A new analytical approach to evaluate the critical-event probability due to wireless communication errors in train control systems

Thi Phuong Khanh Nguyen, Julie Beugin, Marion Berbineau, Mohamed Kassab

A New Analytical Approach to Evaluate the Critical-Event Probability Due to Wireless Communication Errors in Train Control Systems

Khanh T. P. Nguyen, Julie Beugin, Marion Berbineau, and Mohamed Kassab

***Abstract*—Wireless communication links tend to be employed more and more in safety-critical railway applications. Their safe use in an advanced train control system (TCS) is an issue that is addressed in this paper by characterizing the TCS service interruption due to communication errors. More precisely, occurrence probabilities of single errors are first discussed. Then, we obtain probabilistic analytical expressions of several temporal conditions that lead to a TCS service interruption, here a train emergency braking (the critical event). The accuracy of this analytical approach is proved when the results are compared with those given by a simulation approach with a Petri net model. Additionally, as the use case related to the "trains' separation" is considered in this paper, an analytical evaluation process is proposed to discuss the tolerated time margins that can be fixed to limit the critical-event occurrence probability due to the wireless communication errors.**

***Index Terms*—Rail transportation communication, rail transportation reliability, probabilistic model, intelligent transportation systems, wireless communication errors.**

I. Introduction

TRAIN control systems (TCS) are relying more and more on wireless communication systems (WCS) [1] as they improve train operations, especially by offering continuous communications between embedded and ground installations. Today, the European Train Control System (ETCS) Level 2 used for mainlines and high speed, relies on continuous exchanges via wireless cellular network known as Global System for Mobile Communications Railway (GSM-R). Communication Based Train Control (CBTC) systems used for mass transit lines, rely on wireless local area network (WLAN), IEEE 802.11x standards. In the future, among new wireless technologies, the Long Term Evolution (LTE) technology is considered as one of the promising solutions to satisfy the need to develop numerous intelligent and safe train control applications additionally to the TCS one (e.g., DAVS-Driver Assist Video System) [2]. Indeed, its architecture supports multiservice traffic and is also much less vulnerable to security threats than other wireless technologies [3]. For TCS, LTE makes possible the convergence of ETCS and CBTC systems in a unique system combining all features [4]. Besides the operation reliability and safety, the passenger comfort is also addressed by employing social network services for rail traffic applications [5]. Therefore, WCS for future railways is required to evolve from voice and signaling services to multiservice of high data rates [6]. This integration has to be realized by maintaining the current safety conditions provided today by existing TCS. This issue is addressed in this article by analyzing the impact of wireless communication errors on the TCS service interruption.

In the literature, the close relationship between WCS and TCS is generally approached in three ways. The first way, from the automation engineering domain, considers the impact of the WCS performances on the train traffic flow. It is based on the assumptions that performance parameters of the WCS are known and modeled by stochastic or probabilistic variables. In [7], the authors proposed a cellular automata model to investigate the impact of end-to-end communication delay on railway traffic flow. [8] studied the impact of random packet drops due to the frame error rate (FER) and handovers on the stability and performances of CBTC systems.

Unlike the first way that simplifies the WCS modeling, the second way focuses on the performance of the WCS with their close-to-reality-models in train control applications. In this context, the WCS performance issue takes even greater importance and is considered from the telecommunication expert's point of view while the train control modeling is simplified. Using Colored Petri Nets (CPN), the authors in [9] focused on modeling the WCS of the CBTC system in order to evaluate the transfer delay of messages between the trains and the zone controller (ZC). In [10], using OPNET (Optimized Network Engineering Tool) simulations, the authors proved that QoS (Quality of Service) mechanisms of a deployed LTE network are efficient enough for ensuring simultaneously safety and non-safety applications in ETCS. In [11], the authors also used the OPNET simulator to evaluate the performances offered by the LTE system to safety and non-safety applications in urban guided-transport. In [12], the authors derived the stochastic delay thresholds of high speed train control services over fading channels using the analytical analysis based on stochastic network calculus.

Manuscript received November 30, 2015; revised May 4, 2016 and July 28, 2016; accepted August 24, 2016. Date of publication September 13, 2016; date of current version May 29, 2017. This work was performed in the framework of the CISIT project (Campus Interdisciplinaire de recherche, d'innovation technologique et de formation à vocation Internationale centré sur la Sécurité et l'Intermodalité des Transports de surface) and SYSTUF project (SYStème de Télécommunications pour les Transports Urbains du Futur) supported by the French Government under the PIA (programme d'Investissements d'Avenir). The Associate Editor for this paper was S. Siri. *(Corresponding author: Khanh T. P. Nguyen.)*

K. T. P. Nguyen is with the ROSAS Department, University of Technology of Troyes, 10010 Troyes, France (e-mail: thi_phuong_khanh.nguyen@utt.fr).

J. Beugin and M. Berbineau are with the IFSTTAR-COSYS, University of Lille Nord de France, 59000 Lille, France.

M. Kassab is with the HANA Laboratory, ENSI, University of Manouba, 2010 Manouba, Tunisia.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

On the other hand, numerous studies aimed to proposed an efficient solution to limit the negative impact such as ping-pong effect, handover delay, packet loss on the performance of TCS. The paper [13] presented a handoff algorithm with frequency combination that allows for ensuring the channel quality and optimize handoff time. In order to reduce the handover delay, the multiple-input-multiple output (MIMO) assisted handoff scheme is proposed for CBTC system based WLAN technology [14] and for the one based on LTE technology [15]. The authors in [16] proposed using cooperative relaying for train-train communication in order to enhance the train control performance of CBTC systems.

The third way considers the WCS performances from railway operator's point of view and addresses the question whether the WCS ensures the desired performance level for safety application according to the railway safety standards [17]. In this context, a single communication error can be negligible. Only communication errors that last more than a certain time and that can lead to a critical event (CE) like a collision are interesting. Therefore, it is necessary to reduce the WCS model's complexity of the second way when focusing on the railway safety and operation aspects by neglecting WCS details such as fading channel effects, resource allocation, power control, etc. However, the WCS modeling in this third way is more aided than in the first way by taking into account numerous channel features such as transfer delay, loss connection rate, reconnection procedure, handover occurrence rate, handover execution time, etc. The authors in [18] presented a stochastic Petri net (SPN) model for ETCS real-time communication system in order to investigate the impact of train head-to-head distance on the train stopping probability. The proposed discrete event model corresponds to a simplified model of transmission error and recover behavior of the real-time WCS of the ETCS. In [19], authors used stochastic automation networks to model CBTC systems in order to examine the impact of the time interval between two consecutive trains on the probability to trigger the emergency braking of the train behind. A SPN simulation-based approach for the dependability analysis of an LTE-based WCS in CBTC application is presented in [20]. Nevertheless, the efficiency of these above articles, which are based on modeling and simulations, i.e., the ratio between the result accuracy and the execution time, is an issue. Therefore, an analytical treatment is recommended.

The authors in [21] presented an analytical estimation for evaluating the probability of train emergency stopping due to Global System for Mobile Communications Railway (GSM-R) communication errors in ETCS. The communication delays were analyzed in more details in [22]. However, these two studies are only based on the bit error rate (BER) analysis. This value does not take into account any perturbing effects caused by interferences or cell handovers as presented in [23]. In addition, these studies only consider the occurrence rate of communication errors during a long operating time but do not consider the duration of errors. For a TCS, the duration of communication errors is essential in terms of safety because a CE (an emergency braking for example) can occur when consecutive messages are missed for more than a fixed time interval. In [24], a new analytical analysis that examines the duration of every principal error types of the WCS, was proposed. Based on the previous work, we develop an analytical process in this paper. This allows us to analyze the impact of wireless communication errors on the TCS and then to evaluate the occurrence probability of the CE in braking control applications. The contribution of this paper is to develop a methodology from the railway operator's point of view that allows us (1) to analyze and to evaluate communication errors that lead to the CE when no valid position message is received by the train control center (TCC) for more than a certain time, and (2) to calculate the occurrence probability of this CE. This methodology could be applied in general to different communication technologies, such as GSM-R, WLAN, or LTE by considering the corresponding transmission procedure and appropriate parameters.

The paper is structured as follows: in Section II, we will describe the problem statement and formalize the performance parameters of the WCS. The proposed analytical approach that integrates the principal communication errors degrading CBTC services, will be presented in Section III. Then, the case study dedicated to LTE technology, its modeling and the model simulations are summarized in Section IV. An evaluation process based on the analytical approach will be proposed in Section IV-C. The process accuracy will also be proved by comparing its results with those of a simulated PN model in this subsection. Finally, Section V will present the conclusions and the further research works.

