A Dependability Analysis for Integrating a Satellite Positioning System in a Rail Freight Application

Julie Beugin, Juliette Marais, Jean-Philippe Lozach

A Dependability Analysis for Integrating a Satellite Positioning System in a Rail Freight Application

Julie Beugin, *INRETS-LEOST*
Juliette. Marais, *INRETS-LEOST*
Jean-Philippe Lozac'h, *SNCF research division*

BIOGRAPHY

Dr. Julie Beugin received her engineer degree from the ENSIAME (the National School of Engineering for Computer Science, Automation, Mechanics and Electronics) in 2002 and her PhD. in Automation Engineering from the University of Valenciennes (France) in December 2006. She is currently a researcher in the French National Institute for Transportation and Safety Research (INRETS) where she is involved in the analysis of the satellite-based location service in railway applications. Until now her research interest deals with dependability evaluation of complex guided transportation systems.

Dr. Juliette Marais received an engineering degree from the Institut Supérieur d'Electronique du Nord in 1998, and a PhD. degree at the French National Institute for Transportation and Safety Research (INRETS) in 2002, on the analysis of the influence of propagation conditions and masking effects on service availability of satellite localization systems. She joined INRETS as a researcher in September 2002. Her fields of interest deal with: satellite navigation applications in transport environment, availability analysis and performance augmentation. She is involved in national and European projects dealing with navigation research in the field of terrestrial transport.

Jean-Philippe Lozac'h joined the SNCF as district inspector (Equipment function) in 1977 after finishing his studies in the Military college of Saint-Cyr (France). Between 1986 and 1990, he managed the "engineering structure" unit of the Paris–Saint-Lazare region. Since 1990, he has been working at the SNCF research division. He is currently in charge of the three-year research project called Tr@in-MD aimed at improving safety in the transport of dangerous goods by rail.

INTRODUCTION

Supervising freight rolling stocks on railway networks requires the knowledge of each train position. These are today be obtained by infrastructure-based equipments on the track. The use of a GNSS is considered as an interesting alternative as it allows activities related to the logistics of freight transportation to be improved and the trackside equipments to be reduced. This could contribute to make railway transportation of goods more competitive. Furthermore, it will allow supervising the transportation of dangerous goods like chemicals, acids, explosives, etc. because such goods are risky for the environment and the population. This is one of the objectives of the Tr@in-MD project (*Transport intelligent par fer des Marchandises Dangereuses* – intelligent railway transportation of hazardous materials) as well as using intelligent sensors that will detect incidents. A GSM equipment will send the GPS position data to the control centre in case of potential critical situation.

To prove that the satellite-based positioning system meet required performances compared to system specifications and railways requirements, the confidence placed in the system needs to be evaluated. Because such system is devoted to railway safety, a dependability analysis has to be performed. The analysis will prove that, even in case of failures, the studied system is able to guarantee a given level of performances expressed in the railway domain in terms of RAMS parameters (Reliability, Availability, Maintainability and Safety) [3]. These parameters are probabilities that rely on how each component of the system can fail (according to probabilistic characteristics of failure, environmental condition, etc.) and how each of them can influence others (dependencies, common cause failures). Considering the different segments of the GNSS, perturbations that can affect the satellite signals and that can lead to the calculation of a wrong position are the main source of failures that have to be studied. Our research focuses on this particular topic. No dependability analysis on satellite signal propagation exists at this time. Main difficulty will be to take propagation errors caused by signal deviation on obstacles like wagons or railway cuttings into account.

Assuming that no material failures can occur in satellite or receiver equipment (to consider them, a standard study could be performed using failure rates of the components), an original dependability analysis is proposed. This analysis is based on a Petri net approach that models the different states in which the satellite-based positioning system can be. First section of the paper will describe how the failures of the positioning system can be considered in this event driven approach.

Second section will present how such a model can be simulated to derive RAMS values. It refers to a statistical evaluation that depends on the analysis of the states where a wrong position can be obtained by the satellite positioning system. Finally, conclusions will present the interest of such an approach and the results that can be obtained for the rail freight application.

