Study on Model based Hazard Identification for the Hyperloop System

Datian Zhou
School of Electronic Information Engineering
Beijing Jiaotong University
Beijing, China
dtzhou@bjtu.edu.cn

Ali Hessami
VEGA Systems
London, United Kingdom
hessami@vegaglobalsystems.com

Wei Xin
School of Electronic Information Engineering
Beijing Jiaotong University
Beijing, China
13120286@bjtu.edu.cn

Han Wang
APSYS
Airbus group
Beijing, China
han.wang@airbus.com

***Abstract*—The Hyperloop system is a novel conceptual system aimed to provide a high speed public transportation service in the future, featured with a reduced-pressure tube in which pressurized capsules ride on a cushion of air that is driven by a combination of linear induction motors and air compressors. The project of developing Hyperloop is based on the** crowd-**funding-sourcing mode, which is dramatically different to the traditional way. Identifying the hazard of the Hyperloop system would be helpful to the publics' acceptance of the safety from the concept stage. If all the hazards were dealt properly, Hyperloop could be more realizable than ever. From system safety research's point, it is definitely a good opportunity to carry out different safety analysis and hazard identification methods to verify the effectiveness. With the predefined method of the model based HAZOP, a team work to identify the hazards of the Hyperloop system is carried out to verify the effectiveness.**

Keywords-Model based HAZOP; inter-model constraint; the Hyperloop system

I. INTRODUCTION

The Hyperloop system draws lots of attention from both the enthused supporters and the serious critics. The former group believe that the Hyperloop system could be a fifth form of public transportation alongside trains, planes, automobiles and boats. Currently, this conceptual system is at the very early stage of about ten years period of evolution predicted by the original inventor. However, the fantastic idea coupled with an attractive developing mode of crowd-funding-sourcing has attracted one hundred engineers from some traditional company such as Boeing, NASA and Airbus, to dedicate their own spare time to move the concept forward [1].

The most interesting point is that the Hyperloop is a hot topic not only to the enthusiasts, but also to the critics. The most obvious criticism is about whether it will work technically. One of the hurdles is dealing with the temperature of air compression that the heat of compression is always underestimated by engineers [2]. There's also an economic risk. It is claimed that materializing the Hyperloop in California will cost $6 billion about one tenth as much as building a corresponding traditional high speed railway. Some emeritus scholars comment that a big issue is getting enough capital together to demonstrate and build untested technology [3]. From a design standpoint, another challenge is how to integrate Hyperloop stations into the urban environment so people can travel to and from them quickly without waiting before boarding and take off like they do at airports [4].

In theory, it is commonly believed that the project, if it could be said, of building the Hyperloop system is full of risks, including management risks, economic risks, technical feasibility risks and legal risks etc. Actually, a public transportation service provider or equipment supplier should considerate the necessity of how well to deal with the safety risks no matter when the system is delivered. Additionally, the Hyperloop system should not just be demonstrated as a feasible solution but should be demonstrably safe to the public with an acceptable safety analysis. The highest uncertainty is how to find the crucial hazards systematically for the Hyperloop system and the related activities. Making sound hazard identification could help to setup the hazard log which is fundamental to making sound decisions on how to address priority hazards in the log. In practice, there are several kinds of hazard identification methods could be used in the different stages of a V life-cycle in different domain fields, including Preliminary Hazard Analysis, Subsystem Hazard Analysis, System Hazard Analysis, Operating and Support Hazard Analysis, Health Hazard Assessment, Fault Tree Analysis, Event Tree Analysis, Failure Mode and Effects Analysis, Fault Hazard Analysis, Functional Hazard Analysis, Sneak Circuit Analysis, Petri Net Analysis, Markov Analysis, Barrier Analysis, Hazard and Operability Analysis, Cause-Consequence Analysis, Common Cause Failure Analysis, Management Oversight Risk Tree Analysis, etc [5].

