Causal Analysis to a Subway Accident: A Comparison of STAMP and RAIB

Yao Zhou[1] and Fei Yan[2]

[1]*School of electronic and information engineering, Beijing Jiaotong University, Beijing 100044, China*
[2]*National Engineering Research Center of Rail Transportation Operation and Control System, Beijing Jiaotong University, Beijing 100044, China*

Abstract. Accident investigation and analysis after the accident, vital to prevent the occurrence of similar accident and improve the safety of the system. Different methods led to a different understanding of the accident. In this paper, a subway accident was analysed with a systemic accident analysis model – STAMP (System-Theoretic Accident Modelling and Processes). The hierarchical safety control structure was obtained, and the system-level safety constraints were obtained, controllers of the physical layer were analysed one by one, and put forward the relevant safety requirements and constraints, the dynamic analysis of the structure of the safety control is carried out, and the targeted recommendations are pointed out. In comparison with the analysis results obtained by the Rail Accident Investigation Branch (RAIB). Some useful findings have been concluded. STAMP treats safety as a control problem and reduces or eliminates causes of the accident from the controlling perspective. Whereas RAIB obtains causes of the accident by analysing the sequence of events related to the accident and reasons of these events, then chooses one(or more)event(s) as the immediate cause and some of the key events as causal factors. RAIB analysis is based on the sequential event models, but STAMP analysis provides us with a holistic, dynamic way to control system to maintain safety.

1 Introduction

Accident investigation and analysis theory is the way that we find out causes of the accident, helping us to understand why the accident happened and how it happened. It determines whether we can prevent similar incidents from happening. Most accident reports are written inadequately about causes of the accident, and the analysis frequently stops after finding someone to blame--usually a human operator--and the opportunity to learn important lessons is lost [1]. It is also acknowledged that our understanding of accidents remains incomplete and that accidents will continue to occur within complex socio-technical systems [2].

Traditional cause--effect accident models suggest that complex systems accidents are caused by events such as catastrophic equipment failure or an unsafe human action. However, as system complexity has increased over time, many accidents do not simply resulted from such trigger events. These accidents are contributed by different factors, because there are complex phenomenon within the normal operational variability of a system [3]. As a typical complex socio-technical system, subway system involves many stakeholders, so the safety of subway cannot be ignored. With the increase of the speed of subway, global subway accidents continue to increase, resulting in a large number of casualties, which has seriously threatened the people's life. Therefore, accident analysis method that are suitable for the subway accident analysis is urgently needed.

There are currently three dominant accident causation models: Rasmussen's (1997) risk management framework (e.g. [4]); Reason's (1990) omnipresent Swiss Cheese model (e.g. [5]); and Leveson's (2004) Systems Theoretic Accident Modelling and Processes model (STAMP e.g. [6]). STAMP can be used to identify the problems that need to be answered to fully understand why the accident occurred. It provides the basis for maximizing learning from the events [1]. In STAMP, an accident is regarded as involving a complex process, not just individual events. STAMP can present a dynamic process which led to the accident, we can know what safety constraints were violated through the safety control structure, and what systemic control failures happened in the accident. Thereby obtaining targeted measures to make up for system safety vulnerabilities.

The aim of this paper is to compare the analysis results of RAIB with that of STAMP. STAMP was used to analyse an accident and the analysis results were compared with the analysis results of RAIB. Some difference between these methods were found. In order to achieve this aim, we should:

1. Analyse the accident (the passenger trapped in train doors and dragged at Clapham south station) using STAMP, from the analysis process to show how this method is used to find out causes of the accident.
2. In this case, compare causes of the accident obtained by two methods and find the difference among methods and which method can provide a more thorough and complete analysis.

2 The passenger trapped in train doors and dragged at Clapham South station

At about 08:00 hrs on the morning of Thursday 12, March 2015, a passenger's coat became trapped in the doors of a northbound Northern line train at Clapham South Station on the London Underground. The train departed and the passenger was dragged along the platform, fell to the ground, became separated from her coat and then fell into the gap between the train and the platform [7].