1. THE PETRI NET APPROACH TO ANALYSE FAILURES OF THE STUDIED SYSTEM

1.1. Definition of the studied system with a block diagram

The railway application uses data stemming from satellite signals to determine a position. Assuming all SIS (signal-in-space) data are correct because no ground or satellite segment failures, these data are the input of the system considered in this research work. The studied system can be represented by the block diagram of figure 1. Block diagrams, in dependability analyses, model the system in operation with series and parallel blocks. One block corresponds to one subsystem or basic component of the system. Sub-set of data used in the position calculation appears at the output of the diagram. To obtain this output, the combination of four or more navigation messages is necessary. A block "set of pseudo-ranges used to calculate the position" is then created. This last block requires as input the different navigation messages. These messages are carried by signals that are acquired simultaneously through parallel channels in receiver. Generally, receivers can have 12 channels for satellite tracking. They are here represented with 12 blocks in parallel in figure 1. The studied system is not further apportioned with satellite and ground segment parts according to the adopted assumptions. So the system bounds are placed at user level.

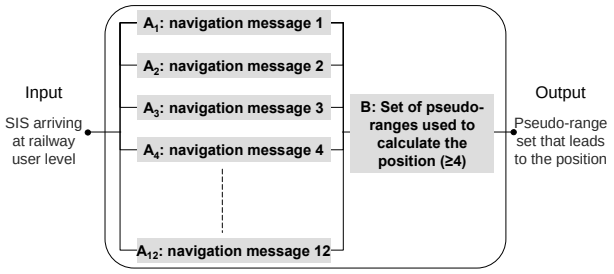

Figure 1: Studied system

1.2. Issue of the dependability analysis

The dependability analysis starts with the identification of each failure in the system. A particular attention is paid to the different failure combinations that lead to the failure of the studied system or the loss of the final output. The dependability analysis can then use the failure rates and the logical combination of each part of the system to achieve the RAMS performance evaluation. However, for the studied system, the navigation message failures are mainly determined by degradations caused by environment. As each place where the train user receiver is located is associated with a specific environment, no common failure parameter for the A_i blocks (like a failure rate) can be considered. Also, dependencies exist between each part of the system. They are the following:

- Block B needs at least 4 out of 12 navigation messages to operate correctly.
- Navigation messages used to calculate the position are selected by the receiver according to quality criteria (for example, with the SNR –signal to noise ratio– or the elevation angle of the satellite that emitted a signal). So the selected messages used to calculate the position at a given instant can be different from the one required later.

Consequently, these dependencies make the number of blocks A_i variable. It means that the structure of the block diagram modelling the system is not fixed.

So we propose first to model the system configuration evolution with time, i.e. the system dynamics, to re-create the different failure combinations associated to this system. For that, a Petri net-based model is envisaged. Evaluation process will be later addressed. Main principles of the Petri net modelling language are below described.

1.3. Main principles of the Petri net modelling language

Petri net (PN) is a mathematical tool devoted to model the dynamic behaviour of a system with time constraints. Formally, a PN includes a set of places P, a set of transitions T, a weight function W and an initial marking M_0. A PN is represented in a graphical structure where a circle represents a place and a rectangle stands for a transition (cf. figure 2). Directed arcs potentially associated to conditions (arrows with a weight or others conditions) and tokens (small black circles) respectively illustrate weight functions and marking. Places can be considered as conditions, and transitions as events. A specific marking of the net with tokens assigned to some places, symbolises that the system is in a certain configuration. It represents thus a given state of the system. Preconditions defined by the weight function require to be validated to fire a transition. When the transition is fired, the system reaches a new state according to post-conditions.

PN can include a time logic that makes possible to represent delay between events and specific firing times of an event. Time constraints are included with timed conditions either in a place (PN is called P-timed PN) or when firing a transition (PN is called T-timed PN). These two PN classes model deterministic behaviours. If delays are randomly distributed, the resulting PN is called stochastic PN (cf. figure 2b and 2c). Tokens can be associated to a value (or t-uple), called "colour", to memorise characteristics of the system (PN is called coloured PN, cf. figure 2d).

