Timed Fault Tree Models of the China Yongwen Railway Accident

Yu Lu[1,*], Zhaoguang Peng[2,†], Alice Miller[1,‡], Tingdi Zhao[3,†] and Chris Johnson[1,‡]
[1] *School of Computing Science, University of Glasgow, Glasgow, United Kingdom*
[2] *China Ceprei Laboratory, Guangzhou, China*
[3] *School of Reliability and Systems Engineering, Beijing University of Aeronautics and Astronautics, Beijing, China*
[*] *y.lu.3@research.gla.ac.uk*
[†] *ghpeng@dse.buaa.edu.cn, ztd@buaa.edu.cn,* [‡] *{alice.miller, christopher.johnson}@glasgow.ac.uk*

***Abstract*—Safety is an essential requirement for railway transportation. There are many methods that have been developed to predict, prevent and mitigate accidents in this context. All of these methods have their own purpose and limitations. This paper presents a new useful analysis technique: timed fault tree analysis. This method extends traditional fault tree analysis with temporal events and fault characteristics. Timed Fault Trees (TFTs) can determine which faults need to be eliminated urgently, and it can also provide a safe time window to repair them. They can also be used to determine the time taken for railway maintenance requirements, and thereby improve maintenance efficiency, and reduce risks. In this paper, we present the features and functionality of a railway transportation system based on timed fault tree models. We demonstrate the applicability of our framework via a case study of the China Yongwen line railway accident.**

Keywords-railway transportation systems; fault tree analysis; risk analysis; timed fault trees

I. Introduction

System safety relies on robust safety design, good management, and efficient maintenance. System safety is an essential requirement of a railway transportation system. Primary risks include derailment, collision and fire to property and personnel [1]. Some of the key safety issues in railway transportation systems are discussed in [2].

Railway safety was recently highlighted in China. In 2011, two high-speed trains travelling on the Yongwen railway line collided on a viaduct in the suburbs of Wenzhou City, Zhejiang Province. In Figure 1, we show that a 16-car CRH1B EMU working train D3115 between Hangzhou and Fuzhou had apparently been brought to a stand by a lightning strike. As it was moving off around 20 minutes later, it was hit from the rear by Beijing-Fuzhou train D301, operated by a 16-car CRH2E. Six cars were derailed, of which four fell off the 20 metres high viaduct and 40 people were killed, at least 192 were injured.

In order to render railway systems as safe as possible, a large number of analysis techniques have been developed, such as hazard and operability study (HAZOP), failure mode and effect analysis (FMEA), fault tree analysis (FTA) [3], functional hazard analysis, and event tree analysis (ETA). FTA is an important logic and probabilistic technique, and is mostly used in system reliability and safety [4].

HAZOP is a structured and systematic examination of a planned or existing process to identify and evaluate risks. This technique is mainly used in chemical process systems, and is a qualitative technique that involves applying a set of descriptors to a number of parameters. FMEA is an effective analytical tool used to examine possible failure modes and to eliminate potential failure during system designs [5]. FMEA effectively depends on the members of the committee, and it is limited by their experience of previous failures, but also is unable to discover complex failure modes. ETA is a logical evaluative process that involves tracing forward in time or through a causal chain, whereas FTA is a deductive process. Although ETA allows one to identify the effect of a given event path on a system, it cannot pinpoint the specific event that leads to an accident.

FTA is a powerful diagnostic technique used to demonstrate the root causes of undesired events using logical and functional relationships among components, processes, and subsystems [6]. A fault tree (FT) is a model which logically and graphically represents the various combinations of possible events, either faulty or normal, that occur in a system and lead to unexpected events or states [7]. FTs can be used to identify the cause of undesired events [4], [8]. Faults can be due to hardware failure, software error, or human error.

Traditional FTA has been applied to various applications. These applications include a number of high hazard industries such as nuclear power [9], the oil industry [10], and traffic [2], as well as applications in mechanical engineering [11], [12]. In general, FTA is useful to analyse and predict system reliability and safety [13].

