Derivation of the safety requirements for control systems based on the interoperability property of the Maglev train

W. Zheng[1], J. R. Müeller[2] & K. Li[1]
[1]School of Electrical and Information Engineering,
Beijing Jiaotong University, China
[2]Institute for Traffic Safety and Automation Engineering,
Technical University of Braunschweig, Germany

Abstract

With the prospect of new and different Maglev train lines to be constructed, the interoperability properties of the Maglev train have become a new issue. The safety performance requirement of the Maglev control equipments for interoperability operation was derived based on the objectives of the crossing boundary between different lines and the corresponding procedures have been modelled with stochastic Petri nets. Firstly, the whole objectives of the crossing boundary of different Maglev lines were defined taking the operation efficiency and safety target into consideration. The train would cross the boundary without decreasing the speed. The operation efficiency and the safety property of the crossing procedure should be guaranteed. In addition, based on the interoperability objectives, the interoperability operation procedure of the Maglev train was specified and the Maglev control equipments used for the interoperability were designed. The control equipments were used to transmit the data between different control systems of different lines. Thirdly, the process of the train passing the boundary of different lines was modelled with the stochastic Petri nets based on the different operation stage of the train. Finally, by means of the simulation of the model, the safety performance requirements of the Maglev control systems were derived based on the defined crossing success rate.
Keywords: interoperability, Maglev train, Petri nets, modelling.

1   Introduction

The Maglev train is one of the new vehicles and it is still in the stage of research and development. In the near future, the new operation of the Maglev train lines will be built and it is necessary that the different lines should be linked to the operation network to improve the flexibility and efficiency. Based on this, the same Maglev train should be able to operate in different lines, and this is called the "interoperability" of the Maglev train in China.

   "Interoperability" means that different lines equipped with different control systems exist and are interlinked together. The train should be able to cross the boundary of different lines, meeting the safety requirements and be efficient. With regard to interoperability research, the Europe Union drew up several documents to define and explain the requirements. Document [1] specifies the safety requirements and document [2] describes the performance requirement. In China, the interoperability research is also undertaken in the laboratory of universities and commercial operation lines. However, there has been no research up to now about the interoperability of the Maglev train.

   In order to guarantee that one Maglev train can cross the boundary of different lines, the crossing process and changed data flow should be specified and analyzed, and all the factors influencing the crossing success rate should be identified so that it can be used as a guideline for the interoperability specification design.

   In this paper, the research is mainly focused on one of the interoperability properties, the ability of crossing boundary of different lines, and the corresponding system design approach is presented. The crossing process of the Maglev train is modelled with Petri nets and the relationship between the crossing boundary success rate and the system equipments dependability is analyzed quantitatively.

2   The objectives of the crossing boundary and system design

The objectives of the crossing boundary of different lines for the Maglev train are the basis of the system design and analysis.

2.1 Objectives

The objectives are described as follows:
   1) The action of crossing boundary of different lines could be proposed by the former system. The target system makes the decision of accepting or rejecting the train based on its own operation conditions.
   2) If the train is allowed to enter into the new line, the train should be able to cross the boundary with the original speed by the way of "stepping" style and it shall be able to operate in the new track based on the diagram.
   3) During the process of passing the boundary, if the train's speed exceeds the limitation, the former and target systems should be able to cooperate to guarantee the safety of the train.

A: Triggering point of crossing boundary； B: Triggering point of stepping；
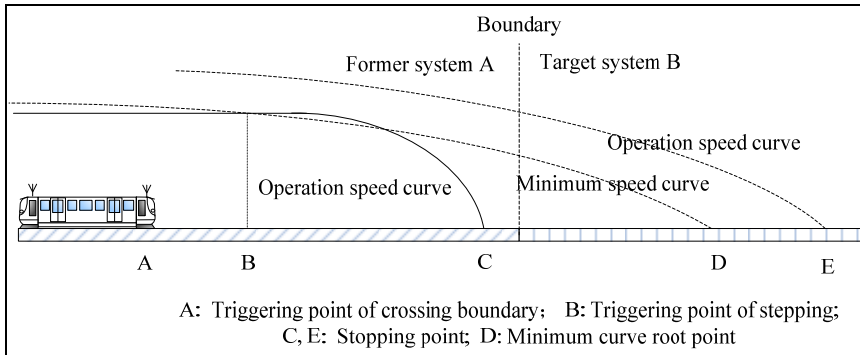C, E: Stopping point； D: Minimum curve root point

Figure 1:   The schematic diagram of the crossing boundary process.