The passenger sustained a broken arm, and injured to her shoulder and face. There was no damage to the train, or to the railway infrastructure, and London Underground staff authorised reopening of the station at 09:11 hrs.

3 Methods

3.1 The analysis methods

3.1.1 RAIB

The Rail Accident Investigation Branch (RAIB) is a British government agency that investigates accidents and incidents which occur on the UK main line networks (Network Rail and Northern Ireland Railways), London Underground, other metro systems, tramways, heritage railways and the UK part of the Channel Tunnel in order to find a cause, not to lay blame. Created in 2005, it is required by law to investigate accidents causing death, serious injuries or extensive damage. It also has authority to investigate incidents that could have resulted in accidents. It currently has two bases - Derby and Farnborough - to allow it to respond quickly to accidents.

3.1.2 STAMP

The accident causation model called STAMP was developed by Prof. Nancy Leveson from MIT. Accidents are seen as resulting from inadequate control. The STAMP accident causation model is built on three basic concepts - safety constraints, a hierarchical safety control structure, and process models [8]. STAMP is a constraints-based model which focuses on the interactions between system components and the control mechanisms used throughout the work system [9]. Unlike conventional accident causation models, STAMP is not based on chain of events. It is based on system theory where each level or the organization plays a major role in contributing to an accident or attaining successful system safety controls. Thus STAMP prevails conventional accident models by accounting for organizational factors, human error, and adaptation to change over time. In STAMP, system safety is not achieved by preventing component failure measures; in fact, it is achieved by enforcing safety constraints continuously [10]. Therefore, accidents do not occur because of failure of components, they occur because of ineffective safety constraint where main focus is not on how to prevent failure, but on how to design better safety controls [6].

3.2 Accident analysis process

3.2.1 RAIB analysis process

The purpose of a RAIB investigation is to improve railway safety by preventing future railway accidents or by mitigating their consequences. It is not the purpose of such an investigation to establish blame or liability [7]. RAIB analysis process is as follows:

Firstly, a summary of the accident tells us what happened and some basic information related to the accident. Then the sequence of events are extracted. Key facts and analysis are composed of four steps: Identification of the immediate cause, identification of causal factors and the factors affecting the severity of consequences and previous occurrences of a similar character. Finally, according to this investigation, comprehensive recommendations for this investigation are made.

3.2.2 STAMP analysis process

STAMP analyses each component and controller of the system according to the safety control structure. Then the safety constraints that were violated at each level of this control structure were obtained, and the reasons that safety constraints was violated were also found. The main steps of STAMP analysis are as follows:

1. Identify the system(s) and hazard(s) involved in the loss.
2. Identify the system safety constraints and system requirements associated with that hazard.
3. Document the safety control structure in place to control the hazard and enforce the safety constraints.
4. Determine the proximate events leading to the loss.
5. Analyse the loss at the physical system level.
6. Moving up the levels of the safety control structure, determine how and why each successive higher level allowed or contributed to the inadequate control at the current level.
7. Examine overall coordination and communication contributors to the loss.
8. Determine the dynamics and changes in the system and the safety control structure relating to the loss and any weakening of the safety control structure over time. Finally, generate recommendations.

4 Applying the analysis models to the accident

4.1 RAIB analysis output

The RAIB analysis output see Rail Accident Investigation report: Passenger trapped in train doors and dragged at Clapham South station 12 March 2015 [7].

4.2 STAMP model analysis

4.2.1 Establish chain of events

While the event chain does not provide the most important causality information, the basic events related to the loss do need to be identified so that the physical process involved in the loss can be understood [1]. The event chain has been described in table 1.

Table 1. Proximity of events.