II. Problem Statement and Model Formulation

A. Requirements of Train Ground Communication for TCS

Focusing on railway control commands, the expected requirements for a WCS are categorized into two groups according to following applications:

1) High-speed railway applications: In Europe, the requirements for a WCS linked to ERTMS are defined in numerous documents (e.g., [25][1]).
2) Urban guided transport applications: The standard IEEE 1474 provides operational and safety requirements of CBTC and mentions general requirements of performance data related to a communication system. However, these requirements could not be directly applied for construction of communication system. To our knowledge, each transport operator group defines its own needs for a specific project in order to design a corresponding WCS, as was done in Systuf.[2]

A summary of the requirements of train ground communication for TCS is outside the scope of this paper because in case of (1), the requirements (qualitative and quantitative) are numerous and in case of (2), the requirements are specific to every operator group and in most cases are non-public.

[1]Note that the requirements defined in this document are not fixed and will evolve according to technology evolution (this is written on the European Railway Agency website at http://www.era.europa.eu/Core-Activities/ERTMS/Pages/The-Program-Evolution-of-Railway-Radio.aspx.

[2]http://systuf.ifsttar.fr/index-en.php

B. Problem Statement

Let us consider an urban railway line equipped with an advanced TCS and assume that train 1 runs ahead of train 2. Let T_m(s) be the journey time of trains. During a journey, the position/integrity messages generated by the trains are transmitted periodically to the TTC each T_s (s). When receiving the position message of train 2, the TCC takes into account the position of train 1 and the signaling states of other trains, and then, sends back a movement authority message (MA) to train 2. A message is considered valid at the reception if and only if its transmission time does not exceed a value T_o (obsolescence deadline for a message). To ensure safety conditions when no valid position message from train 1 is received by TCC within a period of T_b (s), an emergency braking message is sent from the TCC to train 2. It corresponds to a CE that is relevant for safety and dependability evaluations. In order to evaluate the occurrence probability of this CE due to the communication errors during a train journey, the performance parameters of the LTE communication process between the train and the TCC will be examined in next subsections.

C. Performance Parameters of the Communication Process Between the Train and the TCC

1) Transmission Delay: Let D_p be the transmission delay of the packet sent by a train or by a TCC in the normal case. D_p is assumed to follow the exponential distribution with the mean value λ_p. Although this assumption seems to be too simple to take into account the up bound values of the packet delay, it is still widely used in communication systems, especially in the queuing theory. In fact, according to [26] (pp. 44–45), the assumption of exponential distribution for network delays is adequate for a number of experimental observations and applications. Then, the probability density function (pdf) of D_p is given by:

$$f_{D_p}(t) = \lambda_p \exp(-\lambda_p t). \tag{1}$$

2) Retransmission Mechanism: The goal of this paper is to propose a new methodology that could be applied in multiple different communication technologies. Therefore, we present in this section a general retransmission mechanism. When a message is sent, n_r copies are created. If the transmitter (Tx) receives ACK sent by the receiver (Rx), these copies are deleted, for example, see Fig. 1.1) when Tx receives ACK from Rx. Next, for the message 2, see Fig. 1.2), after the retransmission time, T_{RE}, if Tx does not yet receive ACK, it send another copy until all n_r copies are sent. For GSM-R and WILAN, $n_r = 0$ when we do not consider the retransmission mechanism. For LTE, we consider the Sync HARQ with $n_r = 3$. Due to temporarily bad radio signal conditions, the packet loss occurs with rate p_{ET}. The obsolescence deadline T_o includes the $n_r + 1$ versions of a message (1 original version and n_r copies). For example, see Fig. 1.2), Rx does not receive the original version and two first copies of message 2 due to packet loss errors. Next, the third copy arrives at Rx after the obsolescence deadline T_o (counted from the first sending time of the message 2), then it

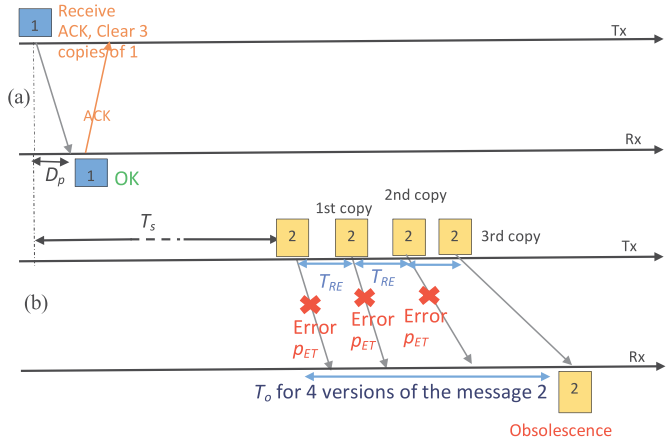

Fig. 1. Examples for the transmission and retransmission mechanisms.

is considered as an obsolescent message and does not valid for train control application.

3) Connection Loss: Let D_l be the time to the connection loss, in other words, the on-time duration of connection, and let D_{rc} be the reconnection time. D_l is assumed to follow the exponential distribution, [18]:

$$f_{D_l}(t) = \lambda_l \exp(-\lambda_l t). \tag{2}$$

The train hardware detects this state after some time-out, T_d and tries to establish a new connection with the failed reconnection probability p_f. In detail, when the reconnection duration is greater than b, the re-establishment is considered as false and then another attempt is made, [18]. The recovery time of a successful connection is assumed to follow the uniform distribution of UNIF$[a, b]$. Thus, for h reconnection with $h \in \{1, 2, \ldots, \infty\}$, the probability density function of the reconnection time is given by:

$$f_{D_{rc}}(t) = \begin{cases} 0 & t \leq a \\ (1-p_f)\frac{1}{b-a} & t \in]a, b] \\ \ldots & \\ 0 & t \in](h-1)b, (h-1)b+a] \\ (1-p_f)p_f^{(h-1)}\frac{1}{b-a} & t \in](h-1)b+a, hb]. \end{cases} \tag{3}$$

If the connection is established at the first attempt, $h = 1$, then the reconnection time, D_{rc}, belongs to the interval $[a, b]$. The probability that the connection is successful at the first attempt is $1 - p_f$. Therefore, the probability density function of the reconnection time is given by $f_{D_{rc}} = 0$ for $t \leq a$ and $f_{D_{rc}} = (1 - p_f)/(b - a)$ for $t \in]a, b]$. Next, the probability that the first attempt of reconnection is failed and the second reconnection is successful $(h = 2)$ is $(1 - p_f)p_f$. In this case, the reconnection time D_{rc}, only belongs to the interval $]b + a, 2b]$. Similarly, if the $(h - 1)$-th attempts are failed and the h-th reconnection is successful, the reconnection time D_{rc} only belongs to the interval $](h - 1)b + a, hb]$.

4) Handover Performance: Handover processes occur every time the train crosses the limit between the communication areas of two neighboring radio base stations (called eNodeB in an LTE network). When the train is operating normally, the

inter-occurrence time of handovers can be associated with one of the two assumptions that follow:

- either it can be considered as a constant, T_{Ho} (s). Then, the distribution of time D_k when handover occurs for the k-th time is:

$$F_{D_k}(t) = \delta_{\{t \geq kT_{Ho}\}} \tag{4}$$

  where $\delta_{\{\text{condition}\}} = 1$ when the condition is true and $\delta_{\{\text{condition}\}} = 0$ when the condition is false.
- or it can be considered as independent and exponentially distributed with the rate λ_{Ho} [18]. Then, the distribution of the time T_k when handover occurs for the k-th time follows the Gamma law:

$$F_{D_k}(t) = 1 - \sum_{j=0}^{k-1} \frac{(\lambda_{Ho} t)^j}{j!} \exp(-\lambda_{Ho} t). \tag{5}$$

The execution time of handovers is assumed to follow the exponential distribution with the rate λ_{eH}, [18]. Let D_{eH} be the handover delay, then its pdf is:

$$f_{D_{eH}}(t) = \lambda_{eH} \exp(-\lambda_{eH} t). \tag{6}$$

When the packet is sent during the handover processes, its transmission delay is defined by $D_{eH} + D_p$.