Considering the issues in terms of the completeness and coverage of hazard identification, the work inherent in developing and assessing the hazard models from the informal specifications, the method named Model based

HAZOP is selected to carry out the project of hazard identification for the Hyperloop system, after an effective and successful experience of using to identify the hazard for CTCS-3 (Chinese Train Control System level 3) funded by then MOR (Ministry of Railway) in China [9].

Coinciding with the benefit of the hazard identification to the Hyperloop system, the open sourcing of this idiosyncratic obligation could give the safety related practitioners to check and improve the methods and make them more scientifically credible. Usually, the hazard log of a commercial or on service system is highly confidential, which could not be accessible freely. Moreover there is very little opportunity to make a sufficient argument and assessment. So it is very usual a safety analysis method to be easily and commonly critiqued as being credibly scientific [7]. The crowd-funding and open-sourcing development is more accessible than the traditional methods and believed to release more detailed design information to the public. Anyone interested with the topic could obtain the same material to make an examination between a pair of different hazard identification methods. Additionally a pair of researchers could make a cross-examination of a given method's effectiveness independent to individual factors.

For ease of specifying the Hyperloop system, the meta-notations were defined explicitly prior to the project. A team accomplished the work packages of modelling the Hyperloop Alpha and identifying the hazards on schedule. With the one hundred forty three person-weeks, the outcome of thirty five models and one hundred twelve hazards identified is achieved. The effectiveness of the model based hazard identification for the Hyperloop system was verified successfully.

II. Method of model based hazard identification

The selected method of model based HAZOP includes REM (Reference Model), STM (State transition Model), FHM (Functional hierarchical Model) and SEM (Sequence Model).

A. Modeling aspects

For the convenience of modelling train control system, several of notations are used. Principally, most of notations were created before. Some are common for each kind of model. Others are only used in a specific model.

1) REM

There are five notations that can be used in REM. First one is the boundary, shown as Fig.1.

Figure 1. The boundary notation

The boundary is using to identify whether a component is belongs and an interface is connected from the outside to the system to be analysed. Then, the component looks like to rectangle, shown as Fig.2.

Figure 2. The component notation

The Component is representing a part combining the system. It can also be regarded as subsystem. For the convenience of defining the inter-model constraints later, the component is abbreviated as N-REM-COM. The interface is used to define a connection between a subsystem and somewhere outside the system, shown as Fig.3. An interface could be single input, single output and dual-directive input-output.

Figure 3. The interface notation

If an interface has just a logical definition, it would be FIS (Functional Interface Specification) interface. And if an interface is needed to be defined in both logically and electronically, it would be FFFIS (Form Fit Functional Interface Specification) interface. The last notation of REM is the note, which is also a common notation to FHM, STM and SEM, shown as Fig.4.

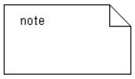

Figure 4. The note notation

The note notation is very important and necessary to record the information of the author and some other critical awareness which can't be addressed anywhere.

2) STM

STM is used to describe the system functions from the outside viewpoint, which are not offered by any of subsystem independently. There is a hierarchy of STMs for a given system. The surface level system functions can be grouped by several states in a STM. The start state notation is a filled cycle, shown as Fig.5.

Figure 5. The start state notation

The start state is default in a STM, and represents the initial state of the system which indicates that the system will provide some system functions after transiting from the start state. There should be an exclusive start state in a STM. Another default state is the end state, which is a filled circle inside a hollow circle, shown as Fig.6.

Figure 6. The end state notation

The end state represents the finishing of the system's work, which indicates that the system will not provide any more system functions. The next one is specific state notation, whose shape is like a round rectangle divided by a bar, shown as Fig.7.

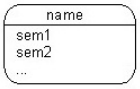

Figure 7. The specific state notation

It could be named by the modeler. To a specific state, it could be bundled with some system functions to show that these system functions can only be provided in the specific state, shown as Fig.8. For the convenience of defining the inter-model constraints later, the system function bundled with a specific state is abbreviated by N-STM-STATE_NAME-SEMi, i can be any number from 1 to N. N means there are N system functions bundled with the specific state named STATE_NAME. There could be several specific states in a STM, except the start state and the end state. The transition notation is used to connect one state and another state or itself, shown as Fig.8.

