on the FTA, a fault tree with the escalator reversal as the top event was established as shown in Figure 14.

Figure 14. Fault tree of escalator overturned accident.

4.2. Result Comparison between FTA and STPA

FTA can fully exploit the accident caused by component failure. At the same time, it can depict the chain of events that caused accidents due to the failure of the underlying components. In the above analysis, both STPA and FTA were used in the analysis of escalator reversal accidents. In order to prove the feasibility of the STPA method, Table 8 starts from different objects and compares the results of the two methods. Excluding some of the more subtle aspects, it can be seen that the STPA can identify the cause of the accident that the FTA can identify, but at the same time there are some reasons that are caused by the interaction of the component objects and components considered from the STPA-specific STAMP theory. Emergence reasons. Although the results of STPA analysis may have been considered or are unlikely to occur, these control theories are still one of the reasons that may cause major accidents.

Table 8. Analysis result comparison between fault tree analysis (FTA) and system-theoretic process analysis (STPA).

Object	Identified by Both FTA and STPA	Identified by STPA Only
sensors	Sensors damaged	Unreasonable installation location; Signal from sensor is disturbed
PLC	Component of PLC damaged	overspeed threshold setting; Command delay; Error algorithm
Brake	Component of brake damaged; Braking force is small	Braking signal trigger setting; Unreasonable trigger threshold; short braking duration
Driving spindle	Component of driving spindle damaged	Long time load
Passengers	Heavy load (high traffic flow)	Reaction time of passengers; Mental states of passengers; Long traveling time

4.3. Improvement on Control Process

In the event of an accident, the impact on the individual or society is enormous. The complexity of the system and unreasonable control process, even the tiny design error, play an important role during the emergency situation. Due to the different perspectives to understand hazards and accidents, some inherent flaws can be hidden for a long time. From the above-mentioned description of hazard analysis of escalator brake system, some improvement measures can be added in the controlled process to prevent accidents or improve emergency response capabilities of EEBS.

Figure 15 shows the improved controlled process. Pink lines and dashed boxes indicate added control paths that may improve system safety.

Figure 15. Improvement to escalator brake process.

(1) Passengers, as the primary carrier of the escalator, should be fully utilized to know and protect themselves during the boarding time in case of emergency.

(2) A manual switch for emergency brake not for driving brake is very important in case of state judgment error of automatic emergency brake trigger. In fact, in most escalator reversal accidents, the automatic emergency brake was not triggered is one of the main reasons for the accidents.

(3) Passenger needs an effective way to sense the speed information to make the right response. Another improvement measure is that a spare emergency brake is necessary to help and share the huge impact energy of mechanical friction when the emergency brake is working.

(4) Necessary traffic flow monitoring and control measures should be added to adjust the heavy load during long working time. Then, necessary feedback which can reflect brake information (such as brake time, brake distance, brake force etc.) can be added to the system. This feedback path can record the processing capacity of the braking system in emergency situations and will have important reference value for the design and improvement of the brake.

In fact, the above-mentioned improvement measures have a good practical significance for design and manufacture of EEBS. For example, over-reliance on broken chain detection (BCD) of anti-reversion device is an obvious casual factor for reversion accidents. So, a new trigger mechanism needs to be designed to trigger the anti-reversion protection device. Perhaps environmental decibel detection or vibration monitoring of key driving components could be a good choice. When accident happens, many people around the escalator including the passengers will make a scream or call for help,

