Analysis of the Safety and the Performance of Railway Operation via Stochastic Petri Nets

Robert Nicolae[1] Florin Moldoveanu[1] Mihai Cernat[1]
Roman Slovák[2], Eckehart Schnieder[2]

[1]*Transilvania* University of Brasov, Faculty of Electrical Engineering and Computer Science
Blvd. Eroilor No. 29, RO-500036 Brasov, Romania
Tel., Fax: +40-268-474718, e-mail: cernat@leda.unitbv.ro

[2]Technical University of Braunschweig, Institute for Traffic Safety and Automation Engineering
Langer Kamp 8, D-38106 Braunschweig, Germany
e-mail: {slovak | schnieder}@iva.ing.tu-bs.de

***Abstract* – The objective of the paper is to investigate the applicability of stochastic Petri nets for the safety and performance analysis of the railway operation control system. The paper presents firstly the application for safety analysis where the quantification of the danger state probability was used as a reference value. Secondly the performance analysis was carried out by probability evaluation of an operation hindering state. Using a simulation based analysis method of the tool TimeNET 3.0 deterministic as well as general stochastic events in the model could be considered. The approximations of general stochastic events by exponential stochastic distribution are discussed in the paper.**

***Index Terms* – Stochastic Petri Nets, Safety Analysis, Performance Analysis, Railway Operation Control System, Maintenance Modelling.**

I. Introduction

The main task of a general Railway Operation Control System (ROCS) is to ensure a safe railway traffic process. This process must be free of intolerable risk, which is defined as the probability of an undesired event or state multiplied by the extent of accidental damage. From the safety point of view according to the norm [1] human life is taken as a reference for the extent of the accidental damage. To estimate the risk of responsible hazard situations in the traffic process, situations to be controlled by ROCS, in the first step the system design has to be analyzed. A suitable model of the traffic process can be applied for identification of the undesired operational events and for evaluation of their occurrence rates [7].

II. Model Analysis

Two kinds of analysis will be performed: the safety analysis, which will estimate the number of possible accidents that can occur and the reliability analysis of the model [6].

A. Safety *Analysis*

A safety analysis must be conducted for every experimental model that has been created, in order to determine how this model behaves under real conditions and to evaluate the risk of a possible accident which could lead to human casualties [2, 3].

The CENELEC standard [1] gives a definition of *risk* as: "the probable rate of occurrence of hazard causing harm multiplied by the degree of severity of the harm". Human life was taken as the measure of severity. According to the same standard *safety* represents: "freedom from unacceptable risk of harm". For safety analysis a case will be analyzed when the train was not detected by the train detection system, which means that the procedures for closing the barriers were never started. Therefore, if the train has not been properly detected, it could have entered the „*Danger zone*", and because the barriers were not lowered an accident could have occurred. The state when the train enters the „*Danger* zone" and the level crossing is not safe is called a hazard state. *Hazard* is defined as: "a physical situation with a potential for human injury" [1].