III. Analysis of Principal Types of Communication Errors in the TCS

For the advanced TCS, a single communication error (such as losing one packet) can be negligible. The communication error becomes important when a fixed time interval is exceeded. In other words, missing consecutive valid messages at the train or the TCC will lead to CE. Therefore, in this section, we will analyze the principal types of communication errors that can lead to missing consecutive valid messages at the receiver. In general, these errors are classified by the following types:

- Type A—loss of n consecutive messages in normal condition (without a handover process or a connection loss) where n is the minimum number of invalid messages that can lead to the CE.
- Type B—long execution time of handovers during more than T_1 s where T_1 is the minimal duration of errors that can lead to the CE.
- Type C—long timeout of connection during more than T_1 (s).
- Hybrid type, i.e., the combination between the above types. The higher the combination order between error types is, the lower the occurrence probability of this event is. Then only the combination of order 2 (i.e., combination between 2 error types) is considered in this paper:
  1) combination between packet losses and a handover.
  2) combination between packet losses and a connection loss.
  3) combination between a handover and a connection loss.

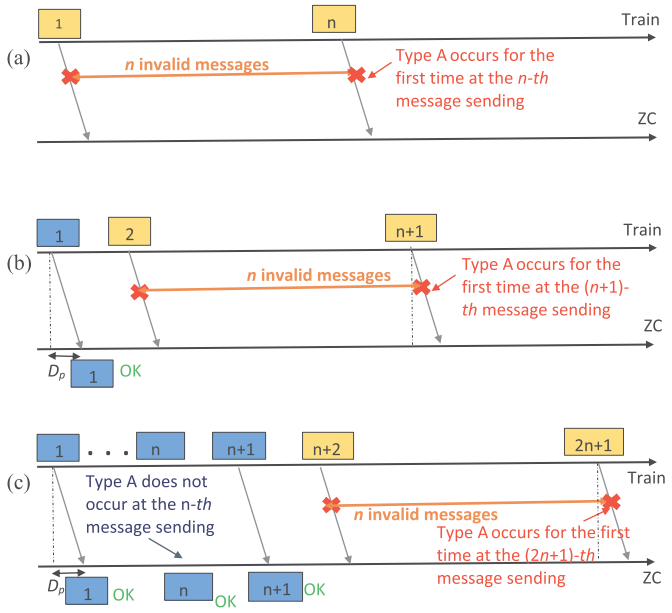

Fig. 2. Time chart of the occurrence of error Type A.

Because of the complexity, the analytical analysis for the hybrid error types is not presented in this section. It will be approximated for a particular case study in Section IV. The value of n, T_1 will also be investigated in Section IV-C.

A. Occurrence Probability of Error Type A

In this paragraph, the mathematical formulation of the probability that n consecutive valid messages cannot arrive at the receiver during normal connection will be derived. As presented in the above section, a message is considered as failed when the $n_r + 1$ packets of the retransmission mechanism are failed. In fact, during normal connection period (without connection loss or handover procedure), the packet error at the reception is caused by:

- the packet error rate, p_{ET}.
- the packet obsolescence: transmission time is more than the obsolescence deadline, T_o.

Then, the probability that the i-th packet transmission is incorrect is given by:

$$p_i = p_{ET} + \mathbb{P}\left(D_p \geq T_o - (i-1)T_{RE}\right). \tag{7}$$

As the errors of packet transmission during normal connection are independent, the probability that a message transmission is failed, p_m, is given by:

$$p_m = \prod_{i=1}^{n_r+1} \left[p_{ET} + \mathbb{P}\left(D_p \geq T_o - (i-1)T_{RE}\right)\right]. \tag{8}$$

Let Q_i be the probability that error type A occurs for the first time at the i-th message sending. It is easy to see that: $Q_i = 0$ for $i < n$ and the probability that error type A occurs at the n-th message sending, Fig. 2(a) is: $Q_n = p_m^n$.

Then, the probability that error type A occurs for the first time at the $(n+h)$-th message sending is: $Q_{n+h} = (1-p_m)p_m^n$ for $0 < h \leq n$. Indeed, we find that error type A occurs for the first time at the $(n+h)$-th message sending $(0 < h \leq n)$ if the h-th message is valid at the receiver and then, n next consecutive messages are failed, for example, $h = 1$, Fig. 2(b).

Next, considering Fig. 2(c), error type A occurs for the first time at the $(2n+1)$-th message sending if:

- the train receives the $(n+1)$-th message, then it does not receive n next consecutive messages.
- and error type A does not occur for the first time at the n-th message sending.

$$Q_{2n+1} = (1-p_m)p_m^n(1-Q_n).$$

Similarly, we have:

$$Q_{2n+2} = (1-p_m)p_m^n\left(1-\sum_{h=n}^{n+1} Q_h\right).$$

In summary, the probability that error type A occurs for the first time at the i-th message sending is given by:

$$Q_i = \begin{cases} 0 & i < n \\ p_m^n & i = n \\ (1-p_m)p_m^n & n < i \leq 2n \\ (1-p_m)p_m^n\left(1-\sum_{h=n}^{i-n-1} Q_h\right) & i \geq 2n+1. \end{cases} \quad (9)$$

Therefore, we obtain the following property:

Property 1: Let $N_m(t)$ be the number of train messages that are sent during $[0,t]$, $t > T_s$, $N_m(t) = \text{int}[t/T_s]$ where $\text{int}[x]$ is the integer part of x; and let D_A be the occurrence time of error type A. The probability that error type A occurs during $[0,t]$ can be calculated by:

$$\mathbb{P}(D_A \leq t) = \sum_{i=n}^{N_m(t)} Q_i \quad (10)$$

where Q_i is defined by the (9).

B. Distribution Function of Error Type B

Error type B can only occur during handover process. Let D_B be the first time occurrence of error type B then D_B is always greater than T_1. It is easy to see that:

$$\mathbb{P}(D_B \leq t) = 0 \quad \forall t < T_1.$$

It remains to calculate $F_B(t) = \mathbb{P}(D_B \leq t)$ for $t \geq T_1$. As the occurrence times of handover are totally independent of the time when the previous handover process finishes, the probability that error type B occurs for the first time during the k-th handover process at t is:

$$F_{B_k}(t) = \mathbb{P}\left(D_k + T_1 \leq t, D_{eH_1} < T_1, \ldots \right. \\ \left. \ldots, D_{eH_{k-1}} < T_1, D_{eH_k} \geq T_1\right)$$

where D_k is the k-th occurrence time of handover process, defined by (4) or (5); D_{eH_k} is the execution time of the k-th handover, defined by (6). As the occurrence times of handover and their relevant execution times are independent, the $F_{B_k}(t)$ can be rewritten as:

$$F_{B_k}(t) = \mathbb{P}(D_k \leq t - T_1)(1-e^{-\lambda_{eH}T_1})^{(k-1)}e^{-\lambda_{eH}T_1}. \quad (11)$$

Finally, we obtain the following property.

Property 2: The probability that at t, $t > T_1$, the handover execution time is more than a certain time, T_1 (s), which is the distribution function of error type B, is given by:

$$F_B(t) = \sum_{k=1}^{\infty} \mathbb{P}(D_k \leq t-T_1)(1-e^{-\lambda_{eH}T_1})^{(k-1)}e^{-\lambda_{eH}T_1} \quad (12)$$

where $\mathbb{P}(D_k \leq t - T_1)$ is calculated by (4) or (5).