which would significantly increase the decibel value of the environmental voice. When environmental decibel value reaches a certain threshold, the trigger can act timely. Or a vibration sensor for condition monitoring of key driving components can also help to trigger the anti-reversion device when abnormal vibration information appears during accident period. It should be noted that the new trigger mechanism here is only an auxiliary protection device and does not replace the original basic protection principle based on BCD. Here we give a more concrete solution to the above-mentioned BCD, environmental decibel detection and vibration detection to solve the anti-reverse device triggering in Figure 16. We hope to use some comprehensive triggering conditions to reduce the possibility of misjudgment by a single trigger. Therefore, by collecting the signal detected by BCD, the sound signal detected by environmental decibels and the vibration signal of key components, and then using signal processing methods to judge the true state of the escalator reflected by above information, and then logically controlling whether or not to determine to trigger the anti-reverse device. The logic control algorithm here requires a lot of experimentation and data analysis. Here is just a way to solve the above-mentioned improvement measures in a practical way, and specific devices or algorithms require extensive experimentation and validation in the future.

Figure 16. Comprehensive trigger mechanism of the anti-reversion device.

5. Conclusions

Operational safety analysis for escalator has become more and more important with the increasing application of escalators in daily life. Traditional hazard analysis methods have certain limitations in complex social-technical systems. Therefore, a system safety analysis method applied for escalator emergency brake related accidents based on system-theoretic accident model and process was introduced in this paper. At the beginning of this paper, a brief illustration of the basic principles of STAMP and STPA are introduced, and some advantages and disadvantages are compared to further understand STAMP. Then, unsafe control actions of escalator emergency braking system are recognized from two-level control structures, and how potentially hazardous control actions will affect the safety of emergency braking system is clearly shown in a specific operation control diagram. Meanwhile, example scenarios of hazardous unsafe control are given to explain some details about emergency situations that may happen in real operation conditions. Next, a fault tree analysis that had been performed on the escalator overturned accident is cited to make a comparison with STPA analysis. An obvious difference between two methods is that majority hazards related with component damaged can be identified by both, while some other hazards that focus on the interaction between system components (such as state judgment algorithm, command delay of control system, insufficient response time margin, response capability and mental state of passengers, etc.) can only be identified by STPA. Based on fully understanding the causal factors that may lead to an accident, some targeted improvements can be realized and modified for a better safe system.

The powerful practicality of STAMP which helps to know the safety of cybernetics provides an effective way for more comprehensive hazard analysis. Hierarchical multilevel model provides the possibility to analyze component interaction failures in complex systems, which is also the vitality of the STAMP model. STAMP and STPA emphasize social factors and component interaction. However, this method is mostly used for qualitative analysis and needs to be combined with other methods for quantitative analysis. This is exactly the direction that needs further study in the future. Some specific experimental work needs to be carried out to verify the conclusion of this paper. Besides, the specific control algorithm or device should be paid more attention to realize the comprehensive trigger mechanism of anti-reversion device proposed in Section 4.3. In future research, we will pay more attention to the relevant signal processing, control theory, and mechanical design theory, and complete the safety improvement strategies proposed in this paper and improve the safety of the escalator braking system.

Author Contributions: Z.Z. proposed the idea of the paper and wrote the paper; Y.Z. proofread the manuscript; J.C. contributed the conclusion and guided the manuscript; T.A. analyzed the case studies.

Funding: This work was supported in part by the National Key Research and Development Program of China under Grant 2017YFC0805701, in part by the National Natural Science Foundation of China under Grant 51775411, in part by National S&T Major Project under Grant 2017ZX04011-013, in part by the China Postdoctoral Science Foundation under Grant 2018M631145 and Natural Science Basic Research Plan in Shaanxi Province of China under Grant 2019JM-041.