The evolution of the physical parameters of a system refers to the deterministic behaviour of the system. The random failures and the demand of each part of the system refer to the probabilistic behaviour. Given a PN model associated to a system, simulations of this model allow dependability evaluation to be performed [1,2].

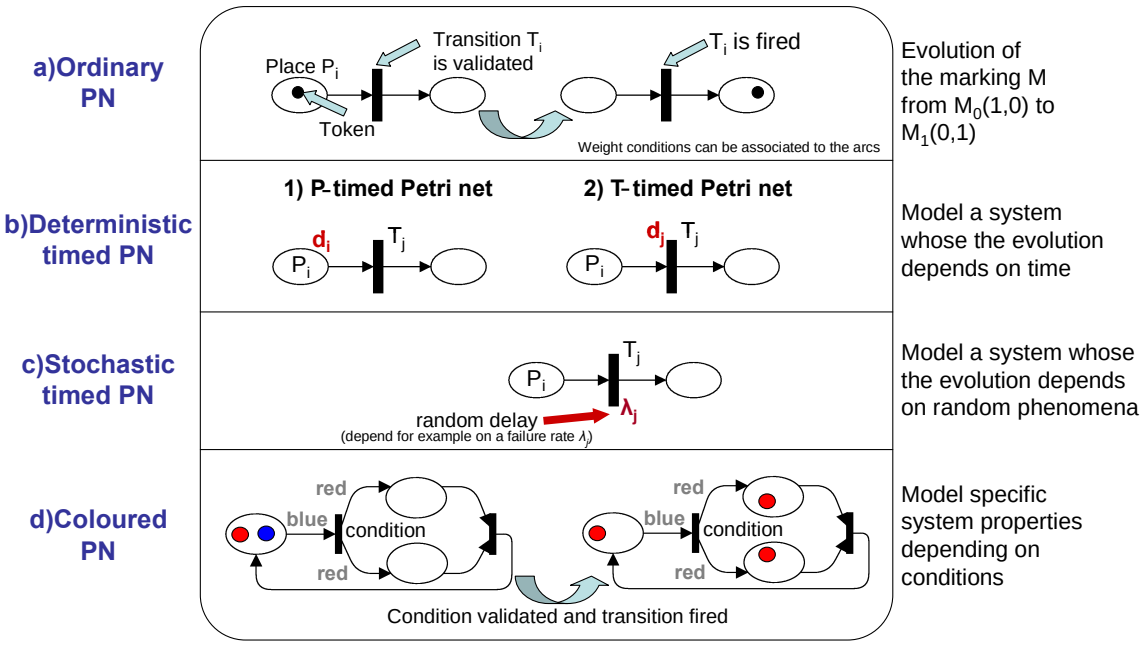

Figure 2: The different Petri net classes used in the analysis

1.4. Modelling deterministic and stochastic behaviours of the studied system with PN

The global Petri net model, which is proposed, is depicted in figure 3. Next paragraphs detail how it has been obtained.

In our model, the *deterministic* behaviour is linked to the reception state of the different signals (line-of-sight, non-line-of-sight states), which depend on the degradations caused by the environment configuration around the train. When signals cannot be received directly, the alternate path signals are the only data for pseudo-range calculation [4]. If the attenuation caused by propagation phenomena is not too strong, the receiver will use alternate paths signals to estimate the pseudo-range thus, induce a position failure due to the propagation delay.

Two failure modes are then identified for the A_i blocks of figure 1, one block corresponding to one signal:

- The signal is not visible.
- The signal is attenuated. According to a given threshold (from previous studies, we have fixed the attenuation threshold at SNR=38dB), one can consider that the signal has been received without any direct ray. The computed pseudo-range is therefore a wrong information that lead to the failure of the studied system. In such a case, B block should not select it for the position calculation.

Each time the position is demanded, the model keeps signals that are not associated to the two failures modes and tests if the number of navigation messages is sufficient.

One failure mode is considered for the B block of figure 1. This one is associated to the DOP (dilution of precision) quality criterion. If the DOP is higher than a threshold (DOP=3 is chosen), then the system fails to give correct position.