Traditional FTA involves events and gates, and employs Boolean algebra. Logic modelling is used to graphically represent relationships among basic events. FTA is usually carried out at two levels: a qualitative level in which a list of all possible combinations of events that lead to an event called the *Top Event* is determined (minimal cut sets), and a quantitative level in which the probability of the occurrence of the nodes in the tree can be calculated [9], [14].

Several methods have been proposed to improve FTA to solve specific problems. One of these involves the use of Binary Decision Diagrams (BDDs) [15], [16]. In this approach, a failure mode is represented using a Boolean

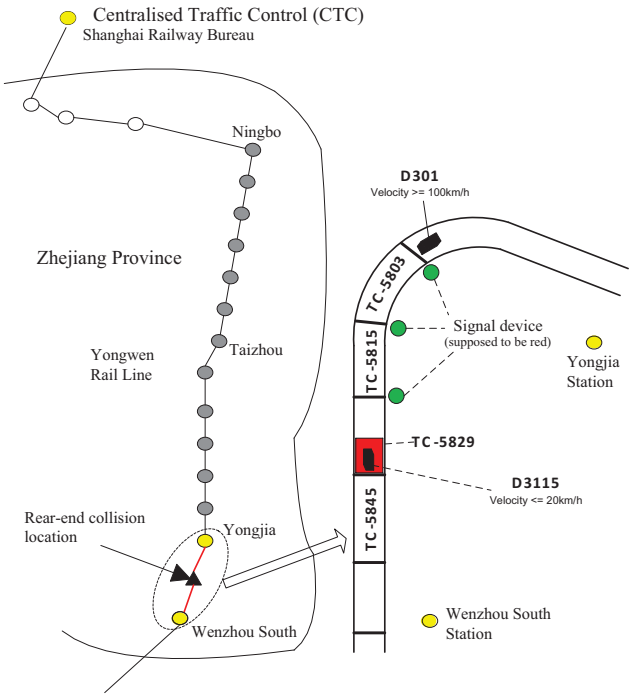

Figure 1. The Yongwen railway line and the accident.

equation, which can be manipulated mathematically. This approach overcomes some disadvantages of traditional FTA by enabling efficient and exact qualitative and quantitative analysis of fault trees [17]. However, the BDD approach does not involve direct analysis of a fault free, but of an alternative representation [18]. This can lead to problems (an error in the BBD representation may be hard to translate to the original context, for example, [18]).

In this paper, we present a case study of using a novel analysis technique, which is Timed Fault Trees (TFTs). The term "Timed Fault Tree" has already been employed in [19] in their future work for temporal fault trees. But the term in our context follows the style of time-dependent fault tree in [20]. The purpose of our TFTs is to analyse the relationship between safety and time in systems that are traditionally modelled using FTA. In this paper, the questions that we want to address, that are not amenable to analysis using FTA include: if two parts of the system require maintenance, which part should be repaired first? How long can a repair wait, so that a given hazard can be avoided?

This paper is organised as follows. First, we present the underlying railway system that will be analysed. Second, we introduce the TFT technique, and describe the analysis process using this technique. Then, we demonstrate the applicability of our technique by a case study of the China Yongwen line railway accident in Section IV. Finally, we conclude and propose directions for future research.

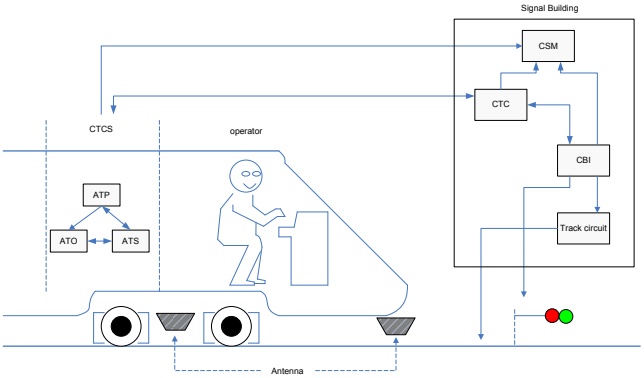

Figure 2. System composition.

