TELKOMNIKA, Vol. 11, No. 10, October 2013, pp. 6034 ~ 6041
ISSN: 2302-4046

Petri Net-based Analysis of the Safety Communication Protocol

Liu Hongjie*, Chen Lijie, Ning Bin
State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing, China
Beijing Jiaotong University, 01051688537
*Corresponding author, e-mail: 07111002@bjtu.edu.cn

Abstract

There is a few research in area of safety-critical system, therefore the study of performance analyzing method of the protocol has important practical significance for transportation engineering. This paper first briefly introduces the execution procedure of safety communication protocol, then explores the application of Petri net to establish the model of the protocol, including the process of state transition and corresponding timer which record the time, then obtains related performance data such as maintainability and failure probability, which users usually pay most attention to, with different probability of time delay and no fault in channel by simulation. Finally this paper finds that how the probability of time delay and no fault in channel could influent the maintainability and failure probability through data process with theory of probability and mathematical statistic, this could provide a certain reference for development of safety communication protocol.

Keywords*: safety communication protocol, Petri net, theory of possibility, mathematical statistics*

1. Introduction

The wireless communication system is always with potential safety threats, such as deletion, insertion, or delay, which could not satisfy the safety-critical requirement of train control system. Therefore, it is necessary to add a safety-related transmission system upon wireless communication system [1]. At present during development of safety communication protocol, there were many people analyzed performance of the protocol by test directly, but there were fewer studies about analyzing method for the protocol.

The need to apply formal or computer-aided methods to analyze the safety of safety-critical system has long been recognized [2-6]. This is especially important for train control system due to the large number of subsystems and the complexity of the function and its dynamic behavior, for instance, [7] for automatic train operation (ATO), or [8] for automatic train supervision (ATS). [9] describes a methodology to verify and test the safety properties of communication protocols for railway signaling in Korea. Unified Modeling Language state chart is proposed to verify the safety properties of the safety communication protocol of the European Train Control System [10].

In this situation, this paper presents Petri net due to its function of rigorous mathematic description, establishes state transition models to reflect the logic of the protocol, and models with time delay or lost packet to reflect the environment of the protocol, then simulated related performance data such as maintainability and failure probability, and finally finds how the lost packet and time delay could influent the maintainability and failure probability through data process with theory of probability and mathematical statistic. In the future, this study will have important practical significance for development of a safety communication protocol in train control system.

2. Function of Safety Communication Protocol

Because the safety of wireless communication system could not fulfill the requirements of train control system, safety communication protocol is proposed to be added as safety-related transmission system. Therefore, it is necessary to display the main function of the protocol, which manages the safety connection, including establishment, maintaining, and release of

Received April 26, 2013; Revised July 11, 2013; Accepted July 22, 2013

connection. Performance analysis is one important step to give certainty about satisfaction of a required property [11]. The safety communication protocol in informal method may have fault, which may cause fatal defection. Therefore, Petri net can be considered as a formal approach for protocol verification [12].

Figure 1 shows the state transition diagram of sender and receiver. Take sender for example, the initial state is IDLE, it will transfer to WAIT once it receives Sa-CONNECT.request, meanwhile sending RFC to receiver, setting Timeout_ACK as 0, and setting X, the serial number of sender, as a random value. The safety state will transfer to DATA from WAIT once it receives ACK from receiver and X is the same as Y, the serial number of receiver, meanwhile sending Sa-CONNECTION.confirm, setting Timeout_DATA as 0, and setting X plus 1. If it does not receive ACK when the state is WAIT, and the value of Timeout_ACK is no more than 4, the state will remain to be WAIT, meanwhile Timeout_ACK will be plus 1. If the value of Timeout_ACK is 5, the state will transfer to HALT from WAIT. When the state is DATA, it will remain to be DATA once it receives Sa-DATA.request and the value of Timeout_DATA is lower than 5, meanwhile sending DATA to receiver, setting Timeout_DATA and X plus 1. If the value of Timeout_DATA is 5, the state will transfer to HALT from DATA. Whatever the state is, as long as it receives Sa-DISCONNECTION.indication, it will transfer to IDLE. The meanings of the state and information are explained in [13] in detail.