In our model, the *probabilistic* behaviour of the system depends on the random demands of each system sub-part. When the position function is demanded by railway users, signals are processed by receiver only if they are already tracked. Otherwise receiver has to acquire visible signals and this operation takes time. This behaviour is considered using the two following random parameters and indicative distributions that do not rely on reality for the moment:

- The random state of the acquisition: either or not signals are already acquired when railway users demand position. The two states are equally distributed with a probability of 0.5.
- The random time period for acquiring signals enough to calculate a position (the *time to first fix*). This time period is normally distributed with N(20,5).

In the model presented figure 3, the deterministic and probabilistic parts of the model are highlighted. In the deterministic part, the places and transitions associated to the two A_i failures modes and the failure mode of the B block can be distinguished with explicit designations. It can be noticed that the transition having double border rectangle includes sub-models which are not depicted here. The token colours used in the model are detailed in table 1.

Name of the token colour	Associated variables	Meaning
DATATIMED	(n,e,a,h)@t	(satellite identifier, signal state, attenuation, identifier of the tested scenario) at a given instant
DATADOPTIMED	(d,h)@t	(DOP value, identifier of the tested scenario) at a given instant
ACQUI	(na,tps)	(acquisition state, time to first fix)

Table 1: Token colours used in the Petri net model

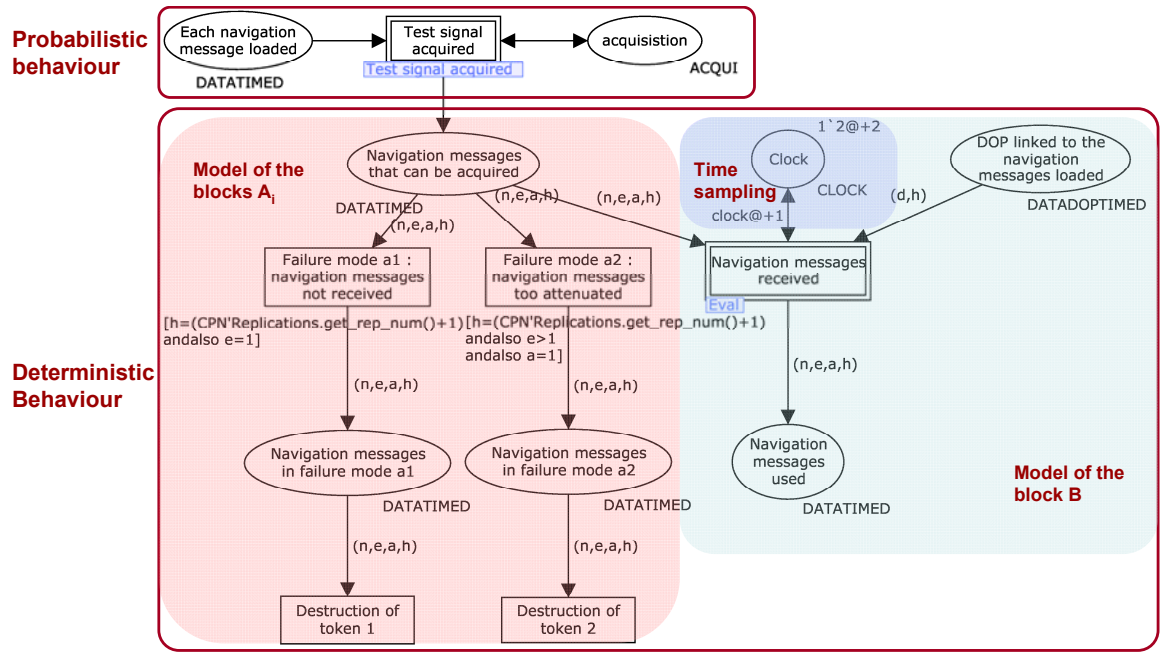

Figure 3: Petri net model of the system with *CPN-Tools* software

The system operation modelled above can then be re-created, to a certain extent, using simulations of the model. *CPN-Tools* software is used for constructing and executing the model [5]. In the model, the numerical values fixed arbitrarily can be readjusted in the future to better reflect the reality. The dependability evaluation is based on simulations of the model as it is described below.