Time	Events
19:59:25	Train stops, and the passenger entered the fourth car using the rearmost double door
19:59:26	Doors open, the passenger step back out of the car and step into the gap of about 300mm between the yellow line and the train
19:59:39	CSA raises baton
19:59:41	Train operator presses door close button
19:59:45	Doors start to close (but do not fully close)
19:59:48	Train operator presses door open buttons because pilot light does not illuminate
19:59:50	Train operator presses door close button
19:59:51	Doors open with normal delayed response from button operation
19:59:56	Doors start to close, trapping the passenger's coat
19:59:57	Doors closed, the passenger noticed that the coat was caught
19:59:50	Train operator presses start buttons
19:59:54	Train starts to move
19:59:58	Passenger dragged past CSA
19:59:58	CSA starts to run and lowers his baton
20:00:00	Train operator applies emergency brake at train speed of 31km/h(He saw this unusual passenger movement on the in-cab screen)
20:00:07	Train stops

4.2.2 Identify the system(s) and hazard(s) involved in the loss

The systems or controllers involved in the accident mainly are: the interlock system, the train operator and CSA (the customer services assistant). The physical process is: when all passengers on board, interlock system detects whether all doors are locked in the fully closed position, and if so, the pilot light in the driving cab will light up. The train operator will press the start button after CSA raise the baton, the system hierarchical control structure diagram is shown in Figure 1, which from bottom to top is the physical layer, the operating layer and management layer, and the hierarchical control structure shows the main components of the system and the interaction between them.

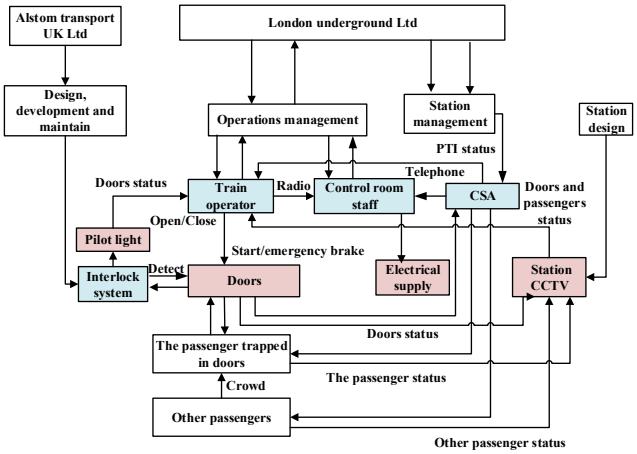

Figure 1. The hierarchical safety control structure.

An accident or loss event for the train moving processes can be defined as the death, illness or injury due to the passengers (or objects carried by passengers) trapped in train doors and dragged. The hazard is that someone trapped in doors while the train is moving. System-level safety constraints as follows:

(1) The train control system must effectively detect objects between the doors before starting.
(2) Before starting, the safety of the platform and the platform train interface (PTI) must be ensured.
(3) Must ensure passengers stay in a safe position on the platform when train enter/leave the station.
(4) Available and effective measures must be taken to deal with the injured person in case of danger.
(5) Emergency treatment measures must be used to protect the passengers and the relevant personnel, minimizing casualties and losses.

4.2.3 Analysing the physical process

Identifying the physical and operational controls and any potential physical failures, dysfunctional interactions and communication, or unhandled external disturbances that contributed to the events [8]. The goal is to determine why the physical controls in place were ineffective in preventing the hazard [11]. Physical processes are shown in figure 2.

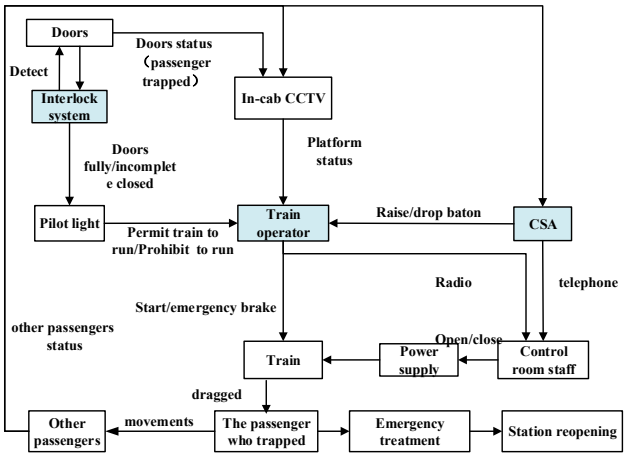

Figure 2. Analysis of physical processes.