II. Railway Transportation Systems

The signal system, which consists of a set of traffic controls and train operation controls, is one of the most important electrical and mechanical systems in the rail transportation system. It is directly related to operation safety, operation efficiency, and service quality. It should guarantee the safety of the passengers and trains, ensuring that the transportation is fast, frequent, and organised. Hazards discussed in this paper are mainly due to signal system failures.

China Railways High-speed (CRH) Electric Multiple Unit (EMU) signal system includes Chinese Train Control System (CTCS), Computer Based Interlocking system (CBI), Centralised Traffic Control System (CTC), and Centralised Signalling Monitoring system (CSM). The system composition is depicted in Figure 2, and can be explained as follows:

- CTCS is a control system that ensures the safe running of the trains. It includes three subsystems: Automatic Train Supervision (ATS), Automatic Train Protection (ATP), Automatic Train Operation (ATO).
- CBI is responsible for the safety interlocking relationship of the turnout, signal, and tracks. It receives command instructions from the ATS or operator, and sends out interlocking information to ATP or ATS.
- As the command centre, CTC is responsible for monitoring train running, tracking trains, adjusting trains' running plan and any temporary speed limit.
- Centralised Signalling Monitoring system (CSM) is responsible for monitoring all the above systems status in the signal system.

CTCS includes ATO, ATP, and ATS. Their roles are described as follows.

- ATP is responsible for the safe distance between trains, over speed protection, and door control, which includes trackside equipment, interlocking equipment, and on-board equipment. Ground-based ATP transmits information to trains, then the on-board ATP calculates and

provides control information to make the trains run under the speed limit. The train doors can only be opened if appropriate information is detected by ATP and the required conditions are met.

- ATS supervises train operation. It is in charge of the transition to automatic switching, scheduling the trains according to the train running plan and passenger traffic, selecting and maintaining routes, automatically or manually adjusting the stop and running time, and transferring command from the Operating Control Center (OCC) to the train. ATS includes the central computer and display equipment in OCC, control and recording equipment, field equipment (station, depot, and parking), and transmission channels.
- ATO is responsible for the automatic adjustment of train speed, traction and braking instructions, and stopping the train within a given accuracy. The ATO equipment includes the controller, receive/transmit antennas, signs coil and so on. ATO is useful for enhancing passenger comfort and reducing the labor intensity of the drivers. Functions of ATO include auto-piloting, automatic speed control, automatic parking, designated parking, and door control.

The relationship between the ATO, ATP, and ATS is described below. ATP is the heart of the safety of CTCS, and is essential for the security of train operation. ATS is a part of the top management and command center of the CTCS. ATO is responsible for the optimisation of the CTCS. A CTCS system relies on the coordination of the three subsystems.

ATO, which is under the supervision of the ATP, obtains the train's running instruction of ATS from ATP. ATO calculates the running speed according to the route status, and determines and executes the control command. After arriving at a station, ATO issues a door open command after the appropriate safety condition has been satisfied (as demonstrated by an ATP check). At the same time, ATO transfers train information to a ground communicator via the Positive Train Identification (PTI) system antenna, which it then sends to ATS. ATS determines a new assignment according to the available train information, and sends it back to ATO through the track circuit. When entering a new track section, ATO will receive new ground information so as to adjust the speed, and flexibly switch to ATO mode.

In order to facilitate the procedure described above, the signal system requires a coordinated set of control systems: ground control, on-board control, field control, and central control. This system is responsible for traffic control, operation adjustment, and automatic pilot. Our new technique, TFTs, is a valuable tool for assessing risks in this context. It will help to determine which faults require urgent attention, and to evaluate the time available to fix a fault before an accident will occur as a consequence of the fault. TFTs can then be used to construct an emergency plan.

III. Timed Fault Trees

In this section, we present formal notation that is relevant to analysis technique using timed fault trees (TFTs).

A. TFTs representation

TFTs are an extension of traditional FTs that follow the same top down approach but includes two additional time parameters. These allow us to discover *urgent* faults and a safe time window to repair them. Time parameters have been included in the definitions of events and gates. Events have two time parameters: the *duration time* and the *start time* of the event. The gate has one time parameter, namely *delay time*. The delay time is the time between an input event and a corresponding output. For example, at an AND gate there may be a delay between the receipt of the two inputs and the output of their sum.

