RAMS analysis of GNSS based localisation system for the train control application

Khanh Nguyen, Julie Beugin, Juliette Marais

RAMS analysis of GNSS based localisation system for the train control application

T.P.Khanh Nguyen[(1)], J. Beugin[(1)], J. Marais[(2)]
Univ Lille Nord de France
[(1)]IFSTTAR, COSYS, ESTAS
[(2)]IFSTTAR, COSYS, LEOST
Villeneuve d'Ascq, France
Emails: khanh.nguyen, julie.beugin, juliette.marais@ifsttar.fr

***Abstract*—Global Navigation Satellite Systems (GNSS) is usually used in non-safety-related applications for various transportation modes. In order to employ GNSS (Global Navigation Satellite Systems) for train control application, numerous projects study if performance of GNSS can satisfy the railway safety requirements. In the railway context, multiple obstacles in local environments can cause different signal perturbations that lead to negative consequences on the position accuracy. Reinforcing the position quality for safety-related applications is necessary. In this context, the European Project - GaloROI is on going. Its working principle is based on the combination of data from GNSS receiver and an Eddy Current Sensor (ECS). According to the development process of GaLoROI system, the dependability and safety analysis is an essential mission in order to prove if it satisfy the safety railway standards. In this paper, we present a procedure for predictive RAMS analysis of a localisation unit based on the combination of GNSS & ECS for the application "control the braking loop". Besides capturing multiple local impacts on satellite signal quality, this approach allows us to analyse complex behaviours of the sensor fusion component and also to take into account the reliability parameters of hardware components.**

Keywords*—Dependability analysis, Dynamic repairable & time dependent Fault Tree, Petri Net modelling, GNSS based localisation system

I. INTRODUCTION

Global Navigation Satellite System (GNSS) becomes an advantageous solution and are usually used in various transport system because it offers an interoperable worldwide localisation solution. Furthermore, using an on-board GNSS based localisation unit can reduce the infrastructure / maintenance costs. These advantages explain why for recent years, numerous European projects studying on GNSS-based localization technologies have been deployed. Some of them are summarized in [3]. These projects consider two different approaches, either standalone GNSS or hybrid GNSS solution (e.g. Combination with others sensor systems) in order to reduce deployment, maintenance costs and also to improve accuracy, integrity, and reliability of train localisation. However, for introduction of GNSS in safety relevant application, the challenge remains to bring the evidences that the GNSS solution designed to meet the safety railway requirements in different operational conditions.

[3], [4], [8] concluded that a standalone GPS/GLONASS satellite navigation system and also its combination with inertial navigation systems (INS) do not meet the strong safety-related requirements mentioned in railway standards, especially in the particular operation environments like forest, tunnels, urban, railway cutting. They emphasized the necessity of reinforcing the performances of GNSS localisation unit by other sensors when they are used in safety applications. Therefore, identifying an appropriate configuration associated to a data combination strategy that meets railway requirements remains an issue. [1] discussed about a short-listing of data fusion options between GNSS signals and other sensors and then highlighted one of the advantages of the Eddy Current Sensor (ECS) compared to INS, which is the avoidance of velocity errors due to slip/slide.

In this context, the European GaLoROI project (Galileo Localisation for Railway Operation Innovation) seeks to develop a new safety application-relevant localisation system that combines satellite positioning data with satellite-independent data, here provided by an ECS, in order to provide a robustness train position on low density railway lines. According to the development process of this new system, the dependability and safety assessment is essential. They are described in the EN50126-2 standard [5]. These two kinds of assessments are interdependent and are realized together during RAMS management activities (Reliability, Availability, Maintainability, and Safety). These activities strive to ensure the quality of the service delivered by the equipment and integrate a standardized process of the systems development life cycle. Normally, the approaches for RAMS analysis can be classified into 2 classes.

1) In an operational approach, a procedure is based on the collection of feedback data mainly achieved by monitoring and observing the system in operation. The analysis of the database permits to extract useful information from the raw data before a statistical evaluation of the RAMS parameters.
2) In a predictive approach, a model is developed in order to capture system behaviours. Through this model, we analyse the causes that lead to system failures and also their consequences. The RAMS parameters of the system are evaluated based on probabilistic features like failure rate or simulation data.

The advantages and disadvantages of the two approach are summarized in the Table I.