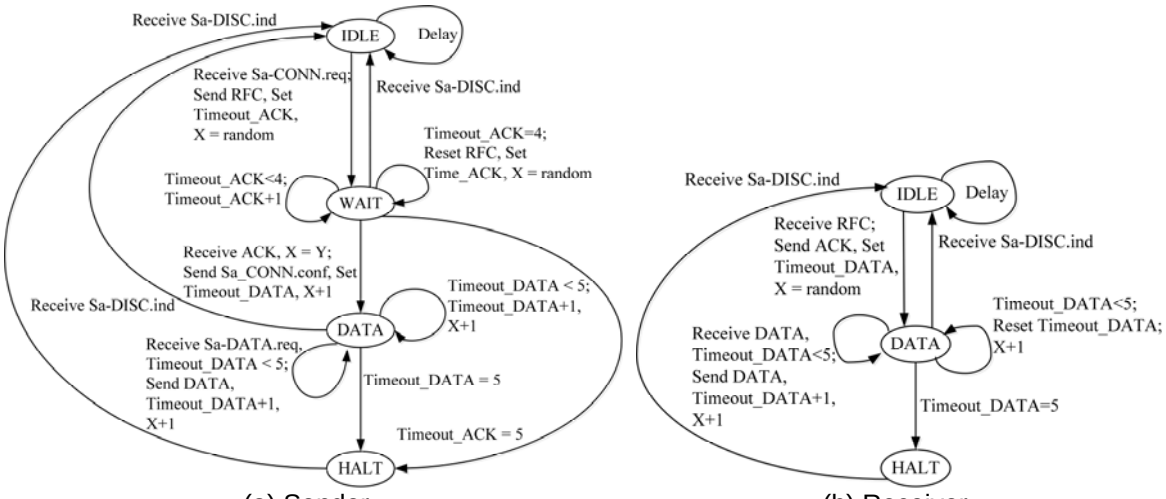


Figure 1. Safety state transition diagram of sender and receiver

Applying these above function, we could establish the function model of safety communication protocol, and obtain related data through simulation.

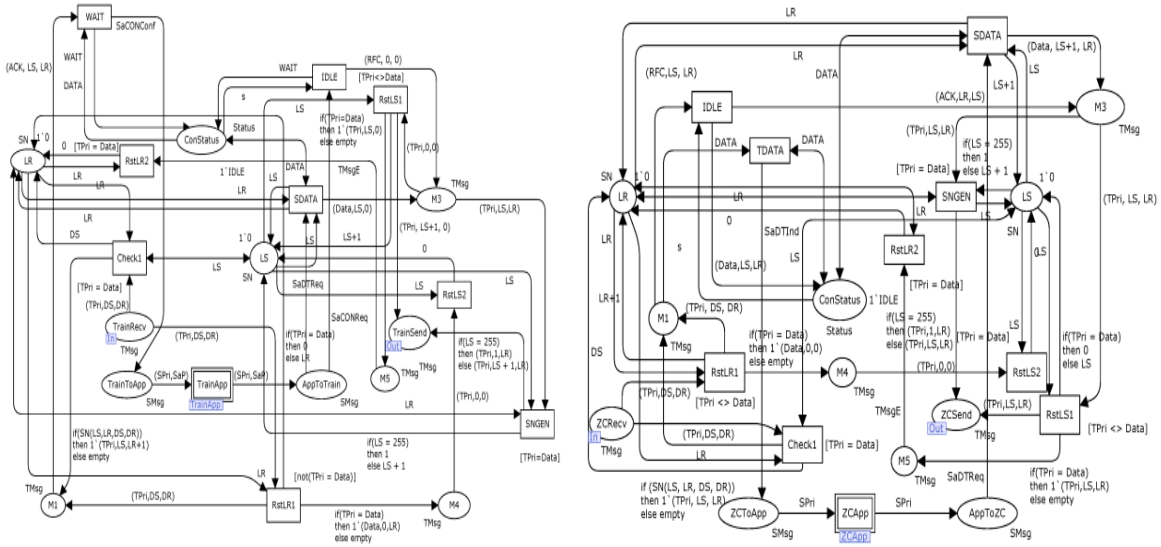
3. Petri NetModels of Safety Communication Protocol