Traditional solution of fault trees involves the determination of the so-called Minimal Cut Sets (MCSs). Cut sets are the unique combinations of component failures that can cause system failure. A cut set is said to be a minimal cut set if, when any basic event is removed from the set, the remaining events collectively are no longer a cut set [21].

B. TFTs notation

In this section, we define the syntax of TFTs. In all cases, capital letters refer to events, and a superscript denotes an event in a sequence (e.g., $A^{(n)}$). Lowercase letters denote duration time (of a fault, event, or hazard), and the duration of event A say is denoted a (etc.). Similarly, the duration of $A^{(n)}$ is denoted $a^{(n)}$.

A duration time a is assumed to belong to interval $[a_{min}, a_{max}]$. (Similarly, $a^{(n)} \in [a^{(n)}_{min}, a^{(n)}_{max}]$). The start time of an event is denoted using the associated lower case letter followed by s. So the start time of event A is denoted as, where $as \in [as_{min}, as_{max}]$. (Similarly, $as^{(n)} \in [as^{(n)}_{min}, as^{(n)}_{max}]$).

Note the difference between a and as: they denote the duration and start time of event A respectively. As an example, suppose that A is the event "applying brakes" and it takes between 15 and 50 seconds for the train to stop. In this case $a_{min} = 15$ and $as = 0$.

We use the superscript * to denote the actual time that an event occurs (i.e., a^* or $a^{(n)*}$). This value depends on the events below A (and $A^{(n)}$) in the fault tree. We use the term *actual time* to refer to this value, and assume that $a^* \in [a^*_{min}, a^*_{max}]$, and $a^{(n)*} \in [a^{(n)*}_{min}, a^{(n)*}_{max}]$.

Gates are denoted $G^{(1)}, G^{(2)}, ..., G^{(n)}$, and we say that gate $G^{(i)}$ has index i. If A is an event, and $G^{(i)}$ a gate, r_A and $r_{G^{(i)}}$ denote the transition rates associated with A and $G^{(i)}$ respectively. The average duration of event A (respectively gate $G^{(i)}$) is denoted $\overline{A}$ (and $\overline{G^{(i)}}$).

The time delay between receiving all inputs to a gate, and production of an output is g, where $g \in [g_{min}, g_{max}]$. $Ar(A)$ represents the arrive rate of the event from the MCS.

A higher $Ar(A)$ means that MCS spends less time between the occurrence of the basic event to the top event A. $N(t)$ represents the smallest unit of time t.

C. Analysis process

In this section we outline the TFTs analysis process. The full list of some properties of gates (AND, OR, XOR, Voting) that are relevant to TFTs can be found in an extended version of this paper [22]. In order to use the technique, the following steps should be followed.

1) Complete the fault tree, and find the MCS. This step is similar to that for traditional FTA.
2) Assign each event and gate a minimum and maximum duration and delay between inputs and outputs respectively.
3) Set the initial start time of the basic fault to 0.
4) From the bottom up, according to the rules of the TFT model, incrementally calculate the minimum and maximum actual time of each event.
5) Calculate the actual time of the hazard.
6) Analyse the chronological relationship between the hazard and the MCS, and calculate the urgent basic fault whose actual time is nearest to the hazard time.
7) Calculate the arrival rate of the hazard. Each MCS corresponds to an arrival rate of the hazard. Calculate each arrival rate, and sort arrival rates in ascending order. The arrival rate reflects the average risk of the basic fault. Thus, we get the average urgent basic fault.
8) Propose a solution to the hazard and use the TFT to prove that the hazard will not occur in the future.

The time of an event and the gate is expressed via two basic parameters: minimal time and maximal time. These values can be obtained from field statistics, experiments, and from values obtained using similar equipment. How much time we need to stop a train in the emergency situation? When we carry out the TFT method, we only need to know the minimal and the maximal time of events and gates.

It is, of course, of greater value to use TFT analysis to prevent accidents, and to produce emergency plans for hypothetical situations so that we are prepared for future disasters. However, we can only demonstrate the effectiveness of our approach by applying it to accidents that have occurred in the past. In the next section, we demonstrate our method by using it to analyse the China Yongwen railway accident.