978-1-4799-2903-0/14/$31.00-©-2014-IEEE

TABLE I. ADVANTAGES AND DISADVANTAGES OF RAMS ANALYSIS APPROACH

Predictive approach	Operational approach
Evaluation of RAMS parameters can be performed in multiple different operation conditions.	The conclusion is limited in given conditions of testing environment.
Uses less data than the other approach.	High testing cost, requires more time for collecting data than the other approach.
Cannot capture all real behaviours of the system, the evaluation therefore can include bias.	Unbiased assessment.

As the testing of global performance of the GaloROI system is still performed then in this paper, we will develop a new model to perform the predictive RAMS analysis of GaLoROI system for the application "control the braking loop". The paper is structured as follow: in Section II, we will present the preliminary of the RAM analysis for the system. Then, we will discuss the qualitative analysis approach in Section III. The approach for quantitative evaluation will be presented briefly in section IV. Finally, Section V will present the conclusion and the future research works.

II. PRELIMINARY OF THE RAMS ANALYSIS

A. Scope of the RAMS analysis

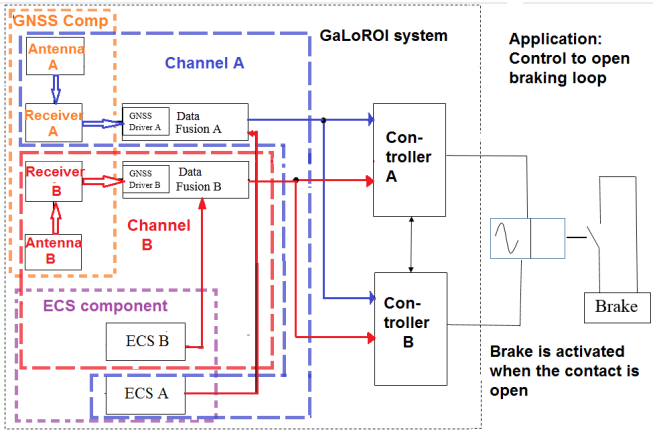

Fig. 1. Global view of the system architecture

The architecture of GaLoROI system uses the composite fail-safety technique described in [6] to ensure that the system meets its safety integrity level in the event of single random fault. Indeed, the safety-related function, e.g. control the braking loop is performed by the safe double controller. In this application, the brake is connected to both controllers. If one controller fails, the system enters in fail-safety state.
Each controller is connected to two redundant multi-sensor (ECS & GNSS) channels A and B, see Figure 1. By comparison of the data provided by two channel, the safe double controller will give decision. In each channel, every data from both GNSS and ECS that contain information about the position and the velocity of the train, are combined in a fusion component. This process is implemented in a computer that integrates a digital track map. With a data fusion algorithm that includes a map-matching process, an accurate train position can be calculated in real time.

B. Description of system functions and component behaviours

Figure 2 shows the sub-functions of the GaloROI systems using the FAST method (Function Analysis System Technique). This technique permits to answer to the question "why a function is performed" by looking at the diagram from right to left; to study "how a function can be made" by looking from left to right; and to consider "when the function is performed" by traversing from top to down. The functions that are simultaneously performed are represented using blue rectangles.

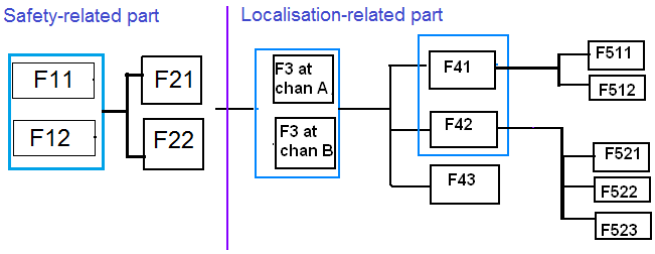

Fig. 2. Functional analysis of the GaloROI system for the control-braking-loop application

- F1: *Control the braking loop.* The brake is only released when both controllers command a release brake action. If one controller fails, the contact is open, brake is activated.
- F21: *Compare the output of two channels.*
- F22: *Give the control decision.*
  - If the data provided by one channel is invalid (missing data or untrustworthy data), the safe double controller gives the decision based on the position result of the other channel output.
  - At least one channel requires to open the braking loop, the brake will be activated.
  - If data provided by two channels are invalid, the brake will be activated.
- F3: *Provide a robustness position.*
- F41: *Collect GNSS positioning data.*
- F42: *Collect ECS speed data*
- F43: *Apply the data fusion & map matching process.* The data fusion is considered as failure if one of the following states occurs:
  - The fusion component failure directly causes an unavailable output.
  - The software errors during the fusion data process can deduce an unavailable output.
  - Unavailable ECS and GNSS data: If there is no ECS and GNSS data for more than T_1 s, the fusion component output can be untrustworthy
  - Unavailable GNSS data: If only GNSS data are missing for more than $T_2 s$, the confidence