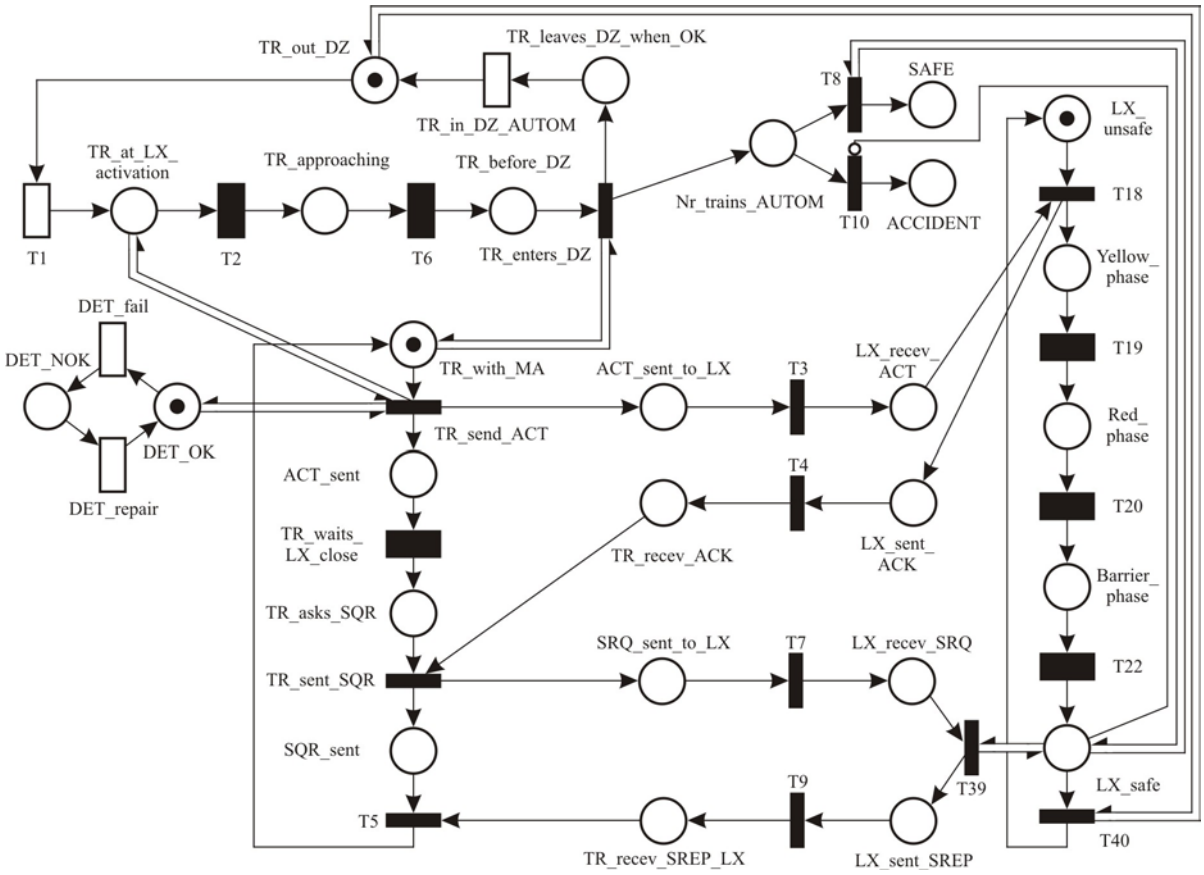


Fig. 1. The model simulated for the Safety Analysis.

The probability of the hazard state can be used for the final risk evaluation in form of the caused human fatalities. A risk acceptance criterion of the standard [1] is to be applied for the final conclusions about the tolerability of the operational risk of the analysed level crossing control system.

Considering that the failure of train detection is not a very frequent phenomenon, some adequate times were chosen for simulation. First it was considered that the detection could fail only one time per year. Then times like 0.5 years, 0.7 years, 2 years, 5 years or 10 years were selected and the model simulated for these values too.

The model from Fig. 4 [7] was modified in order to allow analysis and simulation of this new possible case and is presented in Fig. 1. For the results to be more accurate, the simulation time was set ten times larger than the possibility of defection (e.g. if the failing appeared once in 10 years, the model has been simulated for 100 years).

For the Safety Analysis, the number of tokens from the DANGER place is more important than the number of tokens from the SAFE place, because the purpose for this kind of analysis is knowing the number of possible casualties. Therefore, the hazardous state probability is calculated in percentages and represents the number of trains which are not detected by the train detection system of the total number of trains. With the known values a graph will be obtained as shown in Fig. 2.

B. Performance Analysis

1) *Clarifications*. A performance analysis was conducted in order to determine the reliability of the model. The CENELEC standard [1] defines reliability as: “the probability that an item can perform required

function under given conditions for a given time interval (t_1, t_2)".