IV. Case Study

Figure 3 shows a timed fault tree model representing a simple CRH EMU signal system in the China Yongwen rear-end collision. In a normal state, a train is no closer than a specified safe distance from another train. If a train detects that another train ahead has come to within that safe distance from it, its ATP will send a brake signal to the ATO, and the ATO will brake the train. When the accident occurred in 2011, a train failed to detect that another train had come within the safe distance and so the brake signal was not activated, resulting in a rear-end collision.

We can obtain the time values associated with the gate and events in Figure 3 from known values for similar equipment. For example, the maximum velocity a train can reach is 350 km/h in China, and the required safe distance is 6-8 km. Therefore, if the brake systems fail, there can be a crash in 64.7 seconds. For this reason, the minimum time value of $G^{(1)}$ is assigned to be 64.7 seconds. In China, it is required that a change in equipment state should become visible in the ATS central display within 1 second. Similarly, a command should be issued to the controlled system within 1 second.

Table I
Duration time of the gates.

Gate	Duration time (s)
$G^{(1)}$	[61.7, 90]
$G^{(2)}$	[0.1, 2]
$G^{(3)}$	[1, 4]
$G^{(4)}$	[0.5, 2]
$G^{(5)}$	[0.1, 1]

Table II
Duration time and actual time of the events.

Event	Duration time (s)	Actual time (s)
A	[0, 0.1]	[62, 114]
$B^{(1)}$	[0.1, 1]	[0.9, 24]
$B^{(2)}$	[1, 7]	[2.5, 21]
$B^{(3)}$	[0.1, 3]	[0.7, 10]
$B^{(4)}$	[0.5, 10]	[0.5, 10]
$B^{(5)}$	[1, 5]	[1, 5]
$B^{(6)}$	[0.1, 1]	[0.1, 1]
$B^{(7)}$	[0.1, 5]	[0.1, 5]
$B^{(8)}$	[0.1, 5]	[0.3, 7]
$B^{(9)}$	[0.1, 1]	[0.1, 1]
$B^{(10)}$	[0.1, 1]	[0.1, 1]

The times corresponding to each gate and event are shown in Tables I and II. In Table II, we also give the actual time for each event, obtained through the application of TFTs. So, we can calculate the minimum time between fault and hazard, which could help set the standard for maintenance. We obtain the MCS: $< B^{(4)}, B^{(7)} >, < B^{(4)}, ^{B}(6) >, < B^{(5)}, B^{(6)} >, < B^{(5)}, B^{(7)} >, < B^{(9)}, B^{(10)} >$. The time relationship between the MCS and the hazard is shown in Figure 4. The maximum actual time of $B^{(4)}$ is the closest to the time of the hazard. As a result, $B^{(4)}$ should be prevented with the greatest urgency.

Next, the transition rate is calculated based on the rules of TFTs. For example, as the smallest time unit is 0.1 seconds in this case, the duration time of $B^{(1)}$ is between 0.1 and 1 seconds. So, $N(b)^{i}_{min}$ is 1, and $N(b)^{i}_{max}$ is 10. According to Equations (1) and (3) (see Section 4.3), the average duration of event $B^{(1)}$ ($N(\overline{B^{(1)}})$) is 5. The transition rate of $B^{(1)}$ ($r_{B^{(1)}}$) is 0.2.