interval linked to output data will increase quickly.
    - Inaccurate GNSS data: At least k consecutive position errors of the receiver that are greater than x meters ($PE_r > x$) can lead to a position error in output of the fusion component that exceeds the user tolerance limit.
    - If the ECS data are missing, at least l consecutive $PE_r > x$ m can lead to a position error in output of the fusion component.
      Note that due to the efficiency of the fusion algorithm, $k > l$

- F511: *Collect satellite data.*
- F512: *Calculate GNSS measurements.*
- F521: *Transmit and collect electromagnetic signals.*
- F522: *Analyse electromagnetic signal correlation.*
- F523: *Estimate speed using electromagnetic signals.*

C. Objectives of RAMS analysis

From point of view of railway users, the braking control function is considered as failed in the following cases:

- Case 1 - the brake is activated while the correct decision is to release the brake. This case directly causes a system unavailability.
- Case 2 - the brake is released while the correct decision is to open the braking loop. In this case, the service will be continue, however it can lead to a dangerous failure.

The principal objectives are to calculate the system unavailability based on the occurrence probability of Case 1 and evaluate the PFH - Probability of dangerous failure per hour (Case 2). The decision of the safe double controller is based on the positioning function that is considered as failed in the following cases:

Case A - Unavailable output of the fusion component.

Case B - Untrustworthy position, i.e. the position result has a large estimated confidence interval and cannot be used in safety-relevant train control applications.

Case C - Undetected position errors (PE), i.e. the estimated position is outside accuracy boundaries but is not recognized by the system or the user.

The combinations of causal events leading to system failure will be identified by the qualitative analysis presented in the next section.

III. Qualitative analysis of the GaLoROI system

The failures of GaLoROI system do not only depend on the material but also on satellite signal degradations due to the propagation environment. This latter poses multiple challenges for analysing and evaluating the service failure because common analyse approach cannot adequately take all perturbations affecting GNSS signals into account, especially local impacts of railway environments. In order to overcome this difficulty, we propose to use a Markov process to model the following states of GNSS receiver:

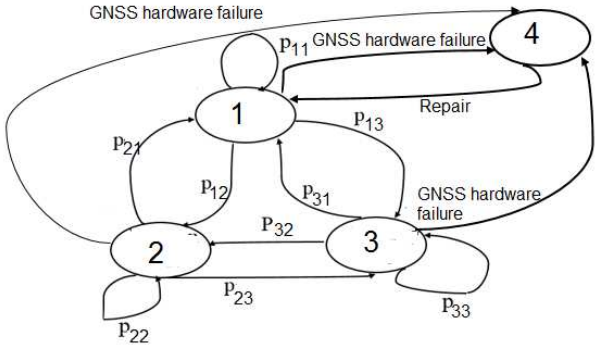

Fig. 3. Markov model for Receiver output

1) Correctly estimated position, $PE_r \leq x$ m.
2) Incorrectly estimated position, $PE_r > x$ m.
3) Unavailable position because of Miss-GNSS-signal.
4) Unavailable position because of a hardware failure.

Hereafter, we will consider the entering event into degradation states (state 2, 3, 4) of receiver output as basic events for system fault tree that will be considered at 2 level: Level 1 - System level and Level 2 - Channel level.

A. Fault tree analysis at system level

The Fault tree at system level is presented in Figure 4.

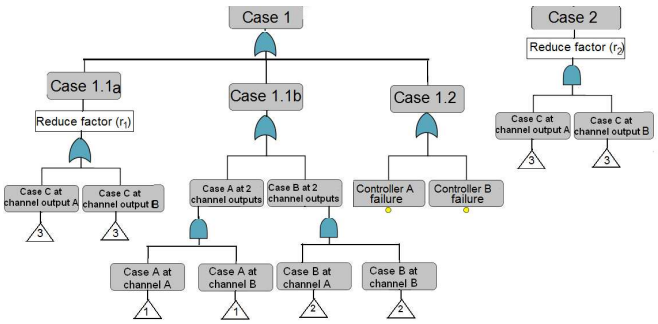

Fig. 4. Fault Tree at system level

The Case 1 - System unavailability can be classified into :

- Case 1.1 - The localisation function is incorrect and the safe controllers give the decision to stop the train.
  Case 1.1*a* - there is at least an undetected position error of one channel and based on it, two safe controllers decide to stop the train. Not all undetected PEs will lead to the wrong decision to open the braking loop instead of the releasing-braking-loop decision, so the reduce factor r_1 is used to represent this behaviour.
  Case 1.1*b* - two channel outputs are invalid.
- Case 1.2 - One of two safe controllers is false, the brake is then activated.