C. Distribution Function of Error Type C

Recall that:

- $D_{l_1}, \ldots, D_{l_k}$ are i.i.d. following $(\mathcal{E}(\lambda_l))$, they are the durations associated to connection losses.
- $D_{oc_1}, \ldots, D_{oc_k}$ are the out-time durations of connection where $D_{oc_k} = D_{rc_k} + T_d$ given that D_{rc_k} are i.i.d. following $(f_{D_{rc}}(t))$ and is the time to reconnection and that T_d is the time to detect the timeout.

$$(D_{l_k})_{k\geq 1} \text{ and } (D_{rc_k})_{k\geq 1} \text{ are independent.}$$

Let D_C be the first time occurrence of error type C. Similarly to case B, we have: $\mathbb{P}(D_C \leq t) = 0$, $\forall t < T_1$ and it remains to calculate:

$$F_C(t) = \mathbb{P}(D_C \leq t) \text{ for } t \geq T_1.$$

If D_{oc_k} is the first out-time duration which is longer than T_1 then:

$$D_C = (D_{l_1}+D_{oc_1}) + \cdots + \left(D_{l_{k-1}}+D_{oc_{k-1}}\right) + D_{l_k} + T_1. \quad (13)$$

The probability that error type C occurs at t is given by:

$$F_C(t) = \sum_{k=1}^{\infty} F_{C_k}(t)$$

where

$$F_{C_k}(t) = \mathbb{P}\left(D_C \leq t, D_{oc_1} < T_1, \ldots, D_{oc_{k-1}} < T_1, D_{oc_k} \geq T_1\right).$$

Because $(D_{l_k})_{k\geq 1}$ are i.i.d. with exponential distribution following $\mathcal{E}(\lambda_l)$, the random variable $D_{l_1} + \cdots + D_{l_k}$ is Gamma-distributed with parameters (k, λ_l). Furthermore as $(D_{l_k})_{k\geq 1}$ and $(D_{oc_k})_{k\geq 1}$ are independent, it implies that in (13), we

can replace the sum $D_{l_1} + \cdots + D_{l_k}$ by a random variable $W_k \sim \Gamma(k, \lambda_l)$. Hence we obtain:

$$F_{C_k}(t) = \mathbb{P}\left(W_k + D_{oc_1} + \cdots + D_{oc_{k-1}} + T_1 \leq t, \right.$$
$$\left. D_{oc_1} < T_1, \ldots, D_{oc_{k-1}} < T_1, D_{oc_k} \geq T_1\right)$$
$$= \mathbb{E}\left(F_{W_k}\left(t - T_1 - \sum_{i=1}^{k-1} D_{oc_i}\right)\right.$$
$$\left. \cdot \delta_{\{D_{oc_1} < T_1\}} \cdots . \delta_{\{D_{oc_{k-1}} < T_1\}} \delta_{\{D_{oc_k} \geq T_1\}}\right)$$

where F_{W_k} is the c.d.f. of W_k.

Property 3: The distribution function of error type C when the time of connection is more than a certain time T_1 is written by $\sum_{k=1}^{\infty} F_{C_k}$

$$F_{C_k}(t) = \int_0^{T_{1C}} \cdots \int_0^{T_{1C}} F_{W_k}(\cdot) d_{D_{rc_1}} \ldots d_{D_{rc_{k-1}}}$$
$$\cdot \int_{T_{1C}}^{\infty} f_{D_{rc}}(u_k) du_k \quad (14)$$

where $f_{D_{rc}}(t)$ is defined in (3), $T_{1C} = T_1 - T_d$, and $F_{W_k}(\cdot) = F_{W_k}(t - T_1 - \sum_{i=1}^{k-1} D_{oc_i})$, given that:

$$F_{W_k}(t) = 1 - \sum_{j=0}^{k-1} \frac{(\lambda_l t)^j}{j!} \exp(-\lambda_l t) \text{ for } t \geq T_1 + (k-1)T_d.$$

IV. Comparison Between Analytical Approach and Simulation Approach: Validation on a Case Study

In the previous section, we derive three properties for evaluating the occurrence probabilities of the principal communication error types. In this section, using these properties, we calculate the occurrence probability of the CE, e.g., "*sending an emergency braking message from TCC to train 2*" due to communication errors between the TCC and train 1. This is a probability related to the T_b value mentioned in Section I. We will firstly describe the case study in Section IV-A. Next, the simulation approach (PN here) will be is briefly in Section IV-B. Finally, the analytical process will be performed (by Matlab) in order to evaluate the CE probability occurrence in Section IV-C. We also compare the results obtained by every step of the analytical process to the ones obtained by the PN simulation to verify their accuracy.

Note that the mathematical formulas in Section IV-C could be evaluated by any numerical computing environment, such as Matlab, R, C++, etc. In this paper, we use Matlab. On the other hand, according to standard IEC 61508-part 6 (page 76), the PN based on Monte Carlo simulation is an efficient method for modeling dynamic system. Therefore, we believe that a comparison with a PN simulation tool (of GRIF platform) is enough to highlight the performance of the proposed approach, which is totally independent of the PN simulation. In fact, our analytical approach is not time-consuming. It allows us to avoid the simulation execution time and to obtain results as good as the one of the classic PN simulation. The difference between analytical result (AR) and simulation result (SR) is quantitatively evaluated by the relative error, ϵ_r:

$$\epsilon_r = \frac{|AR - SR|}{SR}. \quad (15)$$

TABLE I
Input Parameters for the Case Study

Connection loss & Transmission delay	λ_l	p_f	λ_p
	1E-4/h$^{(1)}$	0.001$^{(1)}$	200 $^{(2)}$
Obsolescence deadline & Handover	T_o	m_{eH}	T_{Ho}
	0.05 s $^{(5)}$	0.05 s$^{(4)}$	10 s $^{(5)}$
Retransmission	T_{ACK}	T_{RE}	p_{ET}
	4 ms$^{(3)}$	8 ms$^{(3)}$	0.1$^{(3)}$
Reconnection delay	a	b	T_d
	0 s$^{(1)}$	7.5 s$^{(1)}$	1$^{(1)}$

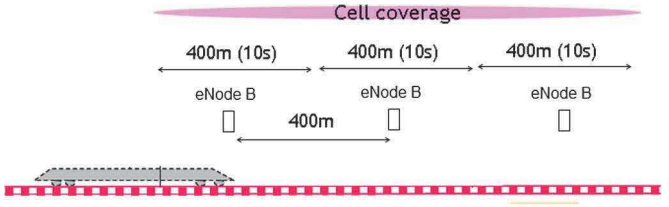

Fig. 3. Distribution of eNode-B along the urban railway line.

A. Description of the Case Study

Considering the train's journey time, $T_m = 3600$ s (average journey duration of urban train, [23]). Several values of T_s, the interval time between two consecutive position message sending of the train, are chosen in the context of CBTC systems (in the SYSTUF project[3]), $T_s \in [0.2, 0.6]$ s. Note that these values are very low compared to the value of 5 s mentioned in ETCS requirements. This is due to the continuous monitoring requirements for the Mass Transit system—CBTC, aiming to enforce train speed profiles, headway and dwell times, [4]. As LTE technology is considered as the final answer-piece in the puzzle to the convergence prospect between ETCS and CBTC systems, our case study is dedicated to a simple example of LTE-based TCS, and furthermore the parameter values in both reference sections of ETCS and CBTC can be inherited, given in Table I.

Note that the input parameters are chosen$^{(1)}$ based on [18],$^{(2)}$ based on [9] (mean transfer delay for a message of 500 bytes is about 5 ms),$^{(3)}$ based on [27],$^{(4)}$ based on [28] with the assumption that the target cell is already known,$^{(5)}$ arbitrarily but try to come close to reality.[4] In fact, Fig. 3 presents the considered distribution of the eNodeB along the urban railway line. As the distance between two eNodeB is fixed and also the relevant velocity parameters of the train are specified in advance, then the occurrence time of the handover could be considered as constant, T_{Ho} s for a given radio planning.

[3]http://systuf.ifsttar.fr/index-en.php
[4]Project SYSTUF.

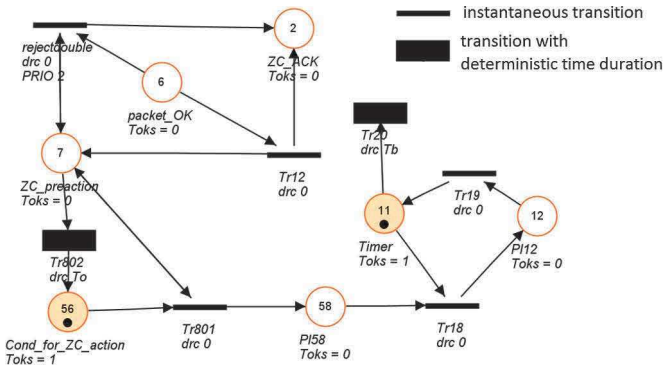

Fig. 4. PN structure for the ZC operation model.