For the model of safety communication protocol, the choice for the description formalism is Colored Petri net (CPN) [14]. CPN is extension of Petri nets: places could contain colored tokens to symbolize data content; hierarchically structured using substitution transitions and subnets [15]. Therefore, it could represent the safety states and information with colored tokens, and the actions with movement of the tokens.

3.1. Modeling of Function for the Protocol

In this paper the sender in figure 1 is considered as Onboard. Figure 2 shows models of safety communication protocol Onboard and trackside respectively, containing states referred in figure 1. Take the protocol Onboard for example, Place ConStatus stores 4 possible tokens, including “IDLE”, “WAIT”, “DATA”, and “HALT”. It contains an initial “IDLE” token, indicating IDLE in initial state.

When transition IDLE receives “SaCONReq” token through place AppToTrain and any token through ConStatus, it fires to deposit “WAIT” token into ConStatus and “RFC, 0, 0” token into place TrainSend finally. The “WAIT” in ConStatus and “ACK, LS, LR” in place TrainRecv enable transition WAIT, and deposit “DATA” into ConStatus and “SaCONConf” into TrainToApp. The “DATA” in ConStatus and the “SaDTReq” in AppToTrain enable transition SDATA to deposit a “DATA” token into ConStatus and “Data, LS, 0” token into TrainSend.



(a) Onboard (b) Trackside

Figure 2. Model of safety communication protocol Onboard and Trackside

3.2. Modeling of Extended Function for the Protocol

During the execution of safety communication protocol, there are requirements about time for the protocol. Figure 1 shows how the timer Timeout_ACK and Timeout_DATA work during the transition of the safety state. Therefore, Figure 3 presents the process from WAIT to WAIT, from DATA to DATA, the timer Timeout_ACK and Timeout_DATA, and Figure 4 presents the exact procedure of Timeout_ACK. The procedure treats safety state as WAIT when Sa-CONNECT.request is received, starting up 5s of timer. Once time-out of the timer happens, it resets if the safety state transfers to DATA, otherwise the state transfers to HALT and Sa-DISCONNECT. indication is sent.

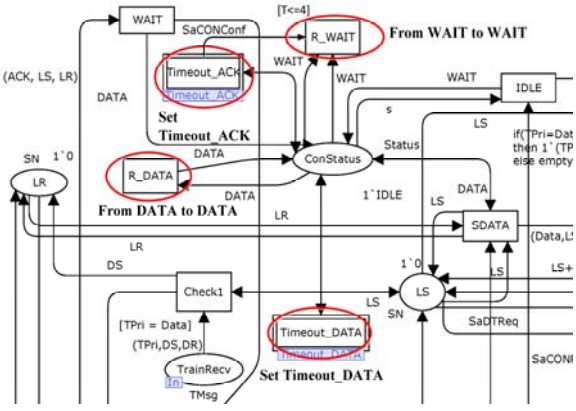


Figure 3. Modification part of the model Onboard with timer

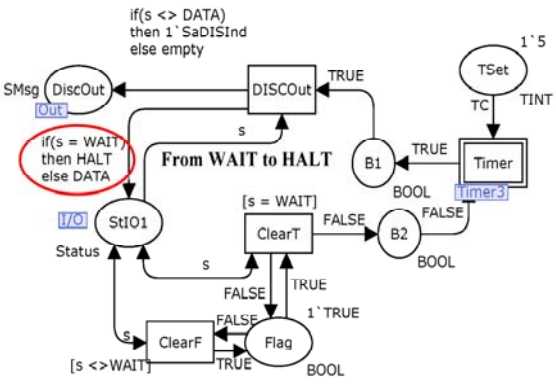


Figure 4. Model of timer for Timeout_ACK

4. Results of Performance Analysis

For safety communication protocol, there are disturbances, which influent the performance of the protocol, in the external environment. Usually, the probability of fault in channel and time delay of data are main factors, therefore, this section will analyze how the probability of no fault in channel and time delay could influent maintainability and failure probability.