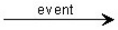

Figure 8. The event guard transition notation

The transition should connect two states. Its name can be specific by the modeler.

3) FHM

To a given system, there could be several FHMs usually. FHM builds a function tree from top level to low level representing the construction of a subsystem's function, which can only be analyzed effectively in a detailed level as low as reasonably practicable. The component is the only top level notation in a FHM. The component represents a subsystem defined in the system's REM, shown as Fig.9.

Figure 9. The function notation

For the convenience of defining the inter-model constraints later, the component is referenced by N-FHM-COMP_NAME. The detailed function notation represents a function nested in a component, shown as Fig.9. A component can consist of more than one detailed function. A detailed function can also be realised by more than one detailed function.

For the convenience of defining the inter-model constraints later, the detailed function is abbreviated referenced by N-FHM-FUNC_NAME. A detailed function belonging to a component can be connected by a connector called the composite notation, shown as Fig.10.

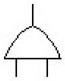

Figure 10. The composite notation

A component or a detailed function can be realised by any number of detailed functions or other detailed functions as a designer wants.

A FHM tree could be build in any level as the analyzer needs.

4) SEM

SEM is used to describe how the subsystems involved cooperate together to achieve a system function defined in the system's STM. Usually a system could have several SEMs. For the convenience of defining the inter-model constraints later, the SEM is referenced by N-SEM-SEM_NAME. The component notation is shaped like a rectangle, shown as Fig.11.

Figure 11. The component notation

For the convenience of defining the inter-model constraints later, the component is referenced by N-SEM-COMP. The components notation represents a subsystem defined in the system's REM. The component contributes detailed functions to a macro system function. The behavior could include forwarding or exchanging control/information. That falls into three categories. The first category/type is the control notation representing that the sender requires the receiver conduct some control functions by sending the control command shown as Fig.12.

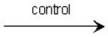

Figure 12. The control notation

The second type is the data notation representing that the receiver uses the data to do some calculations, shown as Fig.13.

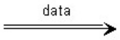

Figure 13. The data notation

The last type is the status notation representing that a receiver is informed the status of a sender, shown as Fig.14.

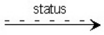

Figure 14. The status notation

Besides the three kinds of exchange, a component conducting something is defined by the activity notation, which is shaped like a hollow bar represented vertically, shown as Fig.15. For the convenience of defining the inter-model constraints lately, the activity is referenced by N-SEM-COMP_NAME-ACTIVITY.

Figure 15. The activity notation

The activity notation represents that a component is conducting an activity, which is defined in the component's FHM. The destination or source component is represented by the delegate notation, which is like a dash line, shown as Fig.16.

Figure 16. The representative notation

The delegate notation should connect to a component. From the side of the delegate connecting point with a component to another side, it represents the chronology of time sequence.

5) *Inter-models constraints*

The multiple-model method has many advantages over the single model method. Firstly, the multiple-model can provide more useful representations of the system and information. Different experts have different perspectives about the system in their minds. Sometimes it is really difficult to reach agreement, because they are thinking from different viewpoints. It's not cost-effective to put too much effort into this kind of opinion based process. Secondly, the multiple-model can represent the system's static and dynamic characteristic. Some models can easily describe the static system, such as the structure. Others have the advantage of showing the dynamic interactions among the different subsystems. Thirdly, each model of the multiple-model method has fewer notations than a single sophisticated model, so that it could represent a system as explicitly and easily understanding as possible.

However the multiple-model has some drawbacks which must be overcome to make sure the model based HAZOP generates value. The key point is about the isolation. Each model of the multiple-model method is not necessarily accessible to others or can be readily comprehended. Without the necessary connections, a person can hardly visualise the system models comprehensively. Beside, the further point is that the isolated multiple-model suite creates a potential for possible conflict. Some contents in different independent models could be cause conflict that runs the risk of making the HAZOP nonsensical. Moreover, the multiple independent models are incomplete representation of the system by themselves and need to be considered in combination.