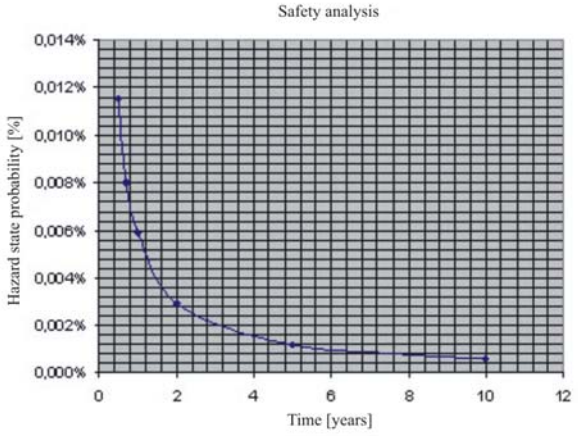


Fig. 2. Number of accidents obtained for 6 simulation times.

When failures were considered in the model, the reliability of the components had to be taken into account. Reliability must be analyzed for all four components of the Level Crossing Dependability Mode: yellow and red lights, barrier and sensor and for the radio component of the Communication Dependability Model.

When one of the components is failing, the transition between the intact place and the defect place is an exponential transition (e.g. YL_OK – >YL_NOK), but the reparation transition (e.g. YL_NOK –> YL_OK) is a general transition. For a better understanding of the differences between the general and the exponential transition in the repairing process, two variants of the model were analyzed.

In one model all the repairing transitions of the radio and level crossing components are exponential transitions and in the other model all the repairing transitions are general transitions.