4.1. Results of Simulation

Usually, maintainability and failure probability are important performance which people pay most attention to. Maintainability could be defined as: the probability of keeping connection of the protocol with different probability of no fault in channel. According to the definition of maintainability, it could be represent as Probability(Train'ConStatus = [DATA] andalso ZC'ConStatus = [DATA]), viz. the probability that the tokens in both the place ConStatus, in the models of train and trackside, which store the safety states, are "DATA".

Figure 5 shows the results of simulation. The X label represents different probability of no fault in channel, and Y label represents the probability of communication connection of the protocol, and different curves represent results with different probability of time delay. The general trend is that the probability of communication connection of the protocol will increase with the increasing of probability of no fault in channel and time delay. For quantitative analysis, it is also required that the probability of communication connection of the protocol should be higher than 0.95. Let x_1 is probability of no time delay, and x_2 is the probability of no fault in channel, figure 6 shows: $x_1 = 0.6$, $x_2 \geq 0.98$; $x_1 = 0.8$, $x_2 \geq 0.96$; $x_1 = 1$, $x_2 \geq 0.95$. If it could satisfy these conditions, it could guarantee the probability of communication connection of the protocol is higher than 0.95. This could be considered as a reference when designing the protocol.

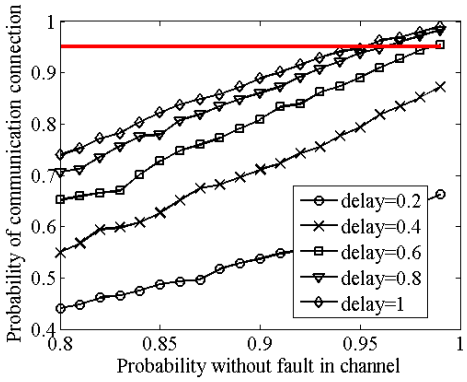


Figure 5. Probability of communication connection

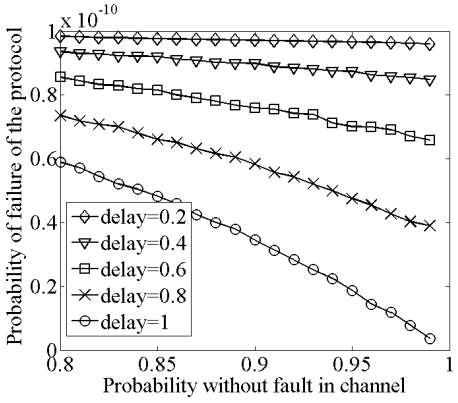


Figure 6. Probability of failure of the protocol

Failure probability could be defined as: the probability of disconnection of sender or receiver, which could be represented as Probability(Train'ConStatus = [HALT] orelse ZC'ConStatus = [HALT]), viz. the probability that the tokens in either the place ConStatus, in the models of train or trackside is "HALT".

Figure 6 shows the results of simulation. The X label represents different probability of no fault in channel, and Y label represents the probability of failure of the protocol. It could conclude that the failure probability of the protocol have a low level.

4.2. Analysis of Influence Factors

In order to find how the probability of no fault in channel and time delay influent the performance of the protocol, the section analyzes how these two factors influent the maintainability and failure probability of the protocol through theory of probability and mathematical statistic [16], which could provide guidance for designing of safety communication protocol.

As mentioned above, set probability of no time delay as xl, and probability of no fault in channel as x2. Here set probability of communication connection as y_1, and failure probability as y_2. Set the range of x_1 is [0.2, 1.0], the range of x_2 is [0.80, 0.99]. Table 1 shows levels of the two influent factors, in order to carry out the initial orthogonal experiment.

