First International Conference on Rail Transportation
Chengdu, China, July 10-12, 2017

Analysing Railway Safety with Systems Thinking

Yadong ZHANG[1], Xiaocheng GE[2*] , Wudong Yang[1] and Jin GUO[1]
[1.] *School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China*
[2.] *Institute of Railway Research, School of Computing and Engineering, University of Huddersfield, Huddersfield, HD1 3DH, UK*
**Corresponding author email:* xiaocheng.ge@gmail.com

Abstract : Railway system is a socio-technical system because the operation of such system also heavily relies on the management of human activities and operating procedures in the organisation, as well as the execution of technical subsystems. Safety of these systems therefore is more than just about engineering their technical subsystems. The latest approach from systems engineering considers that an accident is due to inadequate controlled interactions in the system and is usually a dynamic event chain started from the activation of a hazard and culminated in a complex process of sequential and concurrent events until the system is eventually out of control. Meanwhile the analysis of these systems's safety becomes much harder when simply applying the traditional techniques of safety assessment. It is because, first of all, a social-technical system consists of a lot of complex and non-linear interactions, traditional techniques show their limits when analysing complex systems. And secondly, the safety of a social-technical system requires a system perspective, which should take all the behaviours (desired and undesired but predicted) of a system as a whole in the context of its environment. To capture the information needed, the models for these analyses (i.e., fault tree and FMEA table) will become too complex to have a systemic view of each individual causal factor. In this paper, we proposed an approach based on system thinking and system dynamics to analyse the safety of a social-technical system. The case study of a tram accident is simple enough for the purpose of demonstrating its feasibility and benefits. The comparison with fault tree analysis was conducted, but it was not for the evaluation of our approach. The real evaluation comes from the extensive applications in real world.
Keywords: Socio-technical systems; railway system; safety analysis; system engineering; hybrid system dynamics

1 Introduction

A safety-critical system is a class of engineered systems that may pose significant safety risks to its operators, the public and the environment. The development of these systems demands a rigorous process of assessment and assurance to demonstrate that risks to the system's safety, even if some components fail, are mitigated to an acceptable level. However, significant changes have occurred in the types of systems to be built today and the context in which they are being built (Levenson, 2004). These changes to the system have exposed the limits of traditional safety engineering.

System safety somehow is more than just about engineering a technical system. The concerns of system safety have already extended beyond the boundary from a technical (computer-based) system to include things such as social and managerial processes. There is some explicit evidence to support this view. A recent tram accident involved a point (switch) moving under a tram (RAIB, 2012). Although rigorous hazard and safety assessment had been undertaken for the technical systems, the hazard

was “missed” apparently at least in part because it arose out of the complex interactions, including those between the technical systems and social systems in the entire tram control system. Operation of modern safety critical systems, like a rail traffic management system, involved management of human activities and processes, as well as executions of technical systems, thus the systems are often referred as socio-technical systems. The term “socio-technical” emphasises the interconnections of “social” and “technical” elements in the system. The fundamental ideas/principles of a socio-technical approach are:

1) interactions of social and technical factors create the decisive conditions for successful (or unsuccessful) behaviours of the entire system. These interactions are comprised partly of linear causal relationships, which are normally specified and engineered, for example in various operational procedure. They also increase “non-linear”, complex, even unpredictable relationships, which can lead to emergent properties. An inevitable consequence of considering social components as well as technical components when analysing a system (i.e, taking a socio-technical approach) is that these social components do not necessarily behave like the technical, people are not machines, paradoxically, with growing complexity and interdependence even the technical components can start to exhibit non-linear behaviour.

2) optimisations of either social or far more commonly the technical components tends to increase not only the quantity of unpredictable, “un-designed”, non-linear relationships, but those relationships that are actually injurious to the system's performance. Safety is a system property that high reliability of technical components is neither necessary nor sufficient for system safety. And, there is growing evidence that accidents in socio-technical systems usually have multiple causal factors, in the form of an inter-connected network of events, rather than a simple cause-effect chain.