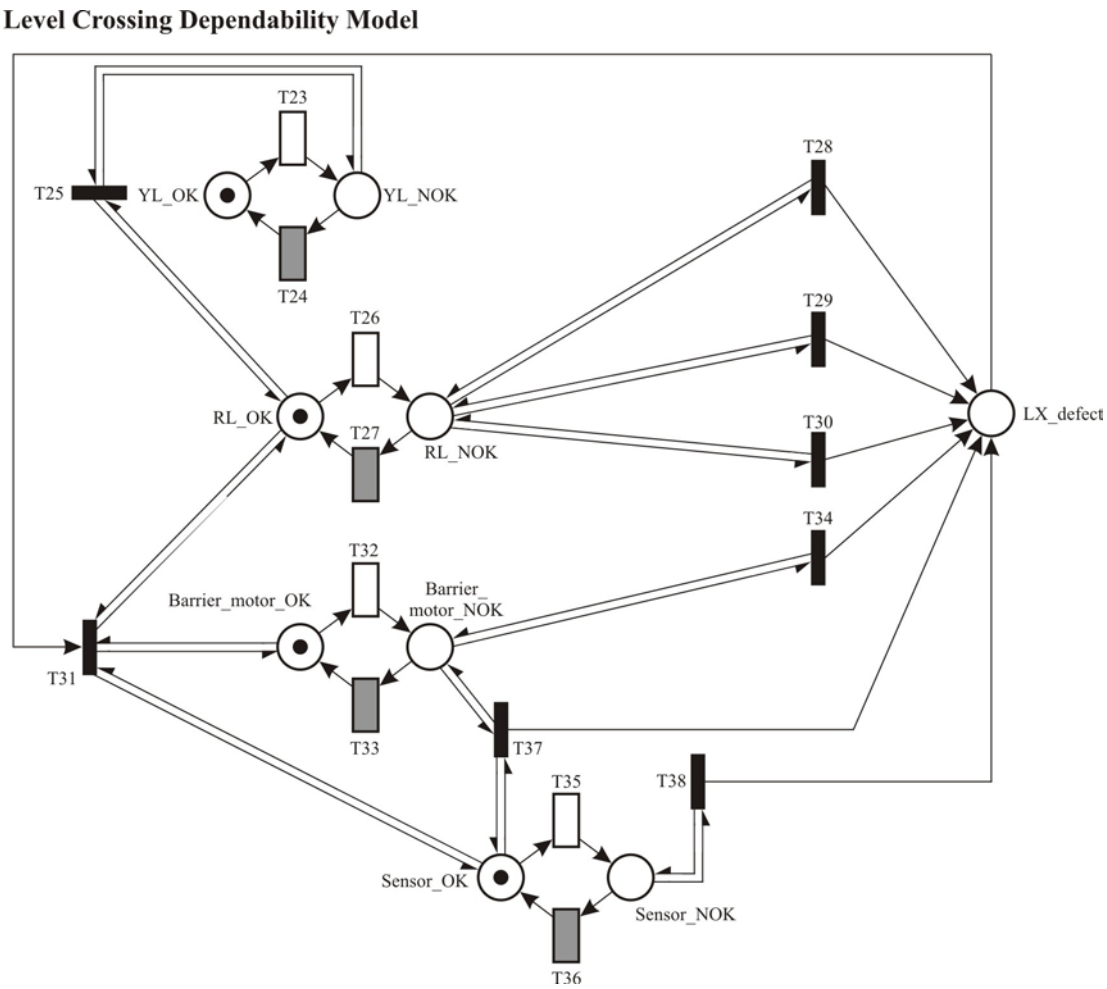


Fig. 3. The Level Crossing Dependability Model in which the repair transitions are replaced by exponential transitions

While the firing time of an exponential transition is described by an exponential distribution, the firing time of a general transition is described by a uniform distribution.

2) *The Model with Exponential Transitions*. The model with exponential transitions represents a modified version of the model with general transitions. In five cases, the repairing general transitions were replaced by exponential transitions. This can be seen in the Fig 3 (only four cases are presented for the simplification of the figure).

Two places are very important for the Performance analysis: TR_in_DZ_AUTOM and TR_in_DZ_manually. It is very important to know how many tokens will be in these two places after a specified simulation time. The construction of the model does not allow having one token in each place at the same time. The number of tokens in each place practically represents the number of the trains, hence in case of failure of one component, the number of tokens in each place should be very well known. Also, the model accepts that at one time only one component can fail and not more. A number of simulations were conducted in order to calculate the number of trains in both places and to have a better view of the behaviour of the model in the case when possible defects occur. Specified times of failure and repairing were selected in both cases: failure of the radio subsystem or failure of one component of the level crossing subsystem.

The simulations were conducted under special conditions, like when the radio component failed, it was assumed that none of the level crossing components could fail, and vice versa, when one of the level crossing components failed the radio component was considered not defect.