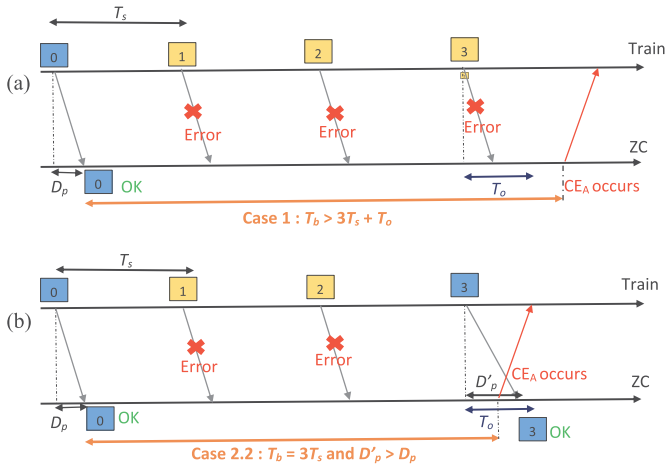

Fig. 5. Missing consecutive valid messages for more than T_b s due to communication error Type A.

B. Modeling and Simulation Approach Applied to the Case Study

Petri net (PN) is a graphical and mathematical formalism for modeling discrete event systems with time-dependent behaviors and is widely employed to model complex systems, [29]. Simulation of PN models is a common technique to perform dependability assessments.

In this paper, we propose to use the PN module of the software platform GRIF[5] for evaluating the occurrence probability of the CE. In detail, SPN with predicates and assertions are used to model the CBTC system based on the LTE technology. Note that in the CBTC system, the TCS is normally called zone controller (ZC). For quantitative evaluation, a high-speed Monte Carlo simulation engine (MOCA-RP) is used.

The CBTC system is modeled with 4 sub-nets describing:

1) handover procedure
2) re-connection procedure
3) transmission and re-transmission procedure
4) Zone controller (ZC) operation.

The sub-nets modeling procedures 1, 2, and 3 are similar to those presented in [20]. Fig. 4 presents the sub-net for modeling the ZC operation: "*sending emergency braking message*". In detail, after receiving a valid packet from the train, "*Tr12*" is triggered and the ZC sends an ACK to the train, i.e., the token in "packet_OK" place (num. 6) is removed and another is created in "ZC_ACK" place (num. 12). The ACK processing of the train is modeled in the "*transmission and re-transmission*" sub-net described in [20]. Another token simultaneously comes to the "*ZC_preaction*" place (num. 7). Within the deadline T_o of the train message, if the ZC receives another copy of this train message, these copies are rejected, i.e., the "*rejectdouble*" transition is then triggered. When a token is created in place 58, the timer (place 11 that validates the "Tr20" transition for the T_b time counting) is reset. If not, after T_b s, the ZC sends an emergency braking message to train 2 and the variable "CE" is set to true.

[5]*GRaphical Interface for reliability Forecasting*, http://grif-workshop.com/grif/petri-module/.

C. Formulation of the Analytical Approach and Discussion of the Accuracy of Its Results

1) Missing Consecutive Valid Messages for More Than T_b s Due to the Communication Error Type A: In the Section III-1, the occurrence probability of error type A (n consecutive valid messages cannot arrive at the receiver during normal connection) was evaluated. Now, in this section we will present the way to evaluate the occurrence probability of the CE caused by error type A (CE_A). This way depends on the relationship between T_b (maximum accepted duration without valid position message) and T_s (time between two position/integrity messages generated by the train). In detail, the occurrence probability of CE_A will be evaluated in the following two cases (where n is an integer such as $n = \text{int}\,[T_b/T_s]$):

1) $\mathbf{T_b > nT_s + T_o}$
2) $\mathbf{T_b = nT_s}$.

As T_o is very small, it is not necessary to consider the case $\mathbf{nT_s < T_b < nT_s + T_o}$. This case can be considered as the case $\mathbf{T_b = nT_s}$.

In the first case when $\mathbf{T_b > nT_s + T_o}$ (cf. case 1) in Fig. 5 where $n = 3$), the CE occurs when n consecutive messages are invalid. In this case the pdf of the CE_A is given by (9).

In the second case when $\mathbf{T_b = nT_s}$, the CE_A will occur if:

1) n consecutive messages are invalid (similar to the first case), or
2) only $(n-1)$ consecutive messages are invalid with the condition that the transmission delay of the n-th message, D'_p, is superior to the transmission delay D_p of the message 0. The message 0 is the last valid message that arrives at the ZC before the missing consecutive messages, (cf. case 2) in Fig. 5 where $n = 3$). The probability that $D'_p > D_p$ is calculated by:

$$\mathbb{P}\left(D'_p > D_p\right) = \int_0^\infty \int_y^\infty f_{D'_p}(x)dx.f_{D_p}(y)dy$$

$$= \int_0^\infty \exp(-2\lambda_p y)\lambda_p dy = 0.5.$$

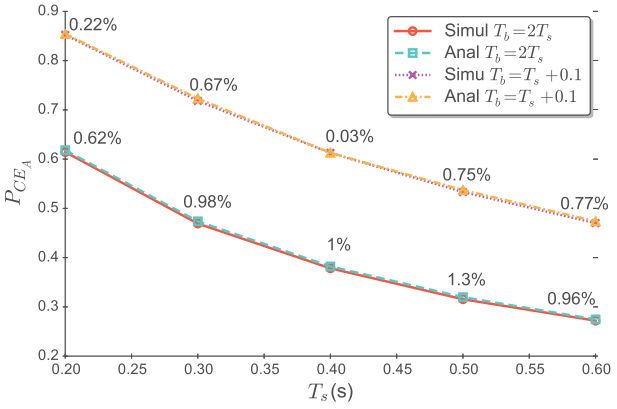

Fig. 6. Occurrence probability of error Type A according to the relationship between T_b and T_s. Note: Simul—Simulation approach; Anal—Analytical approach. The relative error between two approaches is presented by percentage numbers in the figure.

Then, the probability that CE_A occurs for the first time at the n-th message sending is given by:

$$\begin{aligned} Q_n &= \mathbb{P}\left(D'_p > D_p\right) \cdot \mathbb{P}\left(\text{only } (n-1) \text{ invalid messages}\right) \\ &\quad + \mathbb{P}\left(n \text{ invalid messages}\right) \\ &= 0.5 p_m^{n-1}(1-p_m) + p_m^n = 0.5\left(p_m^{n-1} + p_m^n\right). \end{aligned}$$

Therefore, from (9), the pdf of the CE_A (missing consecutive valid messages for more than T_b s) can be rewritten as follows:

$$Q_i = \begin{cases} 0 & i < n \\ 0.5\left(p_m^{n-1} + p_m^n\right) & i = n \\ (1-p_m)0.5\left(p_m^{n-1} + p_m^n\right) & n < i \le 2n \\ (1-p_m)0.5\left(p_m^{n-1} + p_m^n\right) & \\ \quad \times \left(1 - \sum_{h=n}^{i-n-1} Q_h\right) & i > 2n. \end{cases} \quad (16)$$

Fig. 6 compares the results between the analytical approach and the simulation approach of the occurrence probability of the CE_A (presented by the vertical axis) during a train journey when $p_{ET} = 0.1$, $T_b = T_s + 0.1$ (an example for the case $\mathbf{T_b > nT_s + T_o}$) or $T_b = 2T_s$ (an example for the case $\mathbf{T_b = nT_s}$). We find that the results for both approaches are almost the same. In fact, the ϵ_r, that is presented by percentage number according to every value point of P_{CE_A}, is smaller than 1.3% for all cases.

Then, the analytical approach is used to consider how T_b is chosen in order to limit the impact of error type A on the CE during a train journey. It means that T_b is investigated such as $\mathbb{P}_{CE_A}(1\ h) \le 1E-5$. Table II presents the occurrence probability of the CE_A according to every value of T_s, p_{ET}, T_b. All probability values are indicated in the second line of each row corresponding to a value of p_{ET}. Hereunder are two examples taken from Table II:

1) for $T_s = 0.2$ and $p_{ET} = 0.1$, the occurrence probability of CE_A can be negligible when $T_b \ge 0.7$.
2) for $T_s = 0.2$ and $p_{ET} = 0.4$, the occurrence probability of CE_A can be negligible when $T_b \ge 1.3$.

2) Missing Consecutive Valid Messages for More Than T_b s Due to the Communication Error Type B: Let message 0 be the last valid message that arrives at the ZC before the handover occurrence. Similarly to the previous subsection, the occurrence probability of the CE caused by error type B, CE_B will be evaluated in two cases.