The proposed inter-model constraints include the rules connecting four pairs of models, REM versus FHM, STM versus SEM, REM versus SEM, FHM versus SEM, shown in Fig.17.

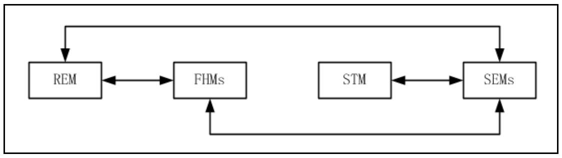

Figure 17. The four types of inter-model constraints

B. *Models of the Hyperloop system*

Totally, there are thirty five models being made for specifying the Hyperloop. The modeled Hyperloop system has nine subsystems, shown in Fig.18.

According to model the STM, the system is bundled to twelve states, including Standby state, Air pressure Transfer state, Contact Operation state and Suspend Operation state, etc, shown in Fig.19.

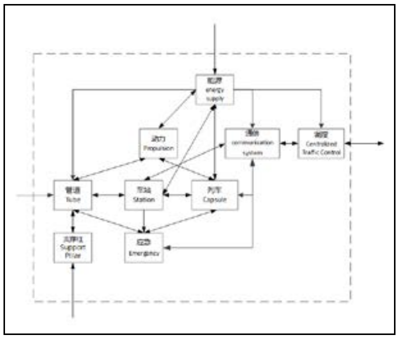

Figure 18. REM of the Hyperloop system

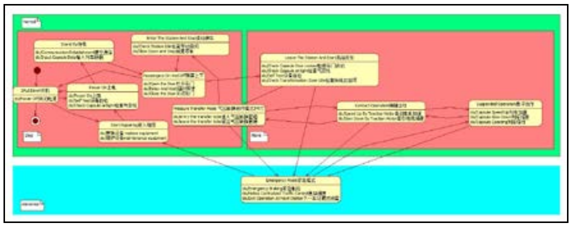

Figure 19. STM of the Hyperloop system

Nine subsystems were modeled for FHMs. The composite of Energy subsystem includs energy storing, power supplying for propulsion system, charging for the onboard batteries, power supply for vaccum pumps, power supplying of Solar energy and mixure power supply control, etc, shown in Fig.20.

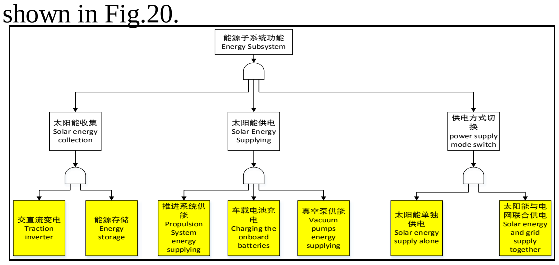

Figure 20. The FHM of Energy subsystem

Fig.21 is modeling a scenario of a capsule departing a station and entering the tube. Some information should be exchanged between the station and the tube to make the air pressure kept at a proper level.

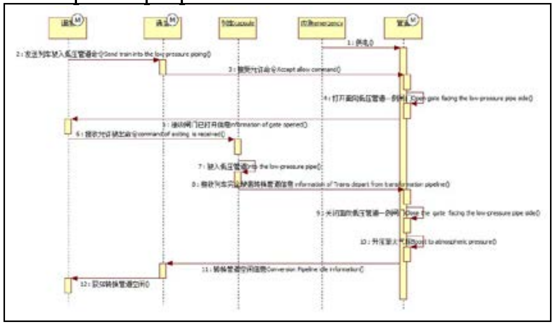
列车capsule
应急emergency
1 : 供电()
2 : 发送列车驶入低压管道命令(Send train into the low pressure piping()
3 : 接受允许命令(Accept allow command()
4 : 打开面向低压管道一侧闸门(Open gate facing the low-pressure pipe side()
5 : 接收闸门已打开信息(information of gate opened()
6 : 接收允许驶出命令(command of exiting is received()
7 : 驶入低压管道(into the low-pressure pipe()
8 : 接收列车完全驶离转换管道信息(information of Trains depart from transformation pipeline()
9 : 关闭面向低压管道一侧闸门(Close the gate facing the low-pressure pipe side()
10 : 升压至大气压(boost to atmospheric pressure()
11 : 转换管道空闲信息(Conversion Pipeline idle information()
12 : 获知转换管道空闲()