Safety engineering techniques are traditionally designed based on an assumption that most accidents occur from the chance simultaneous occurrence of random events. However, system’s operation is not static. Rather than accidents being a chance occurrence of multiple independent events, they tend to involve a migration to a state of increasing risk over time (Rasmussen, 1997). The traditional techniques suffered from the limitation of assuming each accident as a static chain of events waiting to happen. It is necessary, therefore, to establish a systematic approach so that the trend of the propagation of safety risks, which can span multiple technical systems, human activities and organisational processes, can be systematically analysed in an integrated assessment.

In this paper, we adapt system dynamics and system archetypes from systems engineering, and propose a method to analyse the safety of socio-technical systems. The rest of paper is structured as follow. In section 2, we will brief review the approaches of safety assessment and the challenges to the safety of socio-technical systems. In section 3, we introduce the modelling technique used in the proposed model-based safety assessment and our proposed approach. Section 5 is about the case study.

2 Systems thinking in safety analysis

The heart of system safety analysis is hazard analysis, and it is essential in hazard analysis that causes of each identified hazard are thoroughly analysed by using techniques such as fault tree analysis (FTA). After the cause analysis, recommended solutions which can effectively reduce the risk of each hazard are often documented in the report of hazard analysis (e.g., hazard log). However, safety is a system property. Modern safety critical systems consist of many nonlinear, counterintuitive and dynamic “cause-and-consequence” relationships, especially when taking social subsystems into consideration. Sometimes it could be found that the solution to one hazard might have some side effects to the solutions of others, therefore the fundamental solution to the safety of the overall system could have been overlooked. Thus, it is necessary to introduce systems thinking into hazard analysis, more broadly system safety engineering. Since systems thinking is a framework for seeing interrelationships rather than individual pieces, for seeing patterns of change rather than static “snapshots”, it is reasonable to believe the solution to the safety of modern social-technical system comes from systems engineering.

The safety assessment can be seen as a process of:

1) to describe the system;
2) to identify hazards;
3) to analyse consequences of each hazard;
4) to analyse the causes of each hazard;
5) to evaluate risk;
6) to propose mitigation of risk; after all hazards have been analysed then
7) to analyse the residual risk; and
8) to document the results of whole safety assessment.

The process is shown in Fig 1.

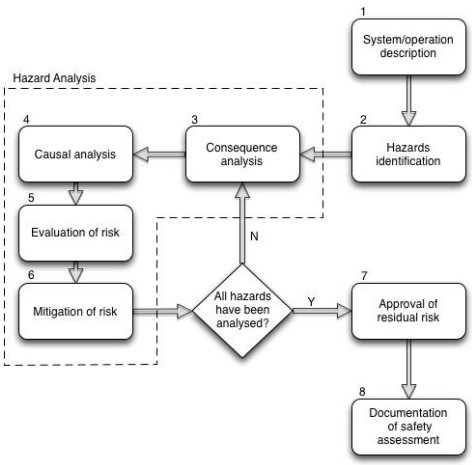

Fig. 1 Process of safety assessment

Hazard is a different concept with failure, actually it is much broader term; it is an existing or potential set of circumstances and actions that can transform an activity involving a hazardous condition into an accident. A hazard can be considered as a dormant/potential harm which is present in one form or another within the system or its environment.

Taking the hazard analysis of the track circuit as an example, a track circuit is a device mounted on the track-side to detect if a particular section of track is occupied by train. It feeds safety data to the train control system, usually automatic train control (ATC) system in the application of a metro system. Table 1 is a section of the hazard assessment of a track circuit.

In the table, the hazardous (undesirable) event is that a train has been lost in the ATC system, which actually means that the ATC system does not know the position of a train (more technically a section of tracks are physically occupied by a train but it says not in the ATC system). Because the ATC system does not know the position of the train, the speed of the following train would not be safely controlled. The worst scenario would be the following train collides into the back of the leading train, which may cause multiple fatalities/injures, or stoppage of service. The reasons for the "lost" can be identified that either due to either environmental interferences, or faults on track circuit device itself or data communication cable connected to the device.