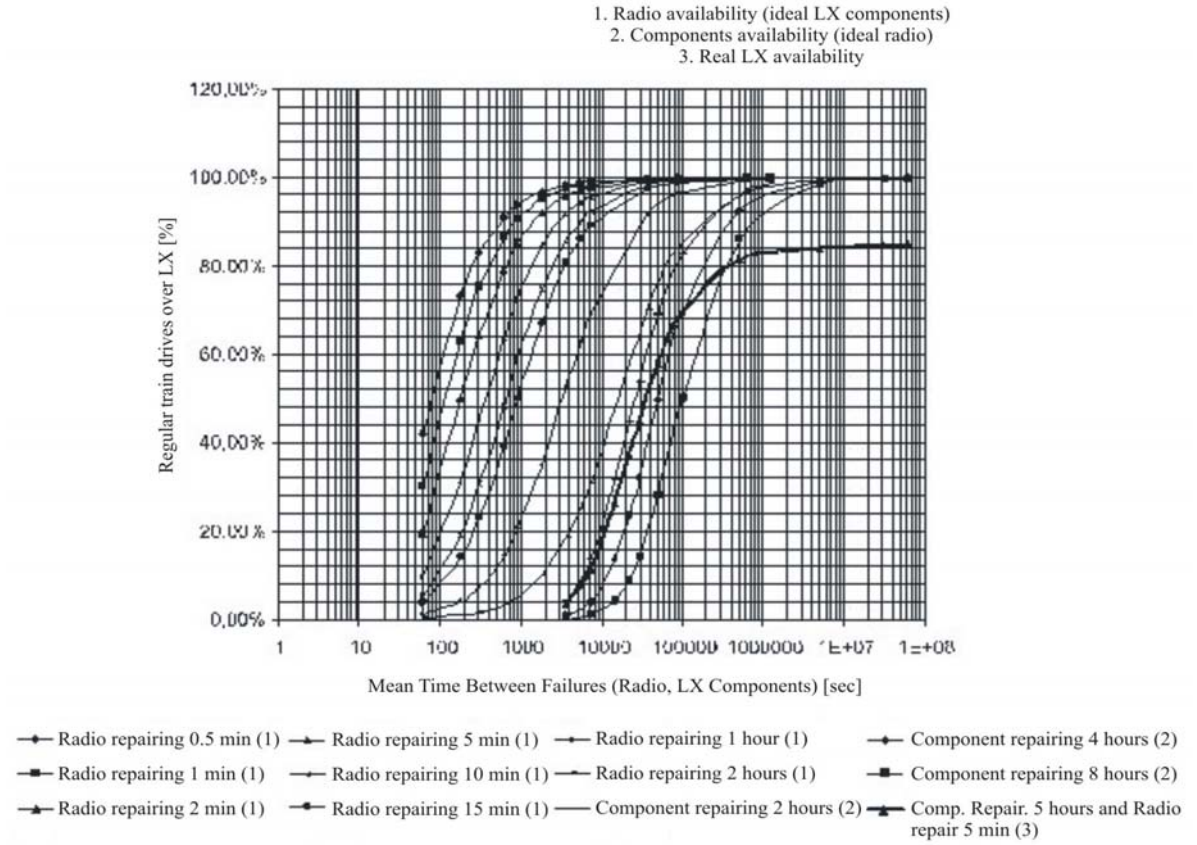


Fig. 4. Representation of the performance of the system with ideal and real case of the subsystem failure

In the end two simulations were conducted, where both radio and level crossing component could have failed, which actually represents the real case. The two diagrams have been presented in the final graph to compare the results.

In Fig. 4 the real case will be represented with a bold line and it can be seen that the reliability in this case is smaller than in the ideal cases. For the real case the reliability grows only up to 84%, unlike the ideal case where it increases up to almost 100%. The real case simulation is closer to reality and should be the one taken in consideration.

3) *The Model with General Transitions*.

The difference between this model and the one with exponential transitions is represented by the fact that general transitions with uniform distribution functions were used for repairing a possible failed component and not transitions with exponential distribution functions.