Figure 21. One of SEMs of the Hyperloop system

C. *Hazard identification*

Once a multi-model representation of the system under study is produced, the hazard identification can be performed according to the process in Fig.22.

- 1) From a model, selecting an element to be examined by HAZOP study
- 2) Choosing one of nine guide words to be considered with the selected element
- 3) Combining the guideword with the selected element to generate an abnormal scenario representing the deviation context according to the design intent
- 4) Agreeing with the experts whether the abnormal scenario is a credible hazard.

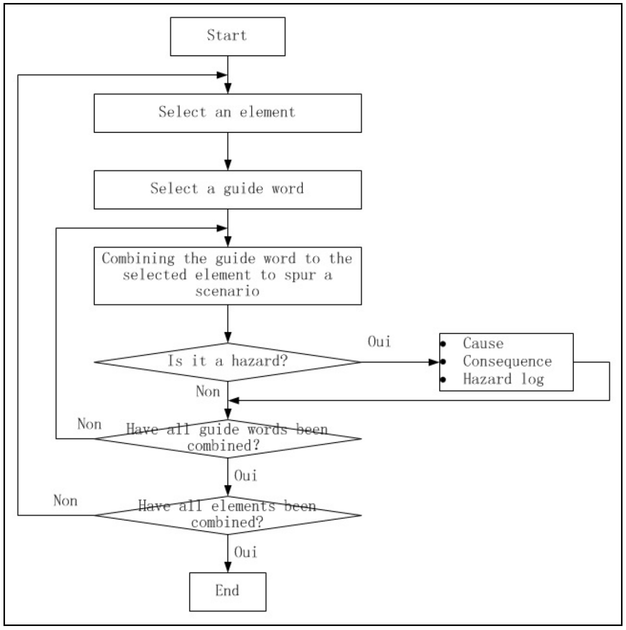
Start
Select an element
Select a guide word
Combining the guide word to the selected element to spur a scenario
Is it a hazard?
Oui
Cause
Consequence
Hazard log
Non
Non
Have all guide words been combined?
Oui
Non
Have all elements been combined?
Oui
End

Figure 22. The procedure of hazard identification

- 5) If it is regarded as a hazard, causes and consequences should be found and noted. Otherwise, the item is ignored. Then go to the step 2) to choose another guide word from unselected ones. Nevertheless, there is no guide word has yet been chosen.
- 6) For a given element, if all the guide words have been used, go to the step 1) to choose another element of the model.
- 7) If all the candidate of the elements has already been analyzed, end the process.

There is some information to be logged for a recognized hazard, including the model name in the blank of reference, the unique identity number of hazard, the unique element identity number of an element, date, initial condition, hazard description, causes, consequences, guide words etc.

Totally, one hundred twelve hazards were identified and recorded in the hazard log. It is easy to trace a hazard from the log domain to the model domain. A sample of hazard scenario of "Stopping operation" is shown in Table I.

TABLE I. THE HAZARD OF STOPPING OPERATION

Record No: HyperLoopHazard-004		**Data: 2015-1-9**		**Exposed Group:**	
Referenced model		Stopping operation		***Passenger***	√
				Neighbor	
				Worker	√
Type of Exchange		***DATA***		√	
		CONTROL			
		OTHER(describe)			
GUIDE WORDS					
NO	√	***AS WELL AS***		***IN ERROR***	√
MORE		***PART OF***		***EARLIER***	
LESS		***REVERSE***		***LATER***	√
HAZARD	For the case that the capsule failed in the middle of the tube, the Centralized Traffic Control fail to give an alarm, neglect the failed capsule, may cause passengers suffocation, or collide with the subsequent capsule, or death of passengers.				