During the analysis, safety engineers always ask themselves "does it currently (not) happen if something A happens?" or "how likely it will happen if something A happens?" The answers to these questions will help identifying the causes and consequences. However, it is hard to identify the causal relationships by answering those questions because a lot of dependencies in a social-technical system are not as simple as Boolean relationships.

Table 2 is a summary of the characteristics of the majority of dependencies in the different parts of a social-technical system. To help the identification of the causal dependencies in the system, questions like "does this happen if something else happen?", but also question "will this positively/negatively change the situation of something else?" will be asked more often. The traditional analytical techniques, for example FTA, are designed to deal with the Boolean relationships, and limited to analyse those complex and non-linear dependencies.

As summarised in Table 3, there is a need to have a "more" capable technique/approach for the hazard analysis. By label it "more" capable, we request the new approach should be able to capture the information necessary to the safety of a social-technical system, represent all the essential dependencies in the system in a clear manner, and then examine/identify the confliction/inadequate dependencies in the system model/models. In addition, the approach should base on systems thinking since it is a framework for seeing interrelationships rather than individual pieces, so that the approach is able to provide capability for balancing overall impacts to the system safety rather than the effect from individual measures.

3 Hybrid System Dynamics Safety Model

System dynamics (Maani, 2007) provides a framework for dealing with dynamic complexity, where cause and effect are not obviously related. The additional benefits from system dynamics are models of system dynamics are formal and can be "executed". The models and their simulations will help to capture complex dynamics of behaviours of a socio-technical system and to understand the safety concerns of overall system.

Inherited from the original system dynamics model, the extension will not be complicated. The only thing needed to anlayse safety of socio-technical systems (as listed in Table 3) is to append the capability to model the Boolean relationship.

The three basic elements of system dynamics model, shown in Fig. 2, are positive/reinforcing feedback, negative/balancing feedback, and delays. In order to have an ability to capture and analyse the Boolean dependencies in the technical system, which is the core of a social-technical system, the system dynamics model could be extended by adding symbols b/b+ and b- (b means Boolean relation).

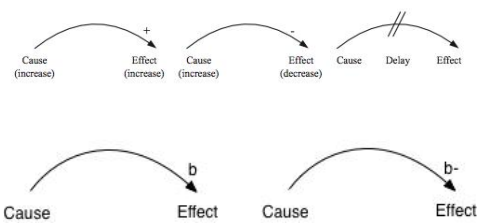

Fig. 2 Dependencies in hybrid system dynamics model

Similar to the elements in original system dynamic model, if two things have a "cause-and-effect" relationship, more precisely thing X is a sufficient condition for thing Y, they are connected by a curly arrow. If the appearance of one thing (the "cause") will result the emergence of the other thing (the "effect"), then the connection is indicated by "b" or "b+" at the head of arrow; And if the appearance of the cause will eliminate the existence of the "effect", then the connection is indicated by "b-" at the head of arrow.

4 Case study

The case study is to demonstrate how the hybrid system dynamics model can help the safety assessment of a tram system – the tram system at East Croydon station.

4.1 Overall system description

East Croydon station is one of 38 stops in the line of regional tram service, provided by Tramlink since May 2000. Trams approaching East Croydon tram stop from the east use a street-running section of double track. There are two running lines divide to serve three platforms at East Croydon. Platform 1 serves eastbound trams, platform 3 westbound trams, and platform 2 serves trams travelling in either direction depending on the operating mode set by the signalling system.

The operation of tram service at East Croydon station is a socio-technical system: a technical system, including the signalling system in the kernel; and operational rules and procedures with the signalling system in order to provide the service, including the maintenance from Bombardier and operation from Tram Operations Ltd (TOL).

Fig. 4 illustrates a part of signalling system at East Croydon station, which controls the tram operation on the westbound line. The westbound line divides at motorised facing points ECR06M, located 98 metres from the tram stop and east of Billington Hill road crossing. After these points the routes run parallel before diverging near the platforms.