For repairing transitions, the best choice is the lognormal distribution function and the use of exponential distribution function is not indicated.

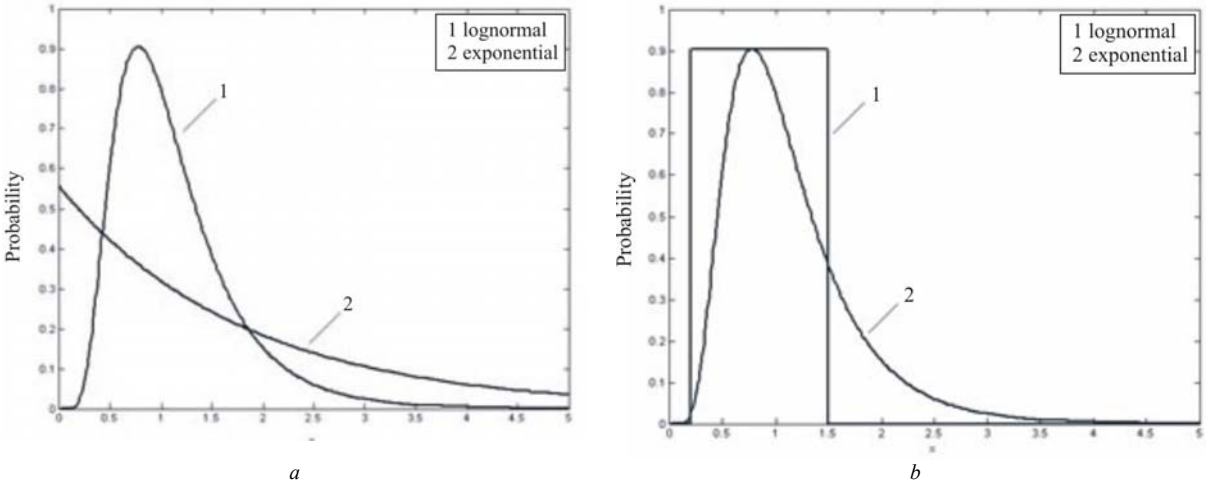
This can be seen in Fig. 5*a* where the exponential distribution does not follow the lognormal distribution graphic. The uniform distribution function represented in Fig. 5*b* can be considered an approximation of the lognormal distribution for the interval (0.25-1.5). Because of this possible approximation, the use of uniform distribution function instead of lognormal distribution function is possible. For the model with general transitions the simulations were performed again in two cases: the *ideal case* when two subsystems (radio communication and level crossing) could not fail at the same time and the *real case* when it is possible for two components to be defect at the same time.