4) During the process of passing the boundary, if any of the components fail, the two control systems of two lines should guarantee that the train stops at a specified point.

2.2 The process of crossing the boundary of different lines

The schematic diagram of a crossing boundary is shown in Fig. 1.

1) As shown in Fig.1, A is the crossing triggering point. When the train reaches this point, CCS-A will transfer the necessary data to CCS-B, such as the information of the train and the demand of the route. The information of the train consists of the train identification, its weight and its length, etc. The route request consists of the track data and segment data, etc. After receiving the route request from CCS-A, CCS-B will reply to CCS-A and inform the DSC-B to set the rout in system B for the train.

2) After the CCS-A has changed the necessary data with CCS-B, the train will execute the step action in point B. DSC-B will send the route data to DSC-A at this point. If the current speed in the operation speed curve for stopping point C is beyond the speed in the minimum speed curve for the next stopping point E, the train will be stepped to E point and it should operation under the operation speed curve of point E.

2.3 Control system design

Based on the process of crossing the boundary, it is clear that the new communication net should be designed to enable the data to be changed between the different control systems for different lines.

The control system of Maglev train is composed of the CCS (Centralized Control System), the DCS (Decentralized Control System) and the VCS (Vehicle Control System). The DCS is composed of the DCC (Decentralized Control Computer), the DSC (Decentralized Safety Computer), the DPS (Decentralized Propulsion Shut-off) and the DSM (Decentralized Switch Module). The main part of the VCS is the VSC (Vehicle Safety Computer）. The structure of the

control system is shown in Fig.1. Wu [3] specified the functions of each component in the control system.

The CCS is connected with the DCS by a control core network and the different components of DCS are interlinked with the safety protection network. Since the control systems of different lines have to exchange the data, it is necessary to add the communication systems between the control systems. As shown in Fig. 2, A-net and B-net are the designed communication systems for the crossing.

The function of A-net is to guarantee the communication between CCS-A and CCS-B. If A-net fails before the train arrives at B point in Fig.1, the crossing action will fail. During the time of train running from B point to the place of the boundary, B-net should be intact so that the DSC-A and DSC-B can communicate with each other all the time so that the train can cross the boundary safely. If B-net fails during this period, the crossing action will also fails.
Based on the process of crossing the boundary, it is obvious that the dependability property of the A-net and B-net has close relationship with the success rate of crossing boundary.

3   Petri net model of the crossing boundary process

As one of the modelling languages, Petri nets has been applied widely in the modelling and performance analysis of traffic control, mechanical engineering, software engineering, medicine and chemistry fields. David and Didier [4] described how the Petri nets can be used in the application of industry engineering. Zheng et al. [5] and Zheng [6] used Petri net to model the level crossing and the computer interlocking and analyze the safety performance of the control system. German [7] presented the basic elements of the Petri nets and Lin [8] specified the performance analysis principle and approach of the stochastic Petri net.

Based on the crossing boundary procedure as shown in Fig. 2, the Petri net model of the crossing process is described in Fig. 3.
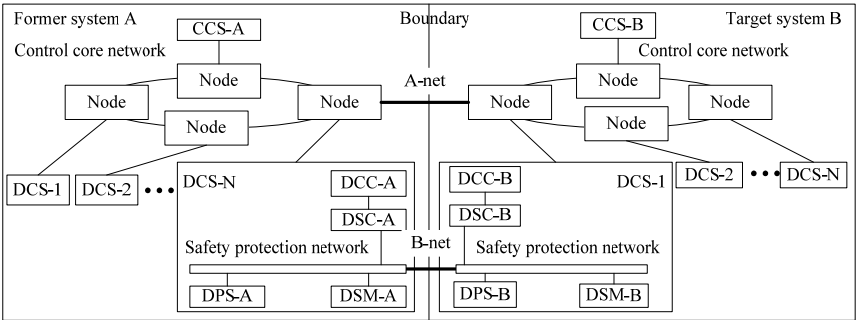