Acknowledgments: The authors would like to sincerely thank all the anonymous reviewers for the valuable comments that greatly helped to improve the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Xing, Y.; Dissanayake, S.; Lu, J.; Long, S.; Lou, Y. An analysis of escalator-related injuries in metro stations in China, 2013–2015. *Accid. Anal. Prev.* **2017**, *122*, 332–341. [[CrossRef](#)] [[PubMed](#)]
2. Shi, C.; Zhong, M.; Nong, X.; He, L.; Shi, J.; Feng, G. Modeling and safety strategy of passenger evacuation in a metro station in China. *Saf. Sci.* **2012**, *50*, 1319–1332. [[CrossRef](#)]
3. Rogova, E.; Lodewijks, G. Braking system redundancy requirements for moving walks. *Reliab. Eng. Syst. Saf.* **2015**, *133*, 203–211. [[CrossRef](#)]
4. Chan, J.P.; Gschwendtner, G. Braking performance analysis of an escalator system using multibody dynamics simulation technology. *J. Mech. Sci. Technol.* **2015**, *29*, 2645–2651.
5. Mishra, K.M.; Huhtala, K. Elevator fault detection using profile extraction and deep autoencoder feature extraction for acceleration and magnetic signals. *Appl. Sci.* **2019**, *9*, 2990. [[CrossRef](#)]
6. Greenwood, M.; Yule, G. An inquiry into the nature of frequency distributions representative of multiple happenings, with particular reference to the occurrence of multiple accidents or disease or repeated accidents. *J. Roy. Stat. Soc.* **1920**, *83*, 255. [[CrossRef](#)]
7. Heinrich, H. *Industrial Accident Prevention*, 1st ed.; McGraw Hill: New York, NY, USA, 1932.
8. Haddon, W. The changing approach to the epidemiology, prevention, and amelioration of trauma: The transition to approaches ethologically rather than descriptively based. *Am. J. Public Health* **1968**, *58*, 1431–1438. [[CrossRef](#)]
9. Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. Available online: [URLhttps://digital.library.unt.edu/ark:/67531/metadc784367/](https://digital.library.unt.edu/ark:/67531/metadc784367/) (accessed on 23 October 2019).
10. Reason, J. *Managing the Risks of Organizational Accidents*; Ashgate: Adershot, UK, 1997.
11. Perrow, C. *Normal Accidents: Living with High-Risk Technologies*; Basic Books: New York, NY, USA, 1984.
12. Porte, T.R.L.; Consolini, P. Working in theory but not in practice: Theoretical challenges in high reliability organizations. *J. Public Adm. Res. Theory* **1991**, *1*, 19–47.
13. Leveson, N.; Dulac, N.; Marais, K.; Carrol, J. Moving beyond normal accidents and high reliability organizations: A systems approach to safety in complex systems. *Org. Stud.* **2009**, *30*, 227–249. [[CrossRef](#)]
14. Rasmussen, J. Risk management in a dynamic society: A modeling problem. *Saf. Sci.* **1997**, *27*, 183–213. [[CrossRef](#)]