The Case 2 - Dangerous failure can be caused when there exist undetected and consistent position errors (PE) at both

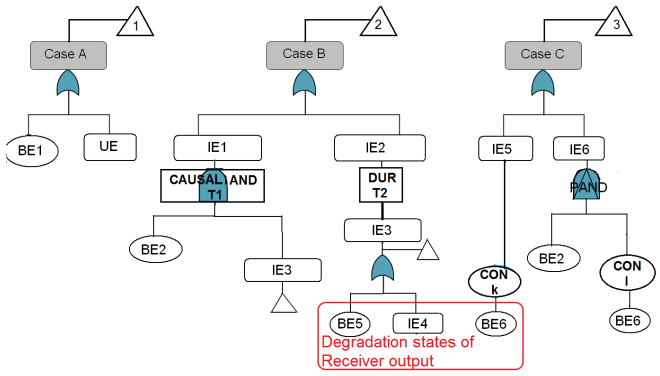

Fig. 5. Hybrid Fault Tree at channel level

BE1: material failure of the fusion component
BE2: ECS failure
BE5: missing GNSS signal (signal in space)
BE6: position error at the receiver output $> x$ m
IE1: lack of both GNSS and ECS data for more than T_1s
IE2: missing GNSS data for more than T_2s
IE3: missing GNSS data
IE4: GNSS hardware failure
IE5: at least k consecutive position errors of the receiver $> x$ m
IE6: at least l consecutive position errors of the receiver $> x$ m | ECS fails
UE: software error in the fusion component

channels. Not all undetected and consistent PE will lead to a dangerous failure, so a reduce factor r_2 is used to represent this behaviour.

B. Fault tree analysis at channel

The fault tree at channel level, Figure 5 show us the causes that lead to positioning failures at the fusion component output. Based on the functional analysis, these failures can be classified into 3 cases A, B, C.

In order to capture the dynamic behaviours of the fusion component, we propose in this paper a hybrid fault tree, i.e. combination between the Dynamic Fault Tree method (DFT) and time dependencies fault tree (TdFT). This approach allows us to consider at each sampling instant if sensor data are available and accurate, and also to handle temporal dependencies.

Recall that the output of the Causal AND gate only happens when its inputs occur together during the given period of time. The DUR gate is defined by the occurrence duration of the input during a given period of time. The output of CON gate only happens when its input consecutively occurs at least N times and the PAND gate output only happens when its inputs occur from left to right.

IV. Quantitative analysis of GaLoROI system

A. Modular approach for fault trees at System level

The Binary Decision Diagram (BDD) allows the calculation of probabilities related to the combinatorial logic gates in order to quantitatively analyse the fault tree's top event. However, this approach is only appropriate for the static system, i.e the system are examined without considering the possible evolution over time. Therefore in this paper, we propose to use the Petri Net (PN) approach based on the Monter Carlos simulation in order to evaluate the hybrid Fault Tree. The PN is a mathematical modelling language for the description of time dependent behaviours of systems and is widely employed in dependability assessments ([9]). Besides, The MC simulation is a powerful statistical method used to solve real problems, in particular when analytical approaches are not feasible. This method is based on the statical evaluation of a large number of scenarios. For this reason, it cannot produce an exact evaluation. The result accuracy strictly depends on the number of scenarios. This combination permits to:

1) consider the repairable multi-state components,
2) take into account sequence dependent behaviours of a system,
3) examine duration conditions of the causes that lead to critical events.

However, their solving time is an issue because the size of the system states increases exponentially in the number of components. In reality, often a very small part of the entire fault tree is dynamic in nature. Hence, the modular approach is proposed to identify and the solve the independent sub trees instead of for the large fault tree as a whole, [7]. Different techniques are applied to each sub tree depending on its characteristics (static or dynamic) and the solutions are integrated to get the solution for the entire fault tree.