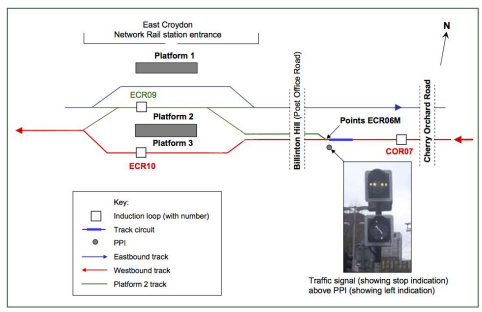

Fig. 3 Schematic diagram of East Croydon Signalling system (derived from (RAIB 2012))

In its operation, the signalling system first detects an approaching westbound tram when it passes over an induction loop (COR07), which is located in the road surface west of Cherry Orchard Road crossing, 35 metres in front of ECR06M points. The signalling system next

detects the tram, when it arrives in either platform 3 or platform 2, by induction loops located at the west end of the platforms (ECR10 and ECR09 respectively). The signalling system controls points ECR06M by sending a voltage pulse to the point controller requesting it to direct trams left towards platform 3, or right towards platform 2. And the route whether is set to the left or the right is displayed to the approaching tram by a points position indicator (PPI), which is mounted on the same post as the signal that authorises tram movements across the points.

Figure 5 shows the architecture of the point control system which controls the points ECR06M. The request (voltage pulse) sent from the signalling system is accepted by the point controller unless the track circuit (TC) or mass detector (MD) has responded to the presence of a tram in the immediate vicinity. But if a tram is crossing over the points, the point controller will have locked the points to prevent movement and the request is ignored. In the case if a second tram is detected by loop COR07 before the first tram has reached loop ECR10 (or ECR09) (which is located at the end of the platform), the signalling system will store the request to the point controller, and let the second tram wait in front of points by showing the traffic signal on the post of PPI. The stored request will be released when the first tram is detected by loop ECR10 (or ECR09).

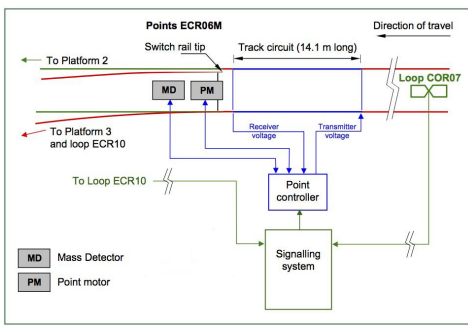

Fig. 4 Schematic diagram of Point control system (RAIB 2012)

Apart from the controls from the signalling system, the TOL also has operating instructions. It requests, first of all, tram has to be stopped on loops at platform; and secondly the following tram has to wait at the PPI until the PPI shows a route to an unoccupied platform, which can be either an empty platform or a platform where the previous tram has started to move away.

4.2 Hazard analysis

There is not enough space to describe the entire hazard analysis in this paper. In the section, we will discuss two typical hazards, "there is a movement of a points when a tram is crossing over it" and "a tram enters into a platform which has been occupied by another tram", in details to demonstrate the usage of proposed hybrid system dynamics model.

4.2.1 Hazard I: there is a movement of the points when a tram is crossing over it

After identifying the causes of the hazard, we find there will be three root factors, which can directly trigger the hazardous event happen. They are "TC fails to detect the tram", "PM is out of control", and "there is an abnormal behaviour of points controller". All these factors are marked with "*" in the hybrid system dynamics model, shown in Fig 5.

As been discussed that the tram system is a social-technical system that means apart from the technical system inside which is the signalling system, there are business systems of TOL (the tram operator) and Bombardier (maintenance) around the technical system. Therefore it is also important to identify the causal factors from these social systems during the analysis.

In the hybrid system dynamics model, these safety barriers and mitigations from social sub-systems can be added (in this case study, they are highlighted in red).