The graphic with the results from both simulation cases are presented in Fig. 6.

Comparing the final representations of the models with exponential and general transitions (uniform distribution) some final conclusions can be drawn.

It is obvious that the model with general transitions with uniform distribution functions is more suitable for modelling the radio and the level crossing repair procedures.

The diagrams from Fig. 7 (dotted line) are increasing faster to the 100% value on the reliability scale, what shows they have a better dynamic than the diagrams for the model with exponential transitions (continuous line). A bigger difference between these two models can be noticed by comparing the radio repairing times over 2 hours.



a *b*

Fig. 5. Graphics of lognormal and exponential (*a*) and lognormal and uniform distribution functions (*b*).

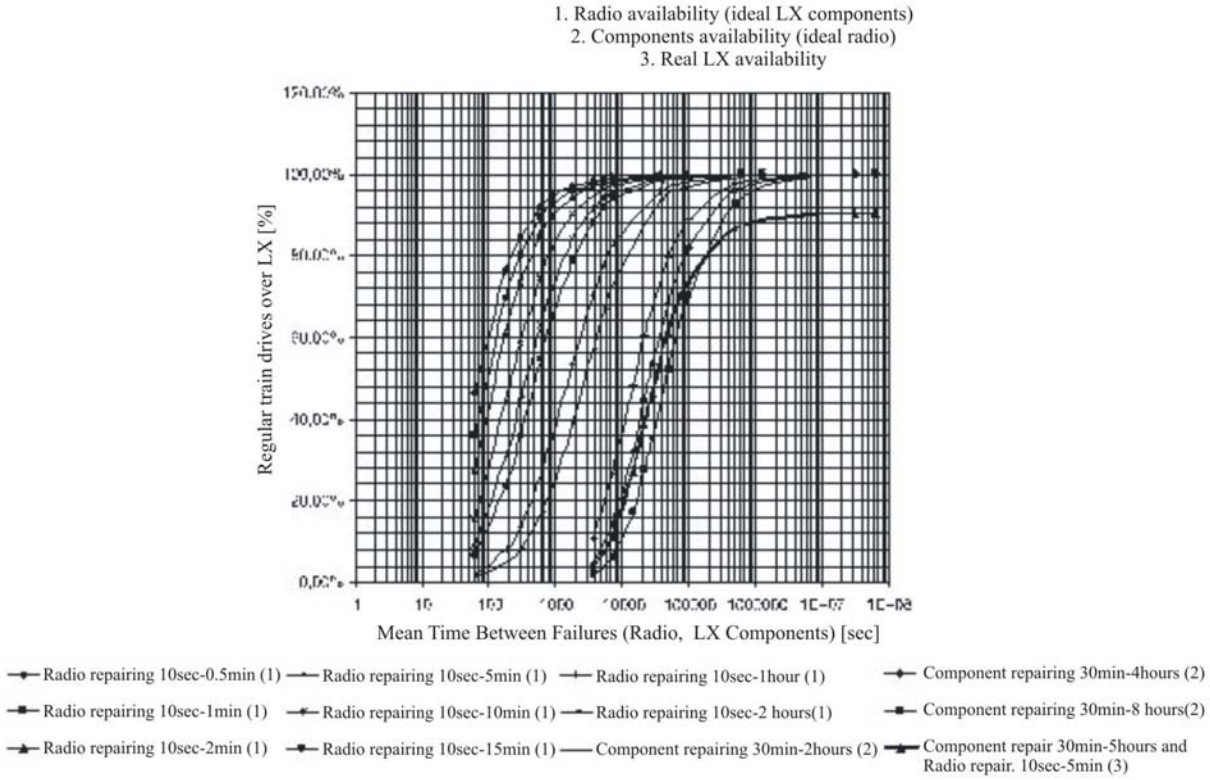


Fig. 6. Representation of the performance of the system in the ideal and real cases of subsystem failure behaviour (considering general stochastic distributions for the modelling of maintenance processes).

Also, the real case represents another motive for favouring the model with general transitions. In both cases the repairing times were 5 hours for the level crossing component and 5 minutes for the radio component. The "real case" of the model with exponential transitions (bold continuous line) reached a reliability level of 82%, while for the model with general transitions (bold dotted line) a level of 90% has been reached. These two results are important because a real case was simulated, when both radio and level crossing components could fail, and the results should be very important when a real model will be created starting from these experimental models.

III. CONCLUSIONS

The applicability of the stochastic Petri nets for the safety analysis of the railway operation control system was investigated. Two kinds of analysis were performed: the safety analysis and the reliability analysis. Representative temporal model parameters were selected such as to approximate real operating conditions.

For the safety analysis only a small numbers of simulations were performed due to the hardware limitations. In this case, the use of TimeNET 3.0 was not limited by the software possibilities although the simulation times were very long. The comparison of the performance results shows clearly a deformation of performance results when the exponential stochastic distributions are used for approximation of all non-deterministic events. Especially the processes of maintenance (repair) are to be analysed carefully and approximated with a suitable stochastic distribution.

For the model, using general transitions with lognormal distribution functions [8] was a necessity, for obtaining better results close to the ones obtained in real conditions. As the model did not support this kind of distribution functions, an approximation was required.