The analysis results of physical layer are shown as follow:

Safety Requirements and Constraints Violated
- The train door control system must be able to detect whether there is an object was trapped between the door leaves during the process of closing the door, not only to detect the distance between the door leaves.
- Door control system must ensure that nothing between the doors, then provide the train operator with the doors is fully closed.
- The position where the detector located must ensure the distance will not affect the detection capability.
- The design of the detector must take into account the effect of the door seals flexibility on the detection capability.
- The station CCTV must be installed in accordance with the relevant standards, and have a record of installation and maintenance.
- The in-cab CCTV system must always ensure the train operator can see the entire length of the train.
- The in-cab CCTV system must be qualified products, to ensure the data can be saved in real time.
- The design of the pushback system must consider the train operation direction and the direction of the possible force, ensue the door can be opened in case of emergency.
- The design of the edge of the platform must meet relevant standards

Failures and Inadequate Controls
- The door control system provide the door is fully closed to train operator, but there is an object was trapped between the door leaves.
- The train's door control system did not detect that an object was trapped between the door leaves.
- The detector does not detect the passenger's clothes, because clothes are far away from the detector.
- The in-cab CCTV had no record of accidents related video.
- The pushback system does not work when the passengers trapped, causing the passenger could not remove the coat from the door.

Physical Contextual Factors
- The design of train doors is intended to ensure that they will not be detected closed if there is a 5 mm visible gap between the door seals when these are not compressed. But the coat material compressed and the gap between the outer faces of the door seals was only 4 mm.
- The detector at the top of the door, and the coat was trapped about 0.5 meters above floor level, so the detector is less sensitive to objects that are positioned lower down.
- Only one leaf of the door with the pushback system, and the passenger apply the force on the fixed leaf.

4.2.4 Analysing the higher levels of the safety control structure

This part will analyse accident involved operators, from the following aspects: safety-related responsibilities, context, unsafe decision and control actions, and mental model flaws [12].

The train operator：
The train operator should check the entire platform-train interface, it is necessary to check again before opening the door, before closing the door and before leaving the station, so that the train operator can promptly eliminate the unsafe state on the platform. Analysis results as follows:

Safety-related responsibilities
- Monitor the train operation.
- Focus on the CCTV, ensure that there is no exceptions at PTI,
- To communication with CSA, grasp the platform status in real time.
- When the view is hindered, should actively look for other ways to check the PTI, and pay attention to other signs may cause exceptions.
- After several times to confirm the safety of platform train interface, then press the start buttons.
- Must always pay close attention to CCTV during the leave station process, ensure the PTI safety.
- Must take emergency measures immediately when necessary.

Context
- The train operator had been driving for 14 years, very skilled and experienced in their own work, and also clear all kinds of emergency response measures.
- The station was crowed, blocking the train operator's vision and can't see the complete doors.

Unsafe decision and control actions
- Press the start buttons while the passenger was trapped in the door.
- Press the close buttons after see that the CSA raises the baton without other confirmation.
- Didn't carefully observe the CCTV and didn't find that the passenger who was trapped in the door.

Mental model flaws
- After the Pilot light indicates that doors fully closed, thought that there is no exceptions.
- Did not know the passenger was trapped in the door.
- Did not know CSA did not find the trapped passenger.
- In order to reduce the station crowd, want to minimize the train stop time

The CSA：
The CSA was performing station assistant duties, including: managing the platform train interface and involve managing passenger behaviour and movements on the platform. Analysis results as follows:

Safety-related responsibilities
- Must ensure that the platform-train interface is safe during the train stop and depart process.
- Effectively manage and organize the passengers on the platform to ensure that the passengers are in a safe position.
- Must ensure that the door is safe then raise the baton.
- Must alerts the passengers to be careful and inform the train operation of station status.
- Must take emergency measures immediately when necessary.

Context
- The CSA about 10 meters from the door where the passenger was trapped.
- CSA needs to organize a large number of passengers during the busy morning peak.
- Must ensure safety and efficiency during door closure and train departure.
- CSA do the same work at other stations.