2. EVALUTION PROCEDURE BASED ON THE PETRI NET MODEL

2.1. What are the dependability evaluations for the satellite-based location system?

Evaluating the dependability of the satellite-based location system, which provides position for the train application, is based on probabilistic evaluations regarding the system failure or the loss of the final output. These evaluations are related to the RAMS parameter evaluation. For the railway user a failure of the system occurs when the error (in meters) between the position calculated by the user receiver and the true position of the user is greater than a threshold defined in the application. This threshold is a requirement on the accuracy performance. If the environment masks some signals, the final output of the system is lost. Accuracy can not be directly measured at user level because the user only knows the calculated position and not the true position. So failures events related to accuracy cannot be identified by the user (they could be detected by an integrity diagnostic mechanism but this one is not included in the studied system). That is why the Petri net model uses quality criteria associated to the propagation errors to distinguish the system failure.

The events linked to a lack of accuracy due to different sources of propagation errors are, in this study, continuity events. The continuity of the position defined on a period of time represents the reliability (R of RAMS). Indeed, reliability is defined by the ability of a system to perform a required function under given conditions, for a given time interval. So, to evaluate the continuity is equivalent to evaluate the reliability.

Availability is a concept used both in GNSS performances description and in dependability analysis. It practically concerns the same concept. Availability-RAMS deals with the correct operation of the service at a given instant *t*. In this case, availability evaluation is only time-dependent. This idea is also considered in the availability definition of GNSS users, which consider furthermore the correct operation of the service at a given location. In this case, the availability evaluation is additionally space-dependent.

Safety concerns the absence of critical failures on a given time interval. The critical failures are those that can have catastrophic effects on the system in which the function is used, i.e. the railway system. These failures concern more the sensors of the tr@in-MD system than the satellite-based positioning function. If for example a sensor fails to detect chemicals leakage, the environment can be seriously damaged. So safety is not assessed in this article.

The repair notion associated to maintainability concerns a reconfiguration of a system that does not deliver intended service to the user because of hardware or software failures of some components. This notion is not developed in this paper because we choose to focus on propagation problems causing position failures. So with the assumption that hardware and software failures do not affect GNSS service, the RAMS study of the positioning function excludes the maintainability evaluation.

The dependability parameter evaluation of the satellite-based location system, which provides position for the train application, is based on several simulations performed on the Petri net model. This is now explained.

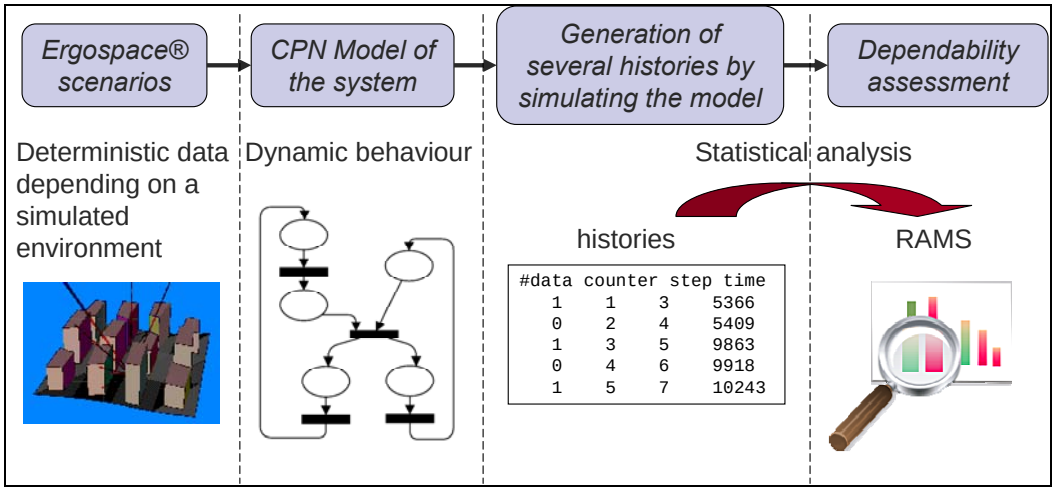

Figure 4: Simulation procedure

2.2. The evaluation procedure using simulations

The global simulation procedure adopted to evaluate the dependability parameters based on the failure of the system is described in figure 4.