In order to make sure there is no critical causes unidentified, a fault tree analysis for this hazard had also been conducted too, shown in Figure 7. Referencing to the fault tree, it is clearly shown that the three single point failures (highlighted in red) have also been identified in the HSD model. In addition, we can argue that there is an implicit dependence between "a tram is crossing over but not detected" and "a tram slowly crosses the point". Because of the mechanism how a track circuit detects a tram, the slower the tram is moving on the track the easier the tram is detected, we can address in the model that the behaviours of driver may contribute the situation that the tram has not been detected although it is superficially a fault in the technical system. And an adequate in TOL safety management will help.

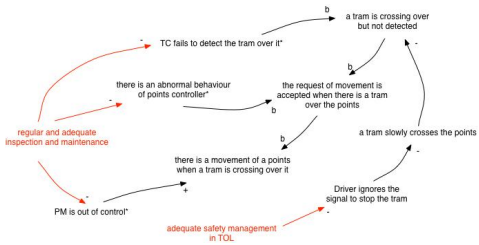

Fig. 5 Hybrid system dynamics model of Hazard I

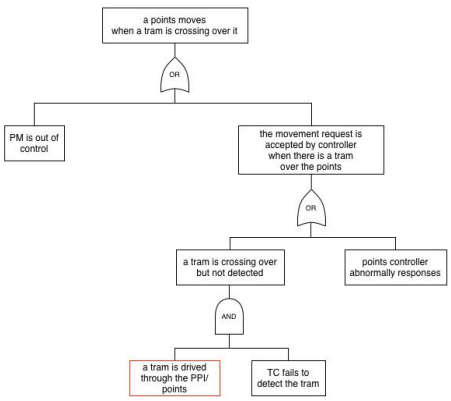

Fig. 6 Fault tree analysis of Hazard I

4.2.2 Hazard II: Tram enters into a platform which is occupied by another tram

Same as the analysis of previous hazard, the HSD model, in Fig. 7 (in appendix), shows that some faults in the technical system are the root causes, for example, the errors in the interlocking algorithm, faults of points and PPI display. Most importantly, during the analysis of social system, we identified that there is no fault in the technical system and driver followed the TOL's instruction but there still could be a hazardous event waiting for happen, in which scenario that the front tram takes long to arrive at platform so that the request of new route setting has been hold, and when the following tram arrives the PPI/points and the driver sees the front tram moving towards the end of platform then he drivers the tram into the route towards to the same platform. So there is a flow in the design of TOL's operating instructions in terms of system safety that allows the driver drives the tram through the points without waiting for the signal if he can see the front tram leaving. And because that behaviour is designed in the operating instructions, it cannot be eliminated by safety measurements from safety management system.

After the analysis based on hybrid SD model, we also conducted a FTA (in Fig. 7) to ensure there is nothing important missed in our analysis.

4.2.3 Discussion

Modern safety critical systems may consist of many nonlinear, counterintuitive and dynamic dependencies. Therefore, although hazards are identified and analysed individually, it should have a "seeing the forest through the trees" approach for the safety assessment. The hybrid SD model provides the capability to analyse the complex dependencies among different hazards. In this case study, based on the model (shown in Fig. 8), we found that these two hazards are implicitly interconnected. If the request of route setting is wrong, then the points may be requested to move so it is more likely that the points controller re-acts incorrectly because the points is an on-demand equipment. And in addition, if the signal and information on PPI are wrong, then it is more likely that driver will drive the tram through the point rather than waiting for the finish of the points' movement. The identification of these cause-and-effect relationships (highlighted in the model) between two hazards is important to the safety analysis because these relationships cannot be addressed in the fault tree analysis (see Figure 5 and Figure 6) so that there is a potential scenario that an error in the signalling system may propagate to points control system, and in some circumstance it emergences in a different form (e.g., the points control is out of control).

By applying the hybrid SD in the safety analysis, we can easily see the dependencies of these two hazards are interconnected: the factors of one can propagate through this dependency "map" to activate the other hazard or at least play an important role in the process of the evolution of the other hazard.