According to Table 1, Table 2 shows the data of orthogonal experiment of the influent factors and performance of the protocol.

Table 1. Level of influent factor for the protocol

Influent factors / Levels	x_1	x_2
1	0.2	0.8
2	0.4	0.84
3	0.6	0.88
4	0.8	0.92
5	1.0	0.96

Table 2. Data of orthogonal experiment for the verification targets

Number	x_1	x_2	y_1	$y_2(\times 10^{-10})$
1	0.2	0.8	0.4403	0.9835
2	0.2	0.84	0.4754	0.9782
3	0.2	0.88	0.5169	0.9739
4	0.2	0.92	0.5531	0.9698
5	0.2	0.96	0.6232	0.9658
6	0.4	0.8	0.5496	0.9363
7	0.4	0.84	0.6083	0.9218
8	0.4	0.88	0.6817	0.9022
9	0.4	0.92	0.7428	0.8853
10	0.4	0.96	0.8185	0.8630
11	0.6	0.8	0.6520	0.8564
12	0.6	0.84	0.7013	0.8202
13	0.6	0.88	0.7724	0.7810
14	0.6	0.92	0.8386	0.7421
15	0.6	0.96	0.9099	0.7001
16	0.8	0.8	0.7067	0.7360
17	0.8	0.84	0.7761	0.6805
18	0.8	0.88	0.8348	0.6166
19	0.8	0.92	0.8921	0.5437
20	0.8	0.96	0.9471	0.4552
21	1.0	0.8	0.7398	0.5893
22	1.0	0.84	0.8037	0.5047
23	1.0	0.88	0.8577	0.3998
24	1.0	0.92	0.9157	0.2839
25	1.0	0.96	0.9628	0.1438

According to the data in Table 2, it could be carried out range analysis, variance analysis, and regression analysis.

(1) Range Analysis

In Table 3, for the probability of both communication connection and failure of the protocol, the range of x_1 is higher than x_2, which illustrate that the influence of time delay for the performance of the protocol is greater than fault in channel.

(2) Variance Analysis

As the purpose of variance analysis is to avoid the fluctuate of data caused by deviation of experiments, Table 4 shows the results of variance analysis.

Table 4 indicates, for both the probability of communication connection and failure of the protocol, the F ratio of x_1 is higher than x_2. This also illustrate that the influence of time delay for the performance of the protocol is greater than fault in channel, which is the same conclusion as above.

Table 3. Range analysis of data of orthogonal experiment for the influent factors and performance

y_1(Probability of communication connection)		
Level	x_1	x_2
1	0.5218	0.6177
2	0.6802	0.6730
3	0.7748	0.7327
4	0.8314	0.7885
5	0.8559	0.8543
Range	0.3341	0.2366
$y_2(\times 10^{-10})$(Failure probability)		
Level	x_1	x_2
1	0.9742	0.8203
2	0.9017	0.7811
3	0.78	0.7347
4	0.6064	0.6850
5	0.3843	0.6256
Range	0.5899	0.1947

Table 4. Result of analysis of variance for the influent factors and performance

Probability of communication connection (y_1)				
Source of variance	Sum of square	Free degree	Mean square	F ratio
x_1	0.3697	4	9.2425×10^{-2}	369.7
x_2	0.1711	4	4.2775×10^{-2}	171.1
Deviation	0.004	16	2.5×10^{-4}	
Failure probability (y_2)				
Source of variance	Sum of square	Free degree	Mean square	F ratio
x_1	1.1321×10^{-20}	4	2.8303×10^{-21}	61.1
x_2	1.1858×10^{-21}	4	2.9645×10^{-22}	6.4
Deviation	7.4121×10^{-22}	16	4.6326×10^{-23}	

(3) Regression Analysis

In order to show the influence of fault in channel and time delay for the protocol more obviously, regression analysis is carried out as follows.