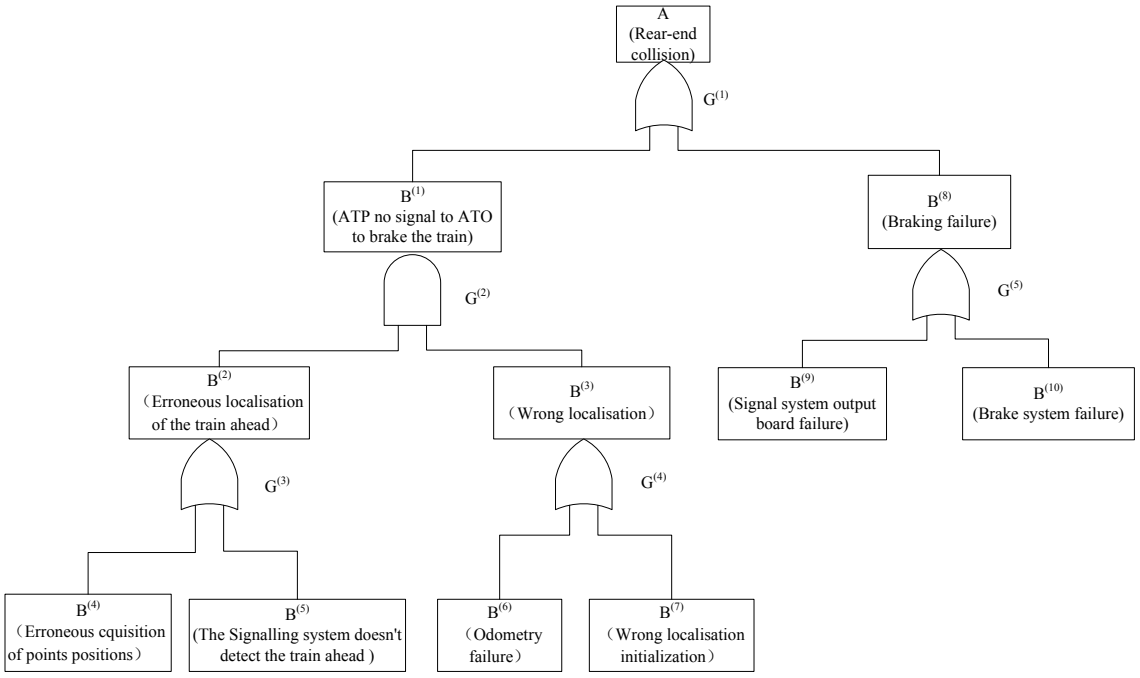

Figure 3. A fault tree representation of a CRH EMU in a rear-end collision.

The durations and rates of the events and gates are shown in Table III. According to the rules of TFTs, the arrival rate of A corresponding to each MCS is as shown in Table IV. The MCSs with minimum arrival rates are $< B^{(4)}, B^{(6)} >$ and $< B^{(4)}, B^{(7)} >$.

Table III
DURATIONS AND TRANSITION RATES OF EVENTS AND GATES.

Event and Gate	Duration time (s)	Transition rate
A	76	0.013
$B^{(1)}$	5	0.2
$B^{(2)}$	40	0.025
$B^{(3)}$	15	0.667
$B^{(4)}$	52	0.019
$B^{(5)}$	30	0.033
$B^{(6)}$	5	0.2
$B^{(7)}$	25	0.04
$B^{(8)}$	25	0.04
$B^{(9)}$	5	0.2
$B^{(10)}$	5	0.2
$G^{(1)}$	76	0.013
$G^{(2)}$	10	0.1
$G^{(3)}$	25	0.04
$G^{(4)}$	13	0.077
$G^{(5)}$	25	0.04

To illustrate the results shown in Table IV, we calculate MCS $< B^{(4)}, B^{(7)} >$. The actual times of event $B^{(4)}$ and $B^{(7)}$ are in the intervals $[0.5, 10]$ and $[0.1, 5]$ respectively. Events $B^{(4)}$ and $B^{(7)}$ refer to "erroneous acquisition of points positions" and "wrong localisation initialisation" respectively.

Table IV
THE ARRIVAL RATE OF EACH MCS.

Minimal Cut Sets	Arrival rate of A
$B^{(7)}, B^{(4)}$	$1/(2 * 10^8)$
$B^{(2)}$	$1/(2 * 10^8)$
$B^{(3)}$	$1/(1.1 * 10^8)$
$B^{(4)}$	$1/(1.1 * 10^8)$
$B^{(5)}$	$1/(4.8 * 10^8)$
$B^{(6)}$	$1/(4.8 * 10^8)$

The hazard (A) will occur if both events $B^{(4)}$ and $B^{(7)}$ occur. As we can see from Figure 3, if $B^{(4)}$ occurs, the hazard will take place after 52 seconds, and if $B^{(7)}$ occurs, the hazard will take place after 57 seconds. Therefore, it follows that the absolute safe times of maintenance of $B^{(4)}$ and $B^{(7)}$ are 52 seconds and 57 seconds respectively.