To simulate the propagation of GPS signals in constrained environments, the Ergospace® software is used to obtain the physical parameters and the quality criteria, i.e. the visibility data, the SNR and DOP data that are calculated by the user receiver. In Ergospace®, a specific itinerary of a train is simulated in a fictive environment. The train takes 43s to cover the itinerary. The train run is simulated at several moments of a given day in order to consider different configurations of the GPS satellite constellation. The train moves through the itinerary at the beginning of each hour of the day. 24 hours are considered, so 24 simulations are performed. These simulations are called scenarios hereunder.

The files generated with Ergospace® are processed to extract the deterministic data and to convert them in formatted files that can be imported in CPN-Tools software. In the Petri net model, the position function is requested by a hypothetical railway user at the beginning of one scenario and until the scenario is finished. At the train start, the signal acquisition state is tested according to the sampling of the probabilistic distributions defined above.

Simulating the Petri net model with the different scenarios leads to several histories related to the studied system. These histories can be statistically analysed to evaluate dependability parameters.

3. SIMULATION OF THE PETRI NET MODEL AND DEPENDABILITY RESULTS

3.1. Availability evaluation

The unavailability of the system is calculated at each time sampling, i.e. each time the position is demanded (the frequency is fixed to 1 per second). It reflects the probability at each time sampling that the system fails or that the final output is lost.

For that a monitor is associated to a place called P_{out} in the model that represents the output of the system. A monitor is a mechanism used in CPN-Tools to observe a part of the net during simulation and to report the observations in files. Here is the marking of P_{out} each time a token enters in the place that is reported in files. One data file corresponds to one generated history. Having these recorded data and performing statistics on these data allows the curve of figure 5 to be obtained.

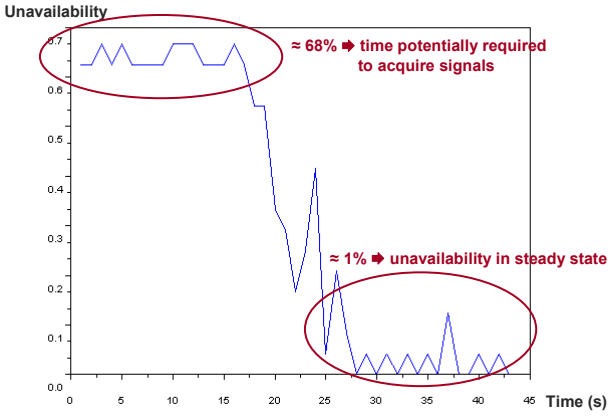

Figure 5: Unavailability of the positioning system according to time

High unavailability with a probability of 0.68 can be observed between 0 and 15s. It reflects the time potentially required to acquire signals at the beginning of the train trip. This probability greatly decreases until about 0.1. It reflects the unavailability of the function given acquired signals.