Unsafe decision and control actions
- Raise the baton while the passenger was trapped in the door.
- No further confirmation of the platform-train interface safety.
- The CSA heard shouting on the platform but did not confirm.
- The CSA did not organize the passengers to stand in a safe position

Mental model flaws
- Did not know the passenger was trapped in the door.
- Thought sounded more like an argument than someone in difficulty.
- Thought that there is no exceptions before raise the baton.

4.2.5 Coordination and communication

To establish an effective safety control structure, effective coordination and communication between parties not in direct hierarchical control levels is important [8]. The development and management team must provide complete operation manuals to the communication between the train operator, the CSA and electricity control operator. In this accident, the CSA uses a baton to transmit signals to the train operator, there is no specific provision about what conditions need to be met before CSA raise the baton, the responsibility distribution of the CSA is not clear.

4.2.6 Dynamic analysis of safety control structure

Most major accidents result from a migration of the system toward reduced safety margins over time. Pressure from commercial competition is one cause of this degradation in safety. It is, of course, a very common one [13]. Usually there are precursors signalling the increasing risks associated with these changes in the form of minor incidents and accidents, but in this case, as in so many others, these precursors were not recognized [13]. For example, in this accident, similar incident didn't attract enough attention and appropriate adjustment measures were also didn't carried out.

In many cases, such as the busy morning peak, in order to maintain the train throughput and expedite prompt boarding of trains, delay of the train will lead to the station congestion and speed up the production of potential risks, this means stop time need to be reduced as much as possible and PTI risk need to be controlled at the same time. Therefore, train operator and CSA will reduce the safety margin, such as the CSA need to minimize the station congestion and to ensure the PTI safety at the same time, the workload is large. In addition, with the extension of working hours, the operator may encounter some common abnormal activities on weekdays, may ignore the rules and regulations. In this accident, the CSA heard shouting on the platform, did not confirm the PTI was safe and give the confirmation signal.

Like the operators, the device will also reduce the safety margin over time. The equipment should always be checked regularly and the equipment breakdown which appeared frequently should be paid enough attention [10]. In this accident, the detection ability of door control system would decrease over time or lose detection capability, that didn't attracted enough attention, if the attention had been paid to the detected faults, a good solution would be taken.

4.2.7 Issue recommendations

Some suggestions are put forward from the aspects of equipment safety constraints, hardware and software design, inappropriate control behaviour and so on.

Physical device：

1. Improving the door control system, so that it can detect objects trapped in train doors, such as installing the sensing element on the door leaf.
2. Only when the distance between the doors meet the requirements, and there is no objects in train doors, the door is fully closed. Considering the installation position of the detector, to ensure the detection accuracy is not affected.
3. Because the congestion will make the train operator's vision is blocked, suggest an appropriate increase in the number of station CCTV or change the location of the CCTV.
4. Installing pushback mechanism on each door leaf, so the force can be applied in any direction and the door will be slightly opened, so that passengers can save themselves if they are trapped.

Operators：

1. The train operator shall always clear the status of the PTI and on-board equipment status in real time and need to confirm again before start, when the operation condition is satisfied, then press the start button. Take emergency measures immediately in case of emergency situations.
2. The CSA should always clear the status of the PTI and use the way of patrol back and forth to check the PTI, and check any abnormal situation may result in danger to ensure the safety of passengers.
3. During the busy morning peak, the CSA is responsible for too many duties, suggest to increase the staff members and reduce the work time, besides, to improve the organization efficiency and reduce the work mistake.
4. Regularly carry out operation and emergency treatment training to operators, pay more attention to the problems that often appeared in daily work. In case of emergency, the proper measures should be taken quickly to minimize the casualties and losses.

5 Discussion

5.1 Comparison of causal analysis process

From the results of the two causal analysis, they are clearly described the accident. According to the analysis of RAIB, we know the details of the accident and sequence of events, but there is no complete and adequate answer to the question of why the accident happened and what is the relationship between them, such as why the train operator presses the start button without being able to see the entire door and why the CSA raises the baton without confirming that the PTI is safe and so on. The accident analysis method used by RAIB can be summarized as shown in Figure 3.

Figure 3. RAIB analysis process.