Suppose that event $B^{(7)}$ has occurred. If event $B^{(4)}$ subsequently occurs then the train will be in danger until the fault is eliminated. Hence, if fault $B^{(4)}$ is not eliminated in 52 seconds, some other effective measure will need to be taken to prevent an accident.

V. FUTURE WORK

The European Train Control System (ETCS) has 4 levels ranging from conventional operations up the use of satellite based augmentation systems within minimal trackside infrastructure. These higher levels of automation rely on the computation of Tolerable Hazard Rates (THRs) for any design. In other words, there is a probability of failure that

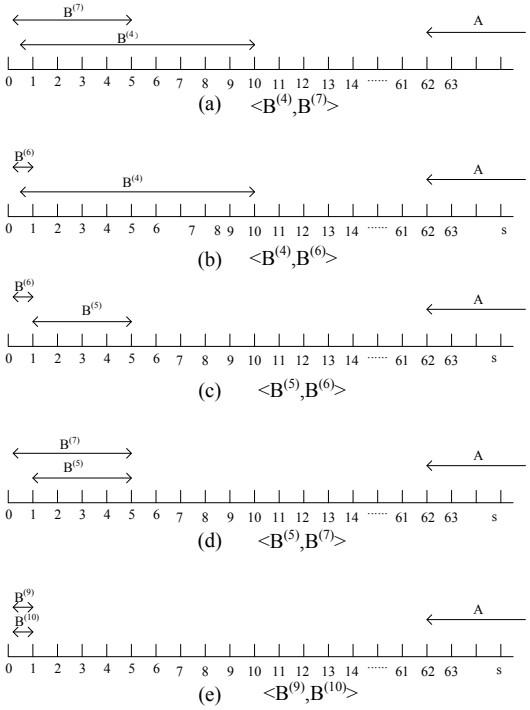

Figure 4. The actual time of MCS and hazard.

is used to assess the suitability of any implementation. We must show that any design or implementation can meet the tolerable rate of hazards. The THR in ETCS was calculated using conventional fault trees [23]. Much of our existing models from the Chinese context might be re-used to support the safety assessment of European infrastructures, especially where accidents are so rare that we must transfer lessons across national borders [24].

REFERENCES

[1] M. An, S. Huang, and C. J. Baker, "Railway risk assessment - the fuzzy reasoning approach and fuzzy analytic hierarchy process approaches: a case study of shunting at waterloo depot," *Proc. of the Inst. of Mech. Engineers, Part F: J. of Rail and Rapid Transit*, vol. 221, no. 3, pp. 365–383, 2007.

[2] E. Jafarian and M. A. Rezvani, "Application of fuzzy fault tree analysis for evaluation of railway safety risks: an evaluation of root causes for passenger train derailment," *Proc. of the Inst. of Mech. Engineers, Part F: J. of Rail and Rapid Transit*, vol. 226, no. 1, pp. 14–25, 2012.

[3] F. I. Khana and T. Husaina, "Risk Assessment and Safety Evaluation Using Probabilistic Fault Tree Analysis," *Human and Ecological Risk Assessment: An International Journal*, vol. 7, no. 7, pp. 1909–1927, 2001.

[4] W. Vesely, J. Dugan, J. Fragola, J. Minarick, and J. Railsback, *Fault Tree Handbook with Aerospace Applications*, 2002.

[5] N. Xiao, H.-Z. Huang, Y. Li, L. He, and T. Jin, "Multiple failure modes analysis and weighted risk priority number evaluation in FMEA," *Engineering Failure Analysis*, vol. 18, no. 4, pp. 1162–1170, 2011.

[6] V. R. Renjith, G. Madhu, V. L. G. Nayagam, and A. B. Bhasic, "Two-dimensional fuzzy fault tree analysis for chlorine release from a chlor-alkali industry using expert elicitation," *J. of Haz. Mat.*, vol. 183, no. 1-3, pp. 103–110, 2010.