The large fault tree of GaloROI system unavailability (c.f. Figure 5) has independent small parts in dynamic nature. Hence, we apply the modular approach to solve them. Consider the Figure 6, using the modular approach, the fault tree of Case 2 can be divided into 3 independent static sub trees. The Static sub tree 2 can be divided into 2 independent dynamic sub-sub-trees (Case B & C at channel output A; Case B & C at channel output B, see Figure 5).

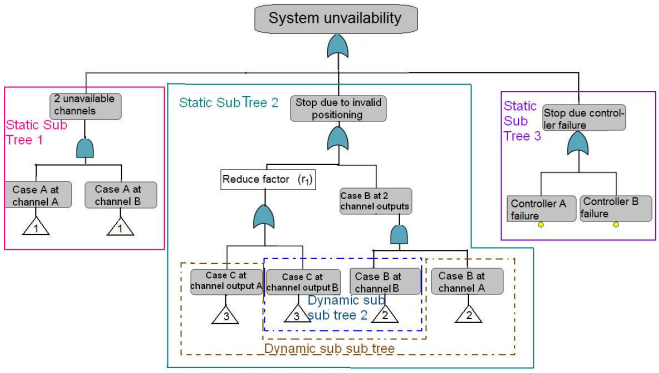

Fig. 6. Modular approach for the fault tree of the System Unavailability.

For calculating the probability of Case B & Case C of one channel output, we use the Dynamic Stochastic Petri Net (DSPN) to model the hybrid fault trees presented Figure 5. This is a powerful approach allows us to model the system states & its behaviours and then to evaluate their relevant occurrence probabilities. The solving approach for hybrid fault tree is summarized by three following steps:
Step 1 - model the evolution of component states over time, see Figure 7 for example.
Step 2 - translate dynamic logic gates through DSPN structure,

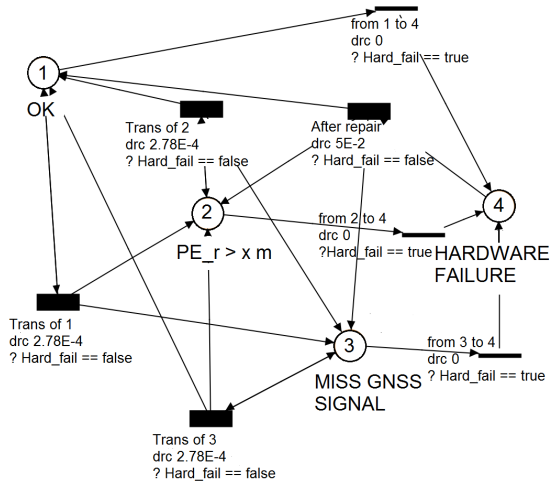

Fig. 7. DSPN structure for position results of GNSS receiver output

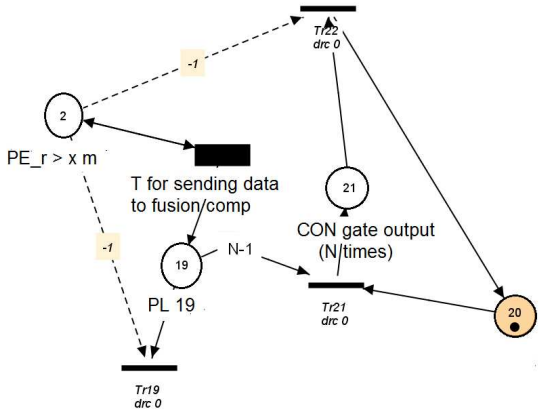

Fig. 8. DSPN structure for CON gate of N consecutive events

see Figure 8 for example.

Step 3 - construct the hybrid fault tree by integrating basic events (critical subsystem places) into the inputs of dynamic logic gates in order to evaluate probabilities of gate outputs.

Similarly, we can evaluate the probability of dangerous failure of the GaloROI system (Case 2 in Figure 4).

B. Quantitative results

In this section, a study case example is considered by following assumptions:

1) Repair rate (μ) is 1/24 and Time To First Fix of the global system is 180 s.
2) The probability transition between the states 1, 2, 3 of the receiver is calculated by simulation data of [3].
3) Let α_a, α_r, α_e, α_f, α_c be respectively the failure rate (/10^{-6}h) of the antenna, the receiver, the ECS, the fusion component and the controller, the input parameters are presented in Table II.

The SAU - system average unavailability and the PFH - probability of a dangerous failure during 1 hours of mission in different railway environments are presented in Table III.