On Friday 17th February 2012, Tram 2538 was approaching the stop in the westbound direction. After observing that the PPI for points ECR06M was displaying the indication to platform 3, the driver applied power to take the tram over the points. The leading bogie of Tram 2538 was directed towards platform 3, but the points moved as the bogie was passing over. As a consequence of the points moving, the centre and trailing bogies derailed. The accident has been investigated and the findings were published in (RAIB, 2012). In this accident report, the direct cause of this accident has been

identified that the track circuit inside of the points ECR06M did not respond to Tram 2538, which is the reliability problem of the TC. In our analysis (Fig 8), it seems that is a single failure if the TC does not respond to the tram over the points because it is a normal event that the tram passes the point. Therefore, there are several safety mechanisms to prevent it happens, including activities from social subsystems, for example adequate inspections and maintenance. However, we also noticed in our analysis that the occurrence of the points' incorrect movement does not only relate to the reliability of the point's but also the frequency of the demands of points' movement, which can be a result of flaws in algorithm of interlocking systems or inadequate operating instructions. In this accident, these two, firstly the driver was allowed to drive the tram through the points without waiting for the signalling system; and secondly drivers' improper operating behaviours (shortly stop at the platform) had not been addressed in the safety management system, are all indirect causal factors, which cannot be easily identified in the fault tree analysis.

In general, the systems to be analysed become more and more complex, especially when taking its social elements into consideration. The dependencies or the cause-and-effect relationships among hazardous events cannot be understood as chains of directly related events. Therefore, a more powerful analytic technique is needed to assist to identify the reasons behind system's dynamic behaviours in order to operate the system safely in a systemic manner.

Table 1 Section of hazard analysis log

<table>
<tr><td colspan="5">Hazard: Spurious signals from track circuit</td></tr>
<tr><td>Causes</td><td>Safety barriers</td><td>Undesirable event</td><td>Potential consequence</td><td>Severity of consequence</td></tr>
<tr><td>Parasitic oscillations due to flaws in device design or improper installation</td><td>Testing before and after installation</td><td rowspan="7">A train is "lost" in the ATC system, i.e., ATC loses the tracking of a train due to improper information of track occupancy.</td><td rowspan="7">Train collision on the affected section of tracks</td><td>Multiple fatalities/injures</td></tr>
<tr><td rowspan="3">Environmental interferences</td><td>Electrical/Magnetic isolation</td><td rowspan="4">abnormal stoppage of service</td></tr>
<tr><td>Regular visual inspections</td></tr>
<tr><td>Automated inspections</td></tr>
<tr><td rowspan="2">Worn data cable</td><td>Regular visual inspections</td></tr>
<tr><td>Automated inspections</td></tr>
<tr><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td></tr>
</table>

Table 2 Requirements analysis for safety analysis of socio-technical systems

What is needed in the hazard analysis of a social-technical system	The capability of traditional techniques (FT, FMEA, WBG, BBN, etc.) can provide
To capture Boolean dependencies	Boolean dependencies can be modelled in the qualitative analysis by using traditional techniques.
To capture non-deterministic dependencies	Non-deterministic relationships can be modelled in quantitative analysis if the probability is known.
To capture complex interrelationship.	Information of complex interrelationship cannot be modelling by using traditional techniques.

Table 3 Dependencies in systems

System	Characteristics of the majority of dependencies
An engineering system, e.g., an electric locomotive	Boolean and nondeterministic dependencies. In the safety assessment of an engineering system, we always focus on the prerequisites of an event and their Boolean relationships.
A human-operated engineering system, e.g., the train driven by a driver.	Cognitive and adaptive dependencies. The safety assessment of these systems focuses on human factors and human decision-making process although it is difficult to understand the exact mental model of human operators at the moment of accident.
A "soft" system which consists of engineering system, human agents and a social institution (organisation), e.g., a train control system	Complex and non-linear dependencies. Safety engineering in social-technical system is about improving situations which are "problematical" [Checkland,1990], rather than "problem situations".

5. Conclusions

In the paper, it has been demonstrated by examples that the approach based on the hybrid system dynamic model provides such capability due to the hybrid system dynamic model allows both Boolean and non-linear dependencies to be presented in a single model so that the safety engineer can have a systemic view of how each individual causal factor effects the overall system.