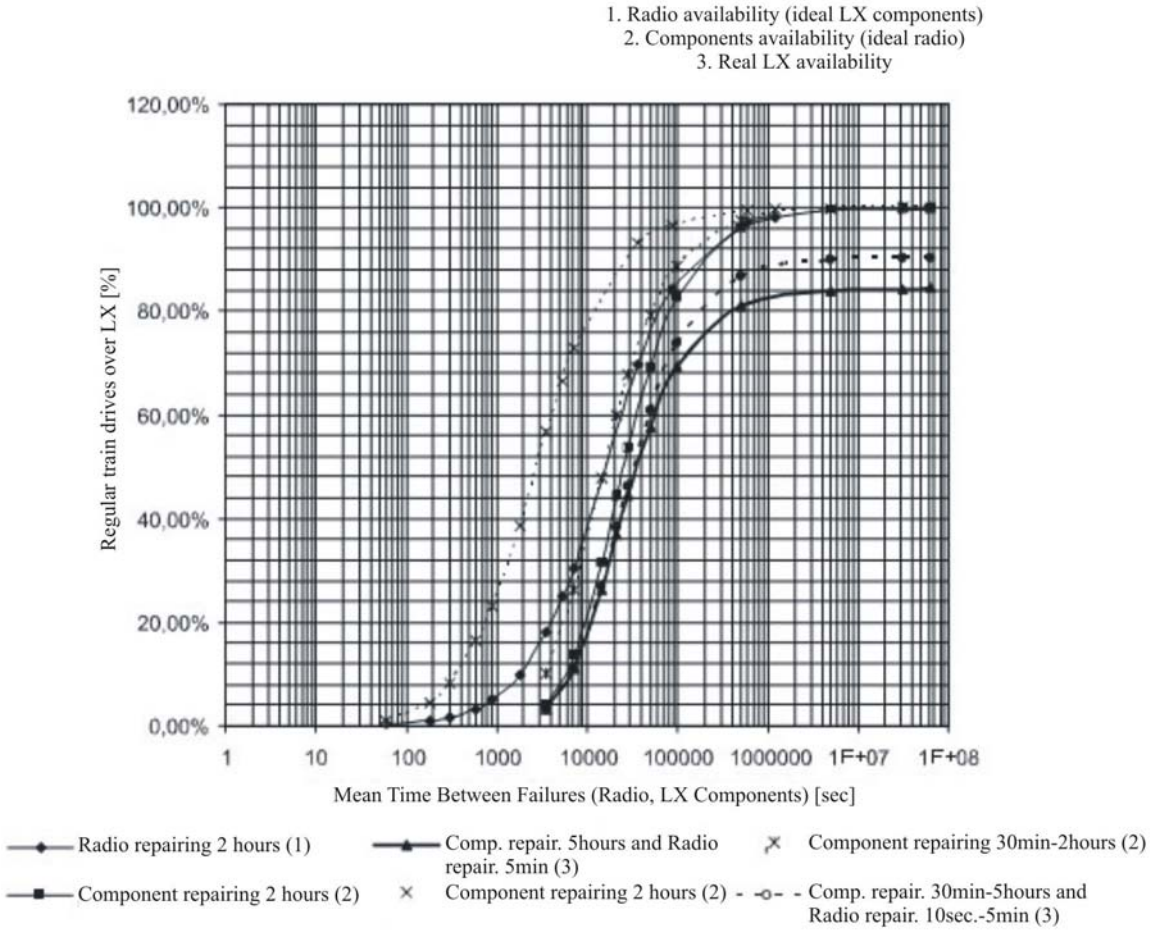


Fig. 7. Comparison of a model with exponential distributions only (continuous line) and a model considering general stochastic distributions of the maintenance events (dotted line).

With this approximation the results can not be the same with the ones that would have been obtained by using lognormal distribution. For this analysis a large number of simulations were performed, due the different types and times of failing.

Therefore in future new possible cases of simulations and new times of simulation can be selected. As a result of the development of hardware new simulation times can be tested and new results can be obtained. Also, using the future versions of software new formulas for distribution functions will be available and the results will be more accurate and closer to the real cases.

Finally it is envisaged that, future will yield more accurate results and allow more possible test cases, undoubtedly benefiting the evolution of traffic safety.

REFERENCES

[1] EN 50216: Railway applications: "The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)", Brussels, 1998.

[2] R. Slovak, J. May, P. Tomasov, E. Schnieder, "Approach to the Quantitative Risk Analysis of a Level Crossing Traffic Process by Means of Stochastic Petri Nets", *Transport* 2002, Sofia, 2002.

[3] R. Slovak, S. Einer, P. Tomasov, "A Petri Net Based Method for Proof of Safety of Railway Operation Control System, Integrated Design and Process Technology", *IDPT*-2002, June 2002, U.S.A.

[4] A. Zimmerman, *TimeNET 3.0 User Manual. A Software Tool for the Performability Evaluation with Stochastic Petri Nets, Performance Evaluation Group*, TU Berlin, June 2001.

[5] http://pdv.cs.tu-berlin.de/~timenet/

[6] R. Nicolae, :Modelling with Stochastic Petri Nets for Safety Analysis of a Railway Operation Control System. Diploma Thesis", *Transilvania* University of Brasov, 2003.

[7] R. Nicolae, et al., "Modeling of the Safety and the Performance of Railway Operation via Stochastic Petri Nets". *The 9th International Conference on Optimzation of Electrical and Electronic Equipment, OPTIM* '04, Brasov, May 20-24, 2004.

[8] K. E. Merphy, C. M. Carter, S. O. Brown: The Exponential Distribution: The Good, the Bad and the Ugly. A practical Guide to its Implementation, IEEE Proc. Reliability and Maintainability Symp. (RAMS 2002), Seattle, 2002.

[9] W. Schneeweiss, *Petri Nets for Reliability Modeling*. Verlag LiLoLe, Hagen, 1999.

[10] M. Marseguerra, E. Zio, Basics of the Monte Carlo Method with Application to System Reliability, Verlag LiLoLe, Hagen, 2002.