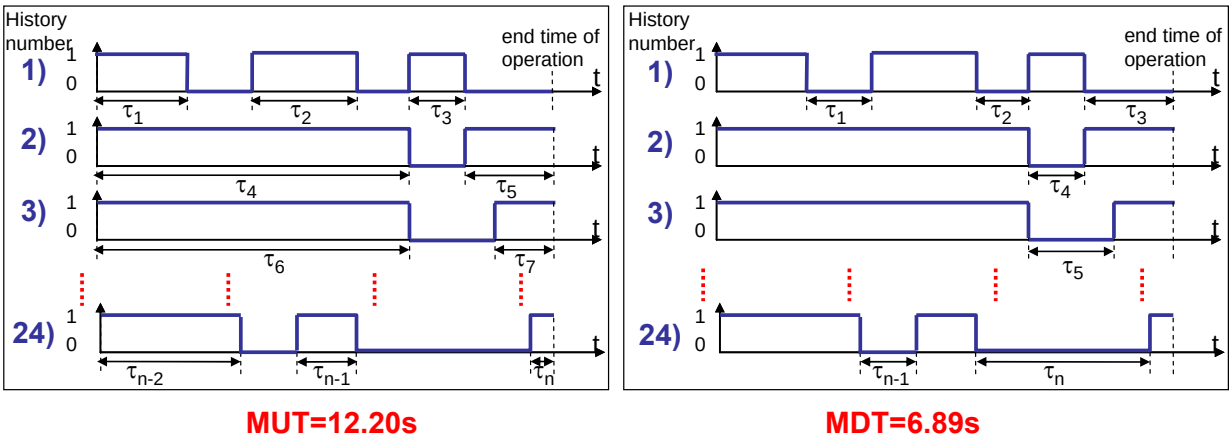

Figure 6: MUT and MDT evaluation

3.2. Reliability evaluation

Reliability is expressed with the MUT and MDT reliability indicators. MUT (Mean Up Time) is the mean time during which the positioning system is in operation, i.e. the failure modes do not lead to the failure of the system. MDT (Mean Down Time) is the mean time during which the positioning system fails. As figure 6 depicts, they are obtained with the statistical analysis of the 24 histories of the system. MUT is calculated using the different time periods when the output of the studied system is correct (state 1). MDT is calculated using the different time periods when the output of the studied system is wrong (state 0). The obtained results show that the system often fails because short MUT (12.20s) compared to the entire time of operation (43s) but is quickly back because also short MDT (6.89s).

It can be noticed that asymptotic unavailability can be obtain with the equation MDT/(MUT+MDT), which leads to a probability of 0.36. This result is much more than the probability of 0.1 obtained just before. This is due to the average calculation, which does not reflect that the system is more unavailable at the beginning than at the end of the operation.

Of course, all these results depend on the parameters entered in the model and have to be adjusted according feedback data or data provided by the supplier of the satellite receiver.

CONCLUSION AND PROSPECTS

In order to evaluate the performances of the satellite-based positioning system, which is used in the rail freight application mentioned in this paper, a dependability analysis is necessary. However, in the current dependability methods evaluating RAMS probabilities, no method is able to quantify the signal propagation errors that stem from environment effects and that affect the user position estimation. We have therefore proposed an original Petri net-based approach to deal with this problem. With such an approach, the dynamic behaviour of the system located in a given environment can be modelled, especially when system failure occur. The Petri net model has been presented and the simulation procedure to derive dependability evaluations has been explained. The obtained quantitative results show the benefice of such an approach that can lead to the dependability performance assessment.

The proposed approach based on a model/simulation scheme to perform evaluation is an alternative to the evaluation procedure using a reference system like in [6]. It could be profitable in future research to compare the both for validation purpose. The use of real input data to perform the evaluation is also envisaged. Indeed, for the moment, the model integrates signal quality criteria provided by a ray tracing tool. Additionally, to obtain a more generic model, we will focus on the integration of integrity data provided by an augmentation system or by the future Galileo system in the model.

ACKNOWLEDGEMENTS

This research is conducted in the framework of the Tr@in-MD project supported by the French Program of Research and Innovation in Terrestrial Transport (PREDIT).

REFERENCES

[1] Bernardi S., Bobbio A., Donatelli S. (2004). *Petri Nets and Dependability*. Lecture on Concurrency and Petri Nets: Advances in Petri Nets, Springer, pp.125-179.

[2] Dutuit Y., Châtelet E., Signoret J.-P., Thomas P. (1997). *Dependability modelling and evaluation by using stochastic Petri nets: application to two test cases*, Reliability Engineering & System Safety 55(2), pp. 117-124.

[3] EN 50126. (2000). *Railway Applications: The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*. UTE.

[4] Marais J., Flancquart A., Berbineau M.. (2003) *Prediction of GNSS availability in railway environments*. WCRR 2003-World Congress on Railway Research, Edinburgh, Scotland, September, pp. 1598-1604.

[5] http://wiki.daimi.au.dk/cpntools/cpntools.wiki

[6] Marais J., Poliak J., Hänsel F. (2007). *Tools for validation and acceptance of GNSS solutions in rail*. ENC-GNSS'07 - European Navigation Conference, Geneva, Switzerland, May, pp. 437-442.