TABLE II
CHOOSING T_b ACCORDING TO T_s AND p_{ET} IN ORDER TO LIMIT THE OCCURRENCE PROBABILITY OF CE_A

T_s	0.2	0.3	0.4	0.5	0.6
p_{ET} = 0.1	$T_b = 0.7$ 2.2E-8	$T_b = 1$ 1.5 E-8	$T_b = 1.3$ 1.1E-8	$T_b = 1.6$ 8.8E-9	$T_b = 1.9$ 7.3E-9
p_{ET} = 0.4	$T_b = 1.3$ 5.5E-6	$T_b = 1.9$ 3.6E-6	$T_b = 2.5$ 2.7E-6	$T_b = 3.1$ 2.2E-6	$T_b = 3.7$ 1.80E-6

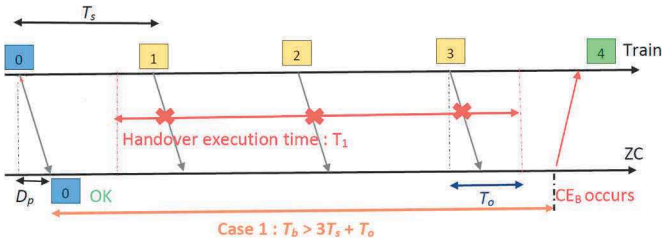

Fig. 7. Illustration of CE_B when $T_b > nT_s + T_o$.

For the first case when $\mathbf{T_b > nT_s + T_o}$ (cf. the example in Fig. 7 with $n = 3$), the CE_B occurs at the k-th handover when the execution time of the handover is more than T_1 s. T_1 is given by:

$$T_1 = \begin{cases} (n-1)T_s + T_o + \left(\text{int}\left[\frac{D_k}{T_s}\right] + 1\right) T_s - D_k; & \\ \qquad\qquad \text{when mod}\left(\frac{D_k}{T_s}\right) > 0 & \\ (n-1)T_s + T_o; \quad \text{when mod}\left(\frac{D_k}{T_s}\right) = 0 & \end{cases} \quad (17)$$

where $n = \text{int}\left[T_b/T_s\right]$, D_k is the occurrence time of the k-th handover, $\text{mod}(D_k/T_s)$ is the remainder when we divide D_k by T_s.

Then, from (11), the probability of the CE_B occurs for the first time at the k-th handover when $\mathbf{T_b > nT_s + T_o}$ is given by:

$$\mathbb{P}(CE_{Bk}) = \delta_{(D_k \le t - T_b)}(1 - e^{-\lambda_{eH} T_1})^{(k-1)} e^{-\lambda_{eH} T_1} \quad (18)$$

where $D_k = kT_{Ho}$ when the time interval T_{Ho} between two handover occurrences is assumed to be constant.

For the second case when $\mathbf{T_b = nT_s}$, the CE_B occurs for the first time at the k-th handover when:

1) the execution time of the handover is more than T_1, given by (17).
2) or the execution time of the handover is more than $T'_1 = [T_1 - Ts]^+$ (where $[x]^+ = \max[0, x]$) and the transmission delay of the n-th message, D'_p is superior to the transmission delay D_p of the message 0. (Fig. 8 when $n = 3$).

Then, when $\mathbf{T_b = nT_s}$, the probability that CE_B occurs for the first time at the k-th handover is given by:

$$\mathbb{P}(CE_{Bk}) = \delta_{(D_k \le t - T_b)} \left[1 - \sum_{i=1}^{k-1} \mathbb{P}(CE_{Bi})\right] \cdot \left[\mathbb{P}(D_{eH} > T_1) + 0.5\mathbb{P}\left(T'_1 \le D_{eH} \le T_1\right)\right]. \quad (19)$$

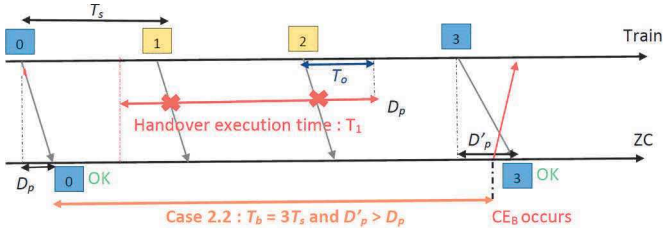

Fig. 8. Illustration of CE_B when $T_b = nT_s$.

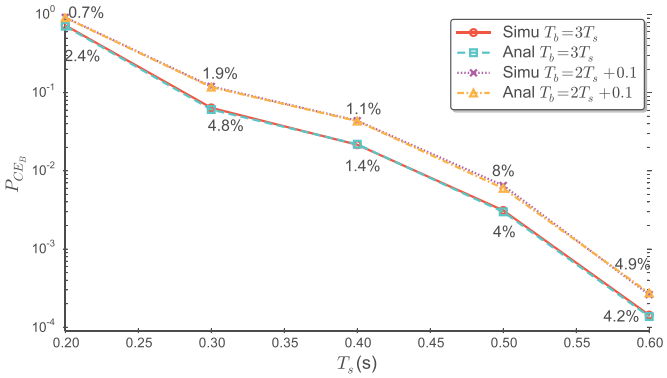

Fig. 9. Occurrence probability of error Type B according to the relationship between T_b and T_s. Note: Simul—Simulation approach; Anal—Analytical approach. The relative error between two approaches is presented by percentage numbers in the figure.

TABLE III
CHOOSING T_b ACCORDING TO T_s AND m_{eH} IN ORDER TO LIMIT THE OCCURRENCE PROBABILITY OF CE_B

T_s	0.2	0.3	0.4	0.5	0.6
m_{eH} = 0.05	$T_b = 1.2$ 7.6E-6	$T_b = 1.3$ 7.7E-7	$T_b = 1.6$ 7.4E-6	T_b =1.6 2.7E-7	T_b =1.9 1.7E-9
m_{eH} = 0.096	$T_b = 2$ 6.9E-6	$T_b = 2.1$ 9E-6	$T_b = 2.4$ 6.3E-6	$T_b = 2.6$ 1.9E-7	$T_b = 2.5$ 5.8E-7

Fig. 9 compares the results between the analytical approach and the simulation approach of the occurrence probability of the CE_B (presented by the vertical axis) during a train journey when $T_b = 2T_s + 0.1$ (an example for the case $\mathbf{T_b > nT_s + T_o}$) and $T_b = 3T_s$ (an example for the case $\mathbf{T_b = nT_s}$). We find that the results of two approaches are almost the same. In fact, the ϵ_r, that is presented by percentage number according to every value point of P_{CE_B}, is not important. In the worst case, when $P_{CE_B} < 0.005$, then $\epsilon_r < 5\%$ of P_{CE_B} obtained by the simulation approach.

Then, the analytical approach is applied to evaluate the occurrence probability of rare events in order to consider for which value of T_b, the impact of error Type B during a train journey can be negligible ($\mathbb{P}_{CE_B}(1\ h) \leq 1E-5$). Hereunder are two examples taken from Table III that has the same presentation principles of Table II:

1) For $T_s = 0.2$ and $m_{eH} = 0.05$, the occurrence probability of CE_B can be negligible when $T_b \geq 1.2\ s$. CE_B can be negligible when $T_b \geq 1.8\ s$.
2) For $T_s = 0.2$ and $m_{eH} = 0.096$, the occurrence probability of CE_B can be negligible when $T_b \geq 2\ s$.

3) Missing Consecutive Valid Messages for More Than T_b s Due to the Communication Error Type C: As the connection loss rate is $10^{-4}/h$ [18], the probability that the connection loss occurs more than 2 times during a train journey is negligible. Therefore, $F_C(t)$ can be re-written as:

$$F_C(t) = F_{W_1}(t - T_1) \int_{T_{1C}}^{\infty} f_{D_{rc}}(u)du \tag{20}$$

where $T_{1C} = [T_1 - T_d]^+$; $f_{D_{rc}}(u)$ is given by (3)

$$F_{W_1}(t - T_1) = 1 - \exp\left(-\lambda_l(t - T_1)\right).$$

Similarly to the communication error Type B, the occurrence probability of the CE_C is calculated in the following two cases:

For the first case when $\mathbf{T_b > nT_s + T_o}$, CE_C occurs if the connection time-out D_{oc} is more than T_1, that is given by (17) when replacing D_k by D_l.

where D_l is the occurrence time of the l-th connection loss.