CAUSES	*1*	Failed capsule Centralized Traffic Control communication outage;
		Alarm device failed;			

	2	The computers in Centralized Traffic Control have logic error;			
	3	The communication latency between failed capsule and Centralized Traffic Control is so big.			
CONSEQUENCES	*1*	A capsule failed but CTC failed to give an alarm;			
	2	Give a wrong alarm in normal state;			
	3	Alarm is not timely, making the time failed train stranded in tube is too long.			

III. MODELS AND HAZARDS OF THE HYPERLOOP SYSTEM

A team directed by a senior graduate student including twelve graduate students has undertaken the model based HAZOP for the Hyperloop system in part time mode. The task was scheduled to take ten weeks to accomplish the work regarding to the specification of Hyperloop Alpha [28]. The real time taken was about 10 percent more than the original plan.

There were five sessions held to discuss the issues related to modelling. For the hazard identification, the team made 35 models including one REM, one STM, nine FHMs and twenty four SEMs. The document of modelling is available at www.rstrc.org/jforum/posts/downloadAttach/2789.page in Chinese and English languages.

Another following nine sessions focused on HAZOP, and identified 112 hazards. The document is available at www.rstrc.org/jforum/posts/downloadAttach/2779.page.

IV. CONCLUSION AND FUTURE WORKS

Identifying the hazard for the Hyperloop system is beneficial to both the engineers dedicated on the conceptual future transportation and the system safety professionals. An updated hazard log could make the Hyperloop system more open and trustworthy than ever and easy to be accepted by the public. A predefined method of model based HAZOP is proven effective to be used to identify the hazard of the Hyperloop system.

The crowd-funding-sourcing mode provides a new thinking to verify the effectiveness of the method of hazard identification. A web based benchmark is worth developing to make more and more open system critical system be more realized than ever.

ACKNOWLEDGMENT

This work is supported by the State Key Laboratory of Rail Traffic Control and Safety (Contract No. RCS2014K009), Beijing Jiaotong University.

I appreciate the opportunity to cooperate with the team directed by Mr. Wei Xin and all the members. It is a really impressive experience to discuss the issues of modelling, hazard identification and the other interesting ideas. The novel idea of multiple model approach and inter-model constraints checking for Model based HAZOP are original from Professor Ali Hessami during the unforgettable and pleasurable three weeks' procedure in 2012 summer. The hard and interesting nostalgia and the spiritual HAZOP sessions are often recalled in my mind. It is common believed that the PCDP (Personal Competence Develop Plan) really has a genuine magic to each member of our team.

REFERENCES

[1] http://www.extremetech.com/extreme/196232-elon-musks-speed-of-sound-hyperloop-is-actually-being-built

[2] http://www.usatoday.com/story/money/cars/2013/08/13/hyperloop-elon-musk-tesla-space-x/2646969/

[3] http://www.technologyreview.com/view/518076/experts-raise-doubts-over-elon-musks-hyperloop-dream/

[4] http://www.dailybreeze.com/technology/20141201/hyperloop-ucla-graduate-students-explore-feasibility-of-high-speed-tube-transportation-system

[5] Ericson C A. Hazard analysis techniques for system safety[M]. John Wiley & Sons, 2005.

[6] IEC 61882:2001 Hazard and operability studies (HAZOP studies) - Application guide

[7] B. J. Tyler,"HAZOP study training from the 1970s to today". Process Safety and Environmental Protection, vol. 90, no. 5, pp. 419-423, 2012.