The hybrid system dynamics approach is complementary to the traditional safety analysis.

Although the comparison to the fault tree analysis had been discussed in the case study, it is not for the purpose of discussing the proposed approach is prior than the traditional approaches. The real evaluation of an approach relies on vast applications of real world cast studies. Meanwhile, we are also working on the software tool which can assist the safety analysis of large-scale complex social-technical systems when the manual analysis is extremely difficult.

Acknowledgement

This work was supported by the Fundamental Research Funds for the Central Universities （Grant No. 2682014BR059）and the Opening Foundation of Gansu Provincial Key Laboratory of Traffic Information Engineering and Control （Grant No. 20161103）.

References

Leveson N. (2004). “Engineering a safer world: systems thinking applied to safety. ” MIT Press,USA.

RAIB (2012). Rail accident report: derailment of a tram at East Croydon 17 February 2012.

Rasmussen, Jens (1997). “Risk management in a dynamic society: A modelling problem.” Safety Science, 27(2-3): 183–213.

Maani, K. E. and R. Y. Cavana. (2007). “Systems Thinking, System Dynamics: Understanding Change and Complexity.” Aukland: Printice Hall.

Appendixes

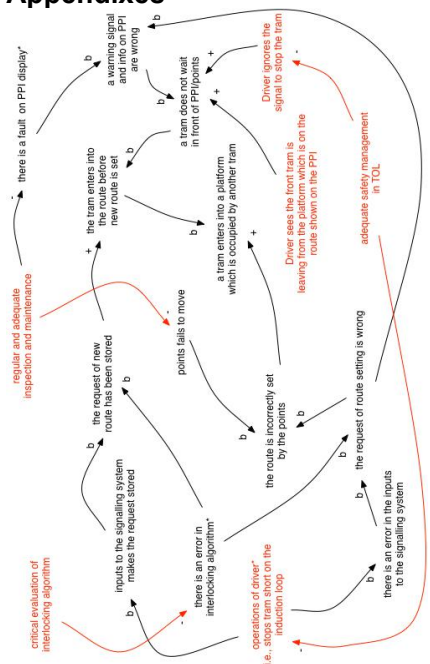

Fig. 7 Hybrid system dynamics model of Hazard II

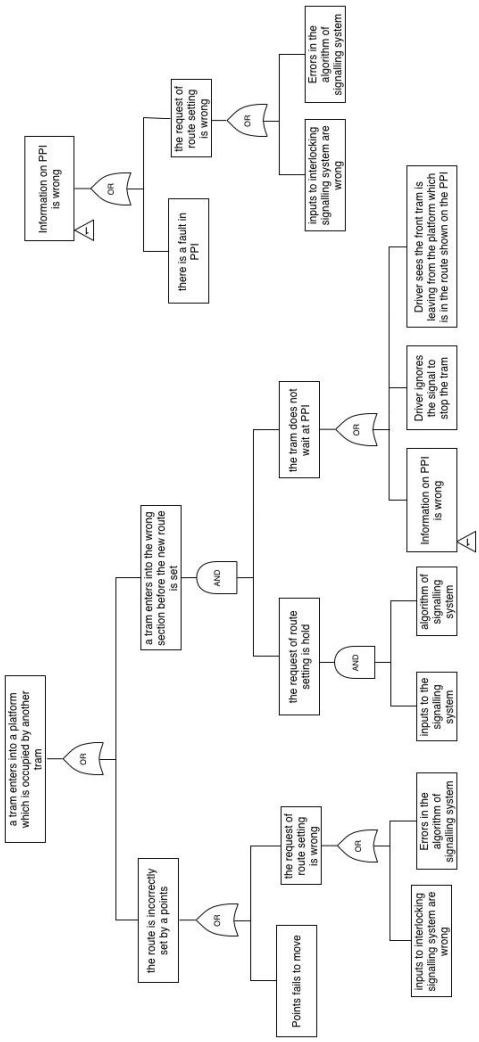

Fig. 8 Fault tree analysis of Hazard II