As $(n-1)T_s + T_o \leq T_1 < nT_s + T_o$, from (20), the occurrence probability of the CE_C in this case is:

$$\begin{aligned}
&\mathbb{P}_{CE_{C_{\text{inf}}}}(t) \leq \mathbb{P}_{CE_C}(t) < \mathbb{P}_{CE_{C_{\text{sup}}}}(t)\\
&\mathbb{P}_{CE_{C_{\text{inf}}}}(t) = F_{W_1}(t - T_b) \int_{T_{1C_{\text{inf}}}}^{\infty} f_{D_{rc}}(u)du\\
&\mathbb{P}_{CE_{C_{\text{sup}}}}(t) = F_{W_1}(t - T_b) \int_{T_{1C_{\text{sup}}}}^{\infty} f_{D_{rc}}(u)du
\end{aligned} \tag{21}$$

where $T_{1C_{\text{sup}}} = [(n-1)T_s + T_o - T_d]^+$, and $T_{1C_{\text{inf}}} = [nT_s + T_o - T_d]^+$.

For the second case when $\mathbf{T_b = nT_s}$, similarly to error type B, the probability that CE_C occurs during $[0, t]$ is given by:

$$\begin{aligned}
&\mathbb{P}_{CE_{C_{\text{inf}}}}(t) \leq \mathbb{P}_{CE}(t) < \mathbb{P}_{CE_{C_{\text{sup}}}}(t)\\
&\mathbb{P}_{CE_{C_{\text{inf}}}}(t) = F_{W_1}(t - T_b)\begin{bmatrix}0.5\,\mathbb{P}\left(T_{1C'_{\text{inf}}} \leq D_{rc} \leq T_{1C_{\text{inf}}}\right)\\ +\mathbb{P}\left(D_{rc} > T_{1C_{\text{inf}}}\right)\end{bmatrix}\\
&\mathbb{P}_{CE_{C_{\text{sup}}}}(t) = F_{W_1}(t - T_b)\begin{bmatrix}0.5\,\mathbb{P}\left(T_{1C'_{\text{sup}}} \leq D_{rc} \leq T_{1C_{\text{sup}}}\right)\\ +\mathbb{P}\left(D_{rc} > T_{1C_{\text{sup}}}\right)\end{bmatrix}
\end{aligned} \tag{22}$$

where $T_{1C'_{\text{inf}}} = T_{1C_{\text{inf}}} - T_s$ and $T_{1C'_{\text{sup}}} = T_{1C_{\text{sup}}} - T_s$.

Fig. 10 compares the results between the analytical approach and the simulation approach of the occurrence probability of the CE_C during a train journey, according to $T_b \in [1, 6]$ s. We find that the simulation results are between the inferior threshold ($\mathbb{P}_{EC_{C_{\text{inf}}}}$) and superior threshold ($\mathbb{P}_{EC_{C_{\text{sup}}}}$) of the analytical approach. Then, hereafter the probability that CE occurs due to error type C can be approximated by:

$$\mathbb{P}_{EC_C}(t) = \frac{\mathbb{P}_{EC_{C_{\text{inf}}}}(t) + \mathbb{P}_{EC_{C_{\text{sup}}(t)}}}{2}. \tag{23}$$

The maximal value of $\mathbb{P}_{EC_C}(t)$ during a journey is about 10^{-4}. Hence, the occurrence probability of any hybrid communication error where one error among the two is a connection loss, is always inferior to 10^{-4}. Therefore, the hybrid error where one error among the two is a connection loss can be negligible in further works.

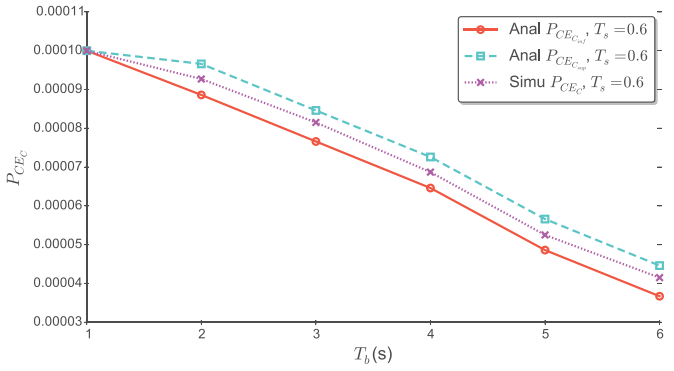

Fig. 10. Occurrence probability of error Type C according to the relationship between T_b and T_s. Note: Simul—Simulation approach; Anal—Analytical approach.

4) Missing Consecutive Valid Messages for More Than T_b s Due to the Hybrid Error "Error Type A and Error Type B": In this section, we examine the cases, in which error Type A occurs before or after the handover process, and this combination leads to missing consecutive valid messages for more than T_b (s). It is called error Type H.

Note that for this hybrid error type, we consider that the duration of handover cannot directly lead to CE as this case was presented before. So, error type A is combined with handover processes in order to have CE_H.

Similarly to other error types, the occurrence probability of error Type H is evaluated in two different cases linking T_b and T_s.

For the first case when $\mathbf{T_b > nT_s + T_o}$,

- The occurrence probability of CE_H, caused by the event that one message is invalid due to error type A before (or after) the k-th handover, is given by:

$$\mathbb{P}_{CE_{H\_1}}(k-\text{th handover}) = 2p_m \cdot \mathbb{P}\left([T_1 - T_s]^+ \leq D_{eH} < T_1\right). \quad (24)$$

  where p_m is given by the (8) and T_1 is given by the (17).
- Similarly, the occurrence probability of CE_H, caused by the event that i messages are invalid due to error type A before (or after) the k-th handover, is given by:

$$\mathbb{P}_{CE_{H\_i}}(\cdot) = 2p_m^i \cdot \mathbb{P}\begin{pmatrix}[T_1 - i\cdot T_s]^+ \leq D_{eH} \\ < [T_1 - (i-1)T_s]^+\end{pmatrix}$$

- Hence, the occurrence probability of CE_H is given by:

$$\mathbb{P}_{CE_H}(\cdot) = \sum_{i=1}^{(n-1)} \mathbb{P}_{CE_{H\_i}}(\cdot). \quad (25)$$

We find that

$$\frac{\mathbb{P}_{CE_{H\_1}}(\cdot)}{\mathbb{P}_{CE_{H\_i}}(\cdot)} = \frac{\exp\left(-\lambda_{eH}\cdot(i-1)T_s\right)}{p_m^{i-1}}.$$

When $(\mathbb{P}_{CE_{H\_1}}(\cdot))/(\mathbb{P}_{CE_{H\_i}}(\cdot)) \gg 1$, the $\mathbb{P}_{CE_H}$ can be approximated by the $\mathbb{P}_{CE_{H\_1}}$.

For the second case when $\mathbf{T_b = nT_s}$,

- The occurrence probability of CE_H, caused by the event that one message is invalid due to error type A before (or after) the k-th handover, is given by:

$$\begin{aligned}&\mathbb{P}_{CE_{H\_1}}(\cdot)\\ &= 2p_m \cdot \begin{pmatrix}\mathbb{P}\left(D_p > D'_p\right)\mathbb{P}(T_{1\_s1} \leq D_{eH} < T_1)\\ +\mathbb{P}\left(D_p \leq D'_p\right)\mathbb{P}(T_{1\_s2} < D_{eH} < T_{1\_s1})\end{pmatrix}\\ &= p_m \cdot \begin{pmatrix}\mathbb{P}(T_{1\_s1} \leq D_{eH} < T_1)\\ +\mathbb{P}(T_{1\_s2} < D_{eH} < T_{1\_s1})\end{pmatrix}\\ &= p_m \cdot \mathbb{P}(T_{1\_s2} \leq D_{eH} < T_1) \quad (26)\end{aligned}$$

  where p_m is given by (8), T_1 is given by (17), and $T_{1\_si} = [T_1 - i\cdot T_s]^+$.
- Similar to the first case, the occurrence probability of CE_H could be approximatively by CE_{H_1}.