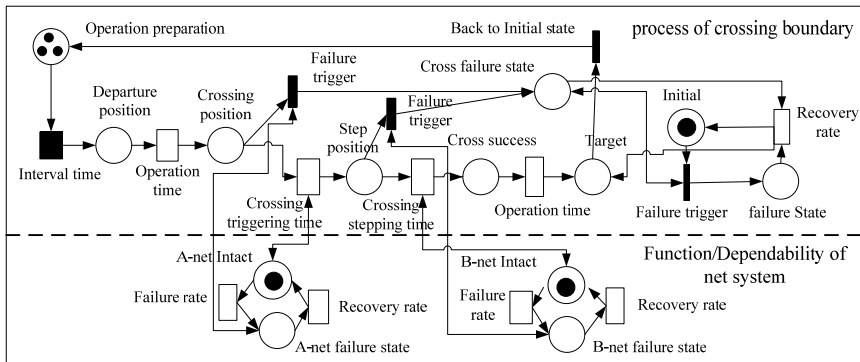Figure 2:   The frameworks of the former system and the target system.

Figure 3:   Petri net model of crossing boundary process.

Slovák et al. [9] introduced the hierarchical modelling approach firstly. Based on this approach for system dependability analysis, two views of the procedure of crossing boundary of the train can be modelled: one is the crossing process of the Maglev train including the failure process and the other is the function and dependability property of the control system.

1) The modelling of crossing boundary process: the state of the Maglev train is composed of places "Operation preparation", "Departure position", "Crossing position", "Step position", "Cross success", "Target" and "Cross failure state". The place "Crossing position" and "Step position" means the point A and point B of Fig.1. About the transition, the "Interval time" is a deterministic one because the headway of the train is fixed. The transitions "operation time", "Crossing triggering time" and "Crossing step time" are defined to be exponential and their parameters mean the corresponding operation time of the train.

2) The modelling of the failure of crossing boundary: the state of a failure process is composed of the place "Initial" and "failure state". The parameters of the transition "recovery rate" represent the recovering time in case of the crossing failure.

3) The modelling of function and dependability of A-net and B-net: for A-net and B-net, the state is both composed of two places "Intact" and "Failure state". The transitions between these two places are exponential and the parameters of the transitions mean the failure rate and recovery rate respectively. The place "Intact" also can act as the function place. The place "A-net intact" is in charge of the function of crossing triggering process and it play its role by a testing arc connected to the transition "Crossing triggering time". The place "B-net" is in charge of the function of stepping process and it is also linked to the place "Crossing step time" with a testing arc.

4   Simulation analysis

The TimeNET4.0 for Windows is a tool for edition and simulation of Petri net models [10]. To the model shown in Fig. 3, based on the assumed necessary

parameters, the expected average marking time of the place "failure state" can be obtained by simulation. Then it is divided by the "recovery rate" and the result will be the failure rate of crossing boundary.

The parameters in the model are assumed as follows: headway of the Maglev train: 0.5 hour; the whole operation time: 2 hours; the average crossing triggering time: 0.5 minutes; the average stepping time: four minutes; the average recovery time of crossing failure: 2 hours.

Simulation results are shown in Fig. 4 and Fig. 5.

As presented in Fig. 4, the failure rate will decreased with the higher dependability of the A-net and B-net.
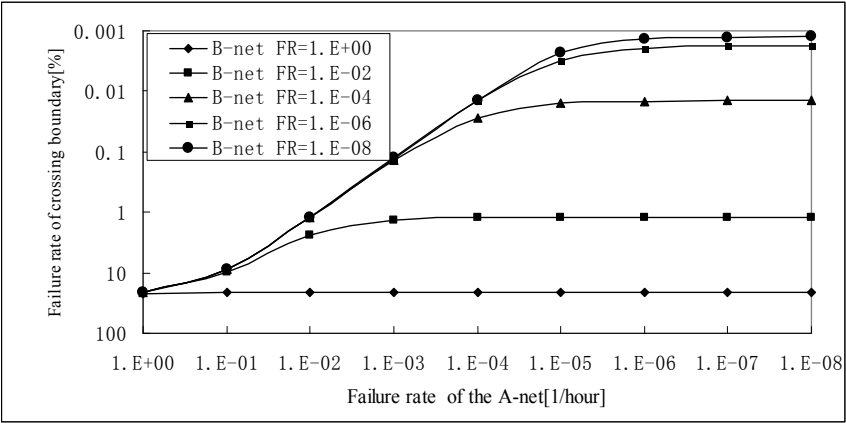