[8] Juraj Labovsky, Zuzana Svandova, Jozef Markos, Ludovıt Jelemensky, "Model-based HAZOP study of a real MTBE plan". Journal of Loss Prevention in the process industry, vol.20, pp. 230-237

[9] Study on Model based HAZOP for Train Control System, Zhou Datian, Ali Hessami, Bu Bing, Yao Xiaofei, Zhang Lu, Huang Caihong, FORMS/FORMAT 2014, Braunschweig, Gemany, 316-324

[10] Formalization of Train Control system Scenario, Zhou Datian, Lv Jidong, Yuan Lei, Li Kaicheng, Tang Tao, FORMS/FORMAT 2012, Braunschweig, Germany, 61-71

[11] S. N. Xiao, G. W.Yang, X. M. Shang, et al,"Research on Two Ends Energy-Absorbing Structure of High-Speed Railway Passenger Car Body", Journal of Advanced Materials Research, vol. 544, pp. 61-66, 2012.

[12] R.Squillante, F.Junqueira, P. E.Miyagi,"Development of control systems for safety instrumented systems", Latin America Transactions, IEEE (Revista IEEE America Latina), vol. 9, no. 4, pp. 451-457, 2011.

[13] C. A.Ericson,"Hazard analysis techniques for system safety", Wiley. com, 2005.

[14] International Electrotechnical Commission,"IEC 61882".Hazard and Operability Studies,(HAZOP Studies)—Application Guide, 2001

[15] ShigenGao,HairongDong,YaoChen,BinNing, GuanrongChen,XiaoxiaYang,"Approximation-based robust adaptive automatic traincontrol:an approach for actuator saturation", IEEE Transactions on Intelligent Transportation Systems, Volume14,Issue4,pp:1733-1742,2013.

[16] Mekki A, Ghazel M, Toguyeni A,"Validation of a New Functional Design of Automatic Protection Systems at Level Crossings with Model-Checking Techniques",IEEE Transactions onIntelligent Transportation Systems, vol. 13, no. 2, pp. 714-723, 2012.

[17] D. C.Karnopp, D. L. Margolis, R. C. Rosenberg,"System Dynamics: Modeling, Simulation, and Control of Mechatronic Systems", Wiley. com, 2012.

[18] S.Schreiber, T.Schmidberger, A.Fay, "UML-based safety analysis of distributed automation systems", Emerging Technologies and Factory Automation, 2007. ETFA. IEEE Conference on,pp. 1069-1075, 2007.

[19] J.Liu, T.Tang, L.Zhao,"Functional Safety Analysis Method for CTCS Level 3 Based on Hybrid Automata", Object/Component/Service-Oriented Real-Time Distributed Computing Workshops (ISORCW), 2012 15th IEEE International Symposium on,pp. 7-12, 2012.

[20] Y. Liu, T. Tang, K. Li, et al,"Fault Model-Based Safety Test Method and Application for CTCS-3 Train Control System",International Conference on Computer, Networks and Communication Engineering (ICCNCE 2013). Atlantis Press, 2013.

[21] X.Yang, X.Li, Z.Gao, "A Cooperative Scheduling Model for Timetable Optimization in Subway Systems". IEEE Transactions on Intelligent Transportation Systems,vol. 14, no. 1, pp. 438-447, 2013.

[22] M.Blaha, J.Rumbaugh,"Object-oriented modeling and design with UML", Upper Saddle River: Pearson Education, 2005.

[23] H.Malgouyres, G.Motet,"A UML model consistency verification approach based on meta-modeling formalization", Proceedings of the 2006 ACM symposium on Applied computing. ACM, pp.1804-1809, 2006.

[24] M.Wimmer, A.Schauerhuber, and G.Kappel, "A survey on UML-based aspect-oriented design modeling", ACM Computing Surveys (CSUR), vol. 43, no.4 , pp. 1-33, 2011.

[25] A. G. Hessami, "Risk management: a systems paradigm", Systems Engineering, vol. 2, no. 3, pp. 156-167, 2011

[26] http://www.spacex.com/sites/spacex/files/hyperloop_alpha-20130812.pdf