5) Analytical Process for Evaluating the Occurrence Probability of CE During the Mission Time:

Input: T_b, T_s, T_o, T_m and all parameters characterized the WCS performance $(\lambda_l, \lambda_p, \lambda_{eH}, p_f, a, b, T_d, T_{Ho}, T_{RE}, p_{ET})$.
Output: Probability that CE occurs during the mission time (T_m) of the train, $\mathbb{P}_{CE}(T_m)$

Initialisation: $i = 1$

1: Evaluate the probability $\mathbb{P}_{CE_1}$, that CE occurs for the first time before the first handover.
  Evaluate $\mathbb{P}_{CE_A}(t \leq T_{Ho})$ by
    Eq. (9) **if** $T_b > nT_s + T_o$
    Eq. (16) **if** $T_b = nT_s$
  Evaluate $\mathbb{P}_{CE_C}(t \leq T_{Ho})$ by
    Eq. (21) & Eq. (23) **if** $T_b > nT_s + T_o$
    Eq. (22) & Eq. (23) **if** $T_b = nT_s$

$$\mathbb{P}_{CE_1} = \mathbb{P}_{CE_A}(t \leq T_{Ho}) + \mathbb{P}_{CE_C}(t \leq T_{Ho}).$$

LOOP Process

2: **for** $i = 2$ to int $[(T_m - T_b)/T_{H_o}]$ **do**
3: Evaluate the probability $\bar{\mathbb{P}}_{CE}$ that CE does not occur yet until the i-th handover.

$$\bar{\mathbb{P}}_{CE_i} = 1 - \sum_{j=0}^{i-1} \mathbb{P}_{CE_j}$$

4: Evaluate $\mathbb{P}_{CE_A}((i-1)T_{Ho} < t \leq iT_{Ho})$ by
    Eq. (9) **if** $T_b > nT_s + T_o$
    Eq. (16) **if** $T_b = nT_s$
5: Evaluate $\mathbb{P}_{CE_C}((i-1)T_{Ho} < t \leq iT_{Ho})$ by
    Eq. (21) **if** $T_b > nT_s + T_o$
    Eq. (22) $T_b = nT_s$
6: Evaluate $\mathbb{P}_{CE_B}((i-1)T_{Ho} < t \leq iT_{Ho})$ by

$$\delta_{\{t \geq T_{Ho}+T_b\}}\mathbb{P}(D_{eH} > T_1) \text{ if } T_b > nT_s + T_o$$

$$\delta_{\{t \geq T_{Ho}+T_b\}}\left[\mathbb{P}(D_{eH} > T_1) + 0.5\,\mathbb{P}\left(T'_1 \leq D_{eH} \leq T_1\right)\right] \text{ if } T_b = nT_s$$

7: Evaluate $\mathbb{P}_{CE_H}((i-1)T_{Ho} < t \leq iT_{Ho})$ by
    Eq. (24) **if** $T_b > nT_s + T_o$
    Eq. (26) **if** $T_b = nT_s$

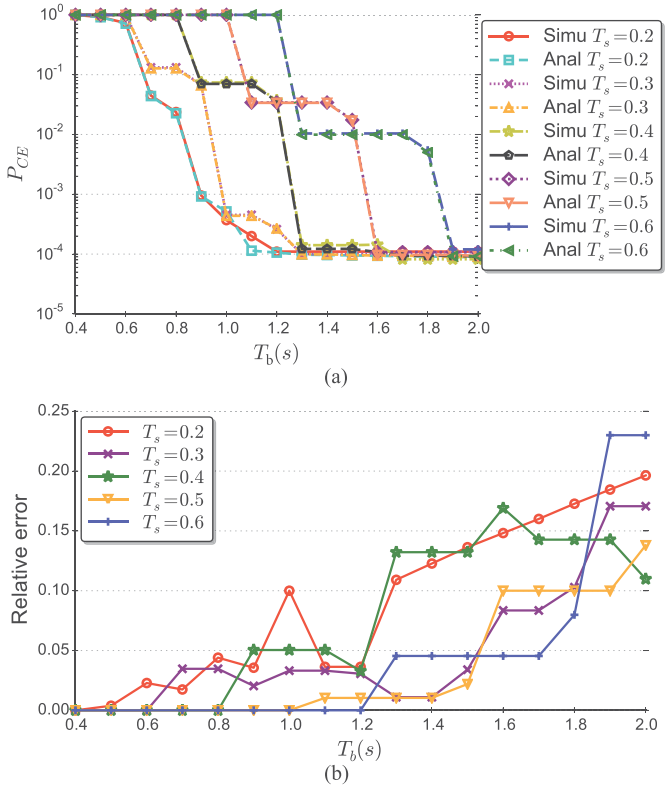

Fig. 11. Comparison between analytical and simulation results of P_{CE}. Note: Simul—Simulation approach; Anal—Analytical approach. (a) Occurrence probability of the CE according to T_b. (b) Relative error between analytical and simulation results.

8: Evaluate the probability $\mathbb{P}_{CE_i}$, that CE occurs for the first time during $](i-1)T_{Ho}, iT_{Ho}]$.

$$\mathbb{P}_{CE_i} = \bar{\mathbb{P}}_{CE_i}\left(\mathbb{P}_{CE_A}(\cdot) + \mathbb{P}_{CE_C}(\cdot) + \mathbb{P}_{CE_B}(\cdot) + \mathbb{P}_{CE_H}(\cdot)\right)$$

9: **end for**

10: Evaluate the probability that CE occurs during the mission time T_m

$$\mathbb{P}_{CE}(T_m) = \sum_{i=1}^{\text{int}\left[\frac{T_m - T_b}{T_{Ho}}\right]} \mathbb{P}_{CE_i}$$

11: **return** $\mathbb{P}_{CE}(T_m)$

Fig. 11 presents the simulation results and the analytical results for the occurrence probability of the CE during a train journey according to T_b. We find that for the case study, the analytical approach gives close results compared to the results of the simulation approach [see Fig. 11(a)]. However, for the small value of P_{CE} ($P_{CE} \cong 1E-4$), the relative error is quite significant $0.2 < \epsilon_r < 0.25$ [see Fig. 11(b)] because of the simulation approach's defect when evaluating the small probabilities. In fact, considering only 10^6 scenarios, the simulation approach cannot give the results within 12 h, for example when $T_s = 0.3$ s and $T_b > 1.2$ s. Therefore, for small probabilities, the analytical approach is more powerful. And based on the analytical approach result, we find that when T_b is large enough compared to T_s, the impact of error type A, B, and H can be negligible. For example when $T_s = 0.6$ s and $T_b = 2$ s, the occurrence probability of the CE strictly depends on error type C: "*connection loss*", $P_{CE}(= 9.25E-5) \simeq P_{CE_C}(= 9.27E-5)$. Moreover, considering Fig. 10, the decreasing of P_{CE_C} is not important according to T_b. Therefore, when $T_b = 2$ s, it is not necessary to increase T_b in order to reduce the occurrence probability of CE.

V. Conclusion

In this paper, we proposed a new analytical analysis to evaluate the consequences on safety level of the wireless communication errors in train control application. In detail, three principal error types, which lead to consecutive invalid messages, such as packet error rate, long handover execution time, and connection loss, were analyzed. The new analytical approach was developed to evaluate the occurrence probability of CE: "*missing invalid consecutive messages sent from the train to the zone controller for more than* T_b s"; where T_b is the waiting time before sending an emergency braking message from the TCC to the train behind. When comparing the new approach with the simulation approach based on a Petri net model, we obtained the same results. Furthermore, the efficiency and the robustness of our analytical approach were highlighted in the cases of small probabilities of CE when the accuracy of the simulation approach and its execution time cannot meet user requirements due to its approximate statistic calculations. Considering the case study of the LTE-based CBTC system, our approach was applied to identify the appropriate threshold of the waiting time, T_b, in order to limit the occurrence probabilities of the CE according to every error type.

The analytical results presented in this paper constitute the prerequisite to analyze the RAMS parameters of the WCS in train control application. In order to ensure the desired level of performance for the safety application (CBTC here), according to the V-model of the product life-cycle presented in the EN 50126 standard, a new system (LTE-based communication system in this case) is not only evaluated and tested in the last phases after the complete development but also in the early design phases. Indeed, following the studies of [10], [11] corresponding to every proposed configuration (or architecture) of the LTE-based communication system, the performance parameters of the communication system (such as packet delay, packet error rate, communication loss rate, etc) can be obtained by OPNET simulation. Then, using these parameters as inputs, the analytical approach proposed in this paper can examine whether the studied system is able to guarantee a given level of performance (an acceptable value of the probability of the critical events) or not. Moreover, our analytical approach could be applied in order to identify the appropriate values for communication performance parameters. Therefore, it aims to make recommendations for implementing the appropriate architecture/configuration of the LTE based CBTC system.

On the other hand, as the assumption about exponential distribution of delay packet and of handover execution time is considered as limitation of our model. It should be better to study which distribution is more appropriate to empirical data. Note that the modification of these assumptions does not

significantly affect