[7] C. A. Ericson, *Hazard Analysis Techniques for System Safety*. Wiley, 2005.

[8] Y.-T. Tsai, "Applying a case-based reasoning method for fault diagnosis during maintenance," *Proc. of the Inst. of Mech. Engineers, Part C: J. of Mechanical Engineering Science*, vol. 223, no. 10, pp. 2431–2441, 2009.

[9] A. Volkanovski, M. Čepin, and B. Mavko, "Application of the fault tree analysis for assessment of power system reliability," *Reliability Engineering & System Safety*, vol. 94, no. 6, pp. 1116–1127, 2009.

[10] Y.-F. Wang, M. Xie, M. S. Habibullah, and K.-M. Ng, "Quantitative risk assessment through hybrid causal logic approach," *Proc. of the Inst. of Mech. Engineers, Part O: J. of Risk and Reliability*, vol. 225, no. 3, pp. 323–332, 2011.

[11] L. Meshkat, J. B. Dugan, and J. D. Andrews, "Dependability analysis of systems with on-demand and active failure modes, using dynamic fault trees," *IEEE Transactions on Reliability*, vol. 51, no. 2, pp. 240–251, 2002.

[12] Y. Dutuit, F. Innal, A. Rauzy, and J.-P. Signoret, "Probabilistic assessments in relationship with safety integrity levels by using fault trees," *Reliability Engineering & System Safety*, vol. 93, no. 12, pp. 1867–1876, 2008.

[13] H.-Z. Huang, X. Tong, and M. J. Zuo, "Posbist fault tree analysis of coherent systems," *Reliability Engineering & System Safety*, vol. 84, no. 2, pp. 141–148, 2004.

[14] G. Merle, J.-M. Roussel, J.-J. Lesage, and A. Bobbio, "Probabilistic algebraic analysis of fault trees with priority dynamic gates and repeated events," *IEEE Transactions on Reliability*, vol. 59, no. 1, pp. 250–261, 2010.

[15] Y. Mo, F. Zhong, H. Liu, Q. Yang, and G. Cui, "Efficient ordering heuristics in binary decision diagram-based fault tree analysis," *Quality and Reliability Engineering International*, vol. 29, no. 3, pp. 307–315, 2013.

[16] H.-Z. Huang, H. Zhang, and Y. Li, "A New Ordering Method of Basic Events in Fault Tree Analysis," *QREI*, vol. 28, no. 3, pp. 297–305, 2012.

[17] R. Remenyte-Prescott and J. D. Andrews, "An Efficient Real-time Method of Analysis for Non-coherent Fault Trees," *QERI*, vol. 25, no. 2, pp. 129–150, 2009.

[18] L. M. Bartlett and S. Du, "New Progressive Variable Ordering for Binary Decision Diagram Analysis of Fault Trees," *QREI*, vol. 21, no. 4, pp. 413–425, 2005.

[19] Z. Andrews, A. Didier, and A. Mota, "Report on Timed Fault Tree Analysis - Fault modelling," Tech. Rep., 2013.

[20] W. E. Vesely, "A time-dependent methodology for fault tree evaluation," *Nuclear Engineering and Design*, vol. 13, no. 2, pp. 337–360, 1970.

[21] D. Kececioglu, *Reliability Engineering Handbook: Volume 2*. DEStech Publications, 2002.

[22] Z. Peng, Y. Lu, A. Miller, C. W. Johnson, and T. Zhao, "Risk Assessment of Railway Transportation Systems using Timed Fault Trees," *QREI*.

[23] C. W. Johnson, "Innovation vs Safety: Hazard Analysis Techniques to Avoid Premature Commitment in the Early Stage Development of National Critical Infrastructures," in *Proc. of the 32nd International Systems Safety Conference*, 2014.

[24] C. W. Johnson, S. Reinartz, and M. Rebentisch, "Practical Insights for the Exchange of Lessons Learned in Accident Investigations across European Railways," in *Proceedings of the 32nd International Systems Safety Conference*, 2014.