a. Test of goodness-of-fit for the regression equations

According to data of orthogonal experiment, the regression equation is fitted through Matlab:

$y_1 = -0.5 + 1.065x_l + 0.4294x_2 - 0.546x_1^2 + 0.5866x_22$

$y_2 = (0.0561 + 0.0014x_l + 0.2218x_2 - 0.0627x_1^2 - 0.195x_2^2)\times 10^{-9}$

Checking goodness-of-fit for the simulation results according to the regression equation, it could be obtained the coefficientR_1^2 = 0.9916 and R_2^2 = 0.944, being explained as the two variety of independent variables in the regression equations are 99.16% and 94.4% of the variety of dependent variables respectively, which indicates that the regression equations have a great goodness-of-fit.

b. Significance test for the regression equations

Table 5 shows the results of significance test for the regression equations.

Table 5. Hypothesis test results of the regression coefficients in the regression equations

Probability of communication connection (y_1)			
Model	Sum of square	F	$F_{0.05}(1, 22)$
Regression	0.5403	590.12	4.3
Residual	0.0046		
Failure probability (y_2)			
Model	Sum of square	F	$F_{0.05}(1, 22)$
Regression	1.2531×10^{-20}	84.35	4.3
Residual	7.4141×10^{-22}		

Table 5 shows the values of Fin two groups of experiments are both much higher than $F_{0.05}(1, 22)$, which indicates the regression equations are both significant.

c. Residual analysis

The residuals are caused by difference between the actual observed value of the data and the predicted value calculated by the regression equations. Figure 7 and figure 8 are diagrams of residuals, which shows that the values of residuals in the two groups of experiments are both near the zero value, and positive value and negative value could be offset basically. This also indicates that the regression equations fit the actual data.

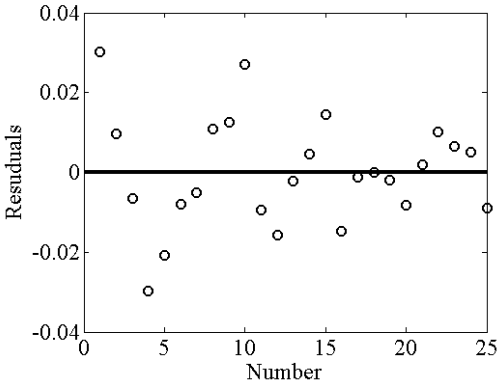


Figure 7. Diagram of residuals for probability of communication connection

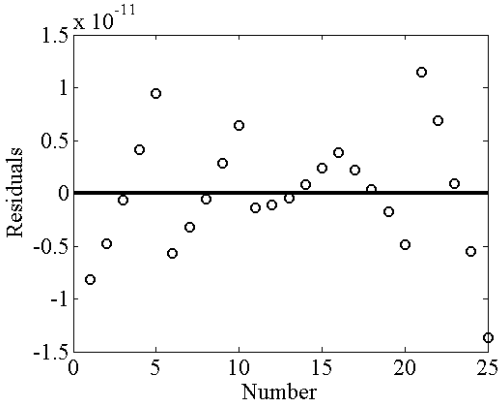


Figure 8. Diagram of residuals for failure probability

The results of regression analysis demonstrate that the regression equations are reasonable. It could be conclude through range analysis, variance analysis, and regression analysis that, compared to fault in channel, time delay is a relatively more important influent factor. This is because, if there is time delay, the safe state will stay at the initial state, but if there is fault in channel, as long as the value of timer Timeout_ACK or Timeout_DATA is lower than threshold, the safety state will transfer to the initial state to establish the safety connection again, no matter what is the safety state currently.