TABLE II. INPUT PARAMETERS FOR CASE STUDY

T_1	T_2	k	l	r_1 & r_2
3 s	60 s	2	10	$[1E^{-6}, 0.1]$
α_a	α_r	α_e	α_f	α_c
4	4.08	2	6.06	0.7

For example, in the urban environment, when the reduce factor (r_1) varies from $1E^{-6}$ to 0.1, the SAU increases from $1.5E^{-7}$ to $4.7E^{-7}$. In the woody environment, the SAU and the PFH are the highest values when comparing with the ones of the other environments because in this woody environment, the multipath-effect becomes important. It causes multiple undetected-GNSS-position-errors that can wrong decisions:

- opening braking loop instead of releasing braking loop that affects on the SAU.
- releasing braking loop instead of opening braking loop that affects on the PFH.

TABLE III. PROBABILITY OF SERVICE FAILURE IN DIFFERENT ENVIRONMENTS

	Urban 1	Woody	Railway Cutting
SAU	$[1.5E^{-7}, 4.7E^{-7}]$	$[1.9E^{-7}, 4.2E^{-3}]$	$[1.5E^{-7}, 3.3E^{-6}]$
PFH	$[2.5E^{-18}, 2.5E^{-13}]$	$[4.4E^{-10}, 4.4E^{-5}]$	$[2.5E^{-16}, 2.5E^{-11}]$

V. CONCLUSION

The combination of GNSS sensors and ECS sensors promise to improve significantly the positioning quality in order to satisfy railway safety requirements. However, such configuration poses numerous challenges when analysing and evaluating the system dependability and safety. We have presented in this paper a practical solution to analyse RAMS parameters of a GNSS and ECS-based localisation unit. For the qualitative evaluation, the hybrid fault tree method is powerful for analysing complex and time-dependent behaviours of the data fusion component. Additionally, the model of the receiver outputs considers local impacts of different railway environments and the hardware failure probability.

The quantitative analysis was implemented by the modular approach for the fault tree at system level. For solving hybrid fault trees at channel level, we translate their elements toward DSPN. Then, a study case example is considered to illustrate the performance of our approach.

In future work, after the system tests in operational environments will be completed, the experimental data will be applied into the model for RAMS assessments. On the other hand, an operational RAMS analysis will also be performed in order to compare the results of this predictive approach. Furthermore, a more efficiency algorithm to improve the simulation time for quantitative evaluation could also be developed.

VI. ACKNOWLEDGEMENTS

This research was conducted as part of the GaLoROI project (Galileo Localisation for Railway Operation Innovation) supported by the European commission. GaLoROI is an

integrated research project within the European 7th Framework Programme.

REFERENCES

[1] A. Acharya, S. Sadhu & T.K. Ghoshal, *Train localization and parting detection using data fusion*, Transportation Research Part C 19, 2011, 75-84

[2] F. Boehringer, *Train location based on fusion satellite and train-borne sensor data*, Proc. SPIE 5084, Location Services and Navigation Technologies, 76 (August 6, 2003); doi:10.1117/12.487062

[3] J. Beugin, J. Marais, *Simulation-based evaluation of dependability and safety properties of satellite technologies for railway localization*, Transportation Research Part C 22, 2012, 42-57.

[4] A. Filip, L. Bazant, H. Mocek & J. Cach, *GPS/GNSS based train position locator for railway signalling*, Computers in Railways VII, 2000, ISBN 1-85312-826-0

[5] EN 50126-2, 2007. Railway applications specification and demonstration of reliability, availability, maintainability and safety (RAMS) Part 2: Guide to the application of EN50126-1. CENELEC European technical report (European Committee for Electrotechnical Standardization).

[6] EN 50129, 2003. Railway applications communication, signalling and processing systems safety related electronic systems for signalling. CENELEC European standard (European Committee for Electrotechnical Standardization).

[7] Gulati, R.; Bechta Dugan, J., *A modular approach for analyzing static and dynamic fault trees*, Reliability and Maintainability Symposium. 1997 Proceedings, Annual , vol., no., pp.57,63, 13-16 Jan 1997 doi: 10.1109/RAMS.1997.571665 .

[8] D.Lu, F. G. Toro and E. Schnieder, *RAMS Evaluation of GNSS for Railway Localisation*, ICIRT 2013 - IEEE International Conference on Intelligent Rail Transportation, Beijing, China, August 2013.

[9] M. Malhotra & K.S. Trivedi. Dependability Modeling Using Petri-Nets. IEEE Transactions on reliability 44 (3), 1995, pp. 428 - 439.