Figure 4: The relationship between the crossing failure rate and the dependability of the control systems.
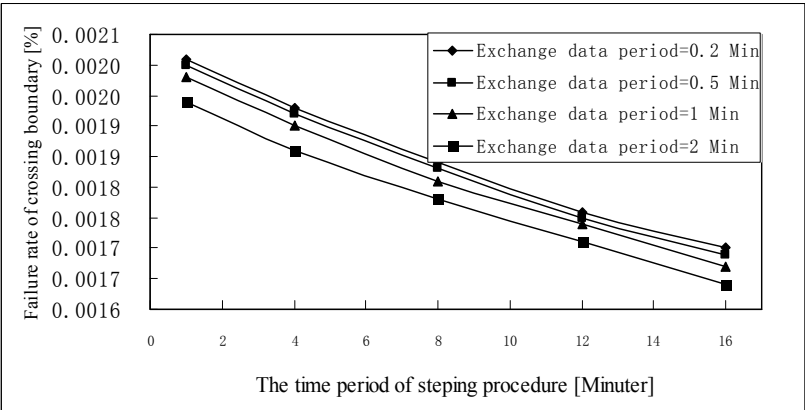

Figure 5: The relationship between the failure rate of the crossing boundary and the triggering and stepping time.

It is assumed that the headway of the train is 30 minutes and every operation process is composed of one action of crossing boundary. Then in one year, the whole time of crossing boundary for the trains is 17520. If only one time failure of crossing boundary is allowed in one year, then the failure rate should at most be $5.7 \times E$-5. From Fig.4, it can be derived that in order to meet this target, the failure rate of net-A and net-B should be lower than $1.0 \times E$-6 per hour.

In Fig.5, it is assumed that the failure rate of the A-net and B-net is $1.0 \times E$-6 per hour, and it is clear that if the triggering time and stepping time of the train are relatively longer, the failure rate of crossing boundary will be decreased slightly.

5   Conclusion

Based on the interoperability objectives and safety requirements, the functions and the structures of the control systems for the crossing boundary of different Maglev train lines were designed. By the results of simulation of the model, the dependability requirements of the added control systems could be identified based on the defined target of success rate of crossing boundary. The triggering time and stepping time of the train have little effect to the failure rate of crossing. The quantitative analysis of the crossing process can be used as the guideline for the formulation of the interoperability specification.

References

[1]   Safety Requirements for the Technical Interoperability of ETCS in Levels 1&2, ERTMS/ETCS-Class 1, SUBSET-091, 2009.
[2]   Performance Requirements for Interoperability, ERTMS/ETCS-Class 1, SUBSET-041, 2005.
[3]   Wu, X.M., *Maglev Train*. Shanghai Science and Technology Press: Shanghai, pp. 98-134, 2003.
[4]   David, V. & Didier, R. B., MORM-A Petri net based model for assessing OH&S risks in industrial processes: modelling qualitative aspects. *Risk Analysis*, **24(6),** pp. 1719-1735, 2005.
[5]   Zheng, W., Müller, J. R., Slovák, R. & Schnieder, R., Estimation of traffic risk of passive level crossing based on stochastic Petri net models and social economic data，*Proc. of the 3rd Int. Conf. on Transport Simulation*, Queensland, Australia, pp. 35-38, 2008.
[6]   Zheng W., Modeling and hazard analysis of railway station protection system based on stochastic Petri nets, *Proc. of the 8th Int. Conf. on Reliability, Maintainability and Safety*, Chengdu, China, pp. 493-496, 2009.
[7]   German, R. *Performance Analysis of Communication Systems – Modelling with Non-Markovian Stochastic Petri Nets*, John Wiley & Sons: Chichester, pp. 36-57, 2000.
[8]   Lin C., *Stochastic Petri Nets and System Performance Evaluation,* Tsinghua University press: Beijing, pp, 19-27, 2005.

[9]   Slovák, R., May J. & Schnieder E., PROFUND modeling for holistic risk and availability analysis by means of stochastic Petri nets applied to a level crossing Control System. *Proc. of Formal Methods for Railway Operation and Control Systems,* L'Harmattan: Budapest, pp.221-232, 2003.

[10]   TimeNET. www.pdv.cs.tu-berlin.de/~timenet/