5. Conclusion

There is a growing demand to build safety communication protocol considered in wireless communication for train control system, involving creating an accurate and correct model, therefore performance is one important arm to guarantee correctness of the protocol. This paper describes the formal model of safety communication protocol with Colored Petri Net (CPN), a common formal tool, mainly including the safety logic of the protocol. In order to analyze performance of the protocol, maintainability and failure probability of the protocol with different probability of fault in channel and time delay are obtained through simulation by CPN, and then how fault in channel and time delay will influent maintainability and failure probability of the protocol are analyzed through theory of possibility and mathematical statistic. By comparison, it is found that time delay has a more obvious influent on performance of the protocol, which could provide a certain guidance for development of safety communication protocol in train control system.

Aknowledgement

This work is supported by the frame of the project “Beijing Laboratory For Mass Transit” under grant no. I13H100010.

References

[1] CENELEC. ICS 35.240.60; 45.020. EN 50159-2 Railway Applications-Safety related communication in open transmission systems, Brussels: CENELEC, 2001.

[2] Taeho Kim, David Stringer-Calvert, Sungdeok Cha. Formal verification of functional properties of a SCR-style software requirements specification using PVS. *Reliability Engineering & System Safety*. 2005; 87(3): 351-363.

[3] Mertke T, Menzel T. Methods and tools to the verification of safety-related control software. *IEEE International Conference on Systems, Man, and Cybernetics. Nashville*, 2000; 4: 2455-2457

[4] Yue Ni, Yushun Fan. Model transformation and formal verification for Semantic Web Services composition. *Advances in Engineering Software*. 2010; 41(6): 879-885

[5] Zhao Shuxu, Wang Xiaoming. Train control system formalization modeling oriented movement authority. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10(5): 992-998

[6] Donglai FU, Xinguang PENG, Yuli YANG. Authentication of the Command TPM_CertifyKey in the Trusted Platform Module. *TELKOMNIKA Indonesian Journal of Electrical Engineering.* 2013; 11(2): 992-998

[7] G.K. Palshikar. Safety checking in an automatic train operation system. *Information and Software Technology*. 2001; 43(5): 855-863

[8] Fabien Belmonte, Walter Schön, Laurent Heurley, Robert Capel. Interdisciplinary safety analysis of complex socio-technological systems based on the functional resonance accident model: An application to railway traffic supervision. *Reliability Engineering & System Safety*. 2011; 96(2): 237-249

[9] Jae-Ho Lee, Jong-Gyu Hwang, Ducko Shin, Kang-Mi Lee, Sung-Un Kim. Development of verification and conformance testing tools for a railway signaling communication protocol. *Computer Standards & Interfaces*. 2009; 31(2): 362-371

[10] Esposito Rosaria, Lazzaro Armando, Marmo Pieto, Sanseviero Angela. Formal verification of ERTMS EURORADIO safety critical protocol. Italy: Ansaldo Segnalamento Ferroviario S.p.A, 2005

[11] Jae-Dong Lee, Jae-Il Jung, Jae-Ho Lee, Jong-Gyu Hwang, Jin-Ho Hwang, Sung-Un Kim. Verification and conformance test generation of communication protocol for railway signaling systems. *Computer Standards & Interfaces*. 2007; 29(2): 143-151

[12] Jae-Dong Lee, Jae-Il Jung, Jae-Ho Lee, Jong-Gyu Hwang, Jin-Ho Hwang, Sung-Un Kim. Verification and conformance test generation of communication protocol for railway signaling systems. *Computer Standards & Interfaces*. 2005; 27(3); 207-219

[13] Euroradio FIS: Class 1 Requirements[EB/OL]. http://www.atif.org/db/doc/com/SUBSET-037V225, 2003.

[14] Jemsen K. Colored Petri nets. Basic Concepts. Analysis methods and practical use, Analysis methods. Monographs in theoretical computer science. Berlin: Springer. 1997

[15] E Nemeth, T Bartha, Cs Fazekas, KM Hangos. Verification of a primary-to-secondary leaking safety procedure in a nuclear power plant using colored Petri nets. *Reliability Engineering & System Safety*. 2009; 94(5): 942-953

[16] D Dubois, H Prade. Possibility Theory: an Approach to Computerized Processing of Uncertainty. Plenum: New York, 1998