RAIB provides sufficient data involved in a particular accident, such as the environment in which the accident occurred, equipment failure and operator failures at the

time of the accident, and the similar accident that occurred before.

A more complete accident analysis should find out why the accident happened and how to prevent it from reoccurring in the future [6]. Causal analysis of STAMP start from the lower layer of the system control structure, check whether the control command in the structure is properly executed, if not, why? Then from the physical layer and operate layer to analyse the various components and controllers involved in the accident one by one, determine the safety requirements and constraints that they violated, and unsafe control action, have a holistic, systematic understanding of the accident [14]. The use of STAMP does not lead to identifying single causal factors or variables. Instead it provides the ability to examine the entire sociotechnical system design to identify the weaknesses in the existing safety control structure and to identify changes that will not simply eliminate symptoms but potentially all the causal factors, including the systemic ones [1]. STAMP provides an overview of how the system should have been controlled and how the accident in question should have been prevented from happening as well as the relations between actors, and the context in which the accident occurred [9]. Not only all of the failure were identified, but the context and mental model flows were also analysed.

5.2 Comparison of accident causes

RAIB analyses the cause of the accident by accident-related events, selects the event which closest to the accident as the immediate cause and other related events as the causal factors. STAMP believes that the accident was caused by a violation of the safety constraints, in this accident, including: the CSA did not fully see the door and raise the baton, during the busy morning peak, only one CSA to check the entire platform is difficult to find out the abnormal situation and may send the wrong message to the train operator. Besides, the train door control system cannot detect the objects between the doors and the train operator cannot see the entire doors in the CCTV in-cab and press the start button. For the reason that CSA did not find the trapped passenger, we cannot simply say that CSA did not fulfil his duties, London Underground's work configuration is not reasonable, did not take into account the peak hours, a CSA cannot check the entire platform. Some adjustments should be made, such as adjusting the number of CSA or adding additional ancillary measures according to the situation at different times to ensure the safety of the platform train interface.

6 Conclusions

RAIB analysis is more of an objective analysis and explanation as the third party in terms of the accident, RAIB can provide the analyst with all the events and details associated with the accident, however, we do not know the relationship between these events and what role it has played in the accident. Therefore, RAIB analysis can be used as an information source for us to understand details of the accident. STAMP analysis provides an overall understanding of the organization, management, and operational framework of the system by the hierarchical control structure. This is what the other methods do not have. Besides, STAMP analyses the relationship between various causal factors and causes for the human error at that time, and provides a comprehensive perspective to ensure the safety of system.

References

1. N. Leveson, Engineering a Safer World: Systems Th inking Applied to Safety, MIT Press, 2011.
2. E. Hollnagel, Ergonomics, **50**(6), 961-962 (2004).
3. P.V.R.D. Carvalho, Reliab Eng Syst Safe, **96**(11), 1 482-1498 (2011).
4. I. Svedung, J. Rasmussen, Safety Sci, **40**(5), 397-417 (2002).
5. W. Ward, J. Brewbaker, English Journal, **94**(6), 111 (2005).
6. H. Altabbakh, M. Alkazimi, S. Murray, G. Katie, J. Loss Prevent Proc, **32**, 109-119 (2014).
7. Branch, R.A.I., Rail accident report: Passenger trapped in train doors and dragged at clapham south station - 12 march 2015 .
8. A. Dong, Application of CAST and STPA to railroad safety in China, 2012.
9. P.M. Salmon, M. Cornelissen, M.J. Trotter, Safety S ci, **50**(4), 1158-1170 (2012).
10. N. Leveson, Safety Sci, **42**(4), 237-270 (2002).
11. M. Ouyang, L. Hong, M.H. Yu, Q. Fei, Safety Sci, **4 8**(5), 544-555 (2010).
12. P. Underwood, P. Waterson, G. Braithwaite, Safety S ci, **82**(42), 129-143 (2016).
13. N.G. Leveson, Safety Sci, **49**(1), 55-64 (2011).
14. K. Hardy, F. Guarnieri, Using a Systemic Model of Accident for Improving Innovative Technologies: Ap plication and Limitations of the STAMP model to a Process for Treatment of Contaminated Substances, 2011.