15. Leveson, N. A new accident model for engineering safer systems. *Saf. Sci.* **2004**, *42*, 237–270. [CrossRef]
16. Mohaghegh, Z.; Mosleh, A. Incorporating organizational factors into probabilistic risk assessment of complex socio-technical systems: Principles and theoretical foundations. *Saf. Sci.* **2009**, *47*, 1139–1158. [CrossRef]
17. Mohaghegh, Z.; Kazemi, R.; Mosleh, A. Incorporating organizational factors into probabilistic risk assessment (PRA) of complex socio-technical systems: A hybrid technique formalization. *Reliab. Eng. Syst. Saf.* **2009**, *94*, 1000–1018. [CrossRef]
18. Fleming, C.H.; Leveson, N.G. Early concept development and safety analysis of future transportation systems. *IEEE Trans. Intell. Transp. Syst.* **2016**, 1–12. [CrossRef]
19. A Comparison of STPA and the ARP 4761 Safety Assessment Process. Available online: <http://sunnyday.mit.edu/papers/ARP4761-Comparison-Report-final-1.pdf> (accessed on 23 October 2019).
20. Ishimatsu, T.; Leveson, N.G.; Thomas, J.P.; Katahira, M.; Miyamoto, Y.; Ujii, R.; Nakao, H.; Hoshino, N.; Fleming, C.H. Hazard analysis of complex spacecraft using systems-theoretic process analysis. *J. Spacecr. Rockets* **2014**, *51*, 509–522. [CrossRef]
21. Xiangkun, M.; Guoming, C.; Jihao, S.; Gaogeng, Z.; Yuan, Z. STAMP-based analysis of deepwater well control safety. *J. Loss Prev. Process. Ind.* **2018**, *552018*, 41–52.
22. Mahajan, H.S.; Bradley, T.; Pasricha, S. Application of systems theoretic process analysis to a lane keeping assist system. *Reliab. Eng. Syst. Saf.* **2017**, *167*, 177–183. [CrossRef]
23. Yunhua, G.; Yuntao, L. STAMP-based causal analysis of China-Donghuang oil transportation pipeline leakage and explosion accident. *J. Loss Prev. Process. Ind.* **2018**, *56*, 402–413.
24. Chi, C.F.; Chang, T.C.; Tsou, C.L. In-depth investigation of escalator riding accidents in heavy capacity MRT stations. *Accid. Anal. Prev.* **2006**, *38*, 662–670. [CrossRef]
25. Algin, A.; Gulacti, U.; Erdogan, M.O.; Tayfur, I.; Yusufoglu, K.; Lok, U. Escalator-related injuries in one of the deepest subway stations in Europe. *Ann. Saudi. Med.* **2019**, *39*, 112–117. [CrossRef]
26. Kefan, X.; Zimei, L. Factors influencing escalator-related incidents in China: A systematic analysis using ISM-DEMATEL method. *Int. J. Environ. Res. Public Health* **2019**, *16*, 2478.
27. Li, W.; Gong, J.; Yu, P.; Shen, S. Modeling, simulation and analysis of group trampling risks during escalator transfers. *Phys. A. Stat. Mech. Appl.* **2016**, *444*, 970–984. [CrossRef]
28. Li, W.; Gong, J.; Yu, P.; Shen, S.; Li, Y.; Duan, Q. Simulation and analysis of congestion risk during escalator transfers using a modified social force model. *Phys. A. Stat. Mech. Appl.* **2015**, *420*, 28–40. [CrossRef]
29. Lee, J.Y.S.; Lam, W.H.K.; Wong, S.C. Pedestrian Simulation Model for Hong Kong Underground Stations. In Proceedings of the Intelligent Transportation Systems, Oakland, CA, USA, 25–29 August 2001; pp. 554–558.
30. Wang, W.; Li, X.; Pan, Q.L. Notice of Retraction Risk Management based on the Escalator Overturned Accident. In Proceedings of the International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering, Emeishan, China, 15–18 July 2013; pp. 22–27.
31. Priestley, K.; Lee, G. Human Factors in Railway Operations. Railway Engineering—Challenges for Railway Transportation in Information Age. In Proceedings of the ICRE 2008: International Conference on IET, Hong Kong, China, 25–28 March 2008.
32. Anis, B.; Nga, N.; Faïda, M.; Jean-Yves, C.; Abdelfattah, M. Improved safety analysis integration in a systems engineering approach. *Appl. Sci.* **2019**, *9*, 1246.
33. Yongming, Z.; Zhe, Y.; Feng, Y.; Jiawei, Y.; Bao, D. A novel reconstruction approach to elevator energy conservation based on a DC micro-grid in high-rise buildings. *Energies* **2019**, *12*, 33.
34. Al-Kodmany, K. Tall buildings and elevators: A review of recent technological advances. *Buildings* **2015**, *5*, 1070–1104. [CrossRef]
35. Stamatis, K. Predictive maintenance of hydraulic lifts through lubricating oil analysis. *Machines* **2014**, *2*, 1–12.
36. Oh, S.; Hwang, D.; Kim, K.H.; Kim, K. Escalator: An autonomous scheduling scheme for convergecast in TSCH. *Sensors* **2018**, *18*, 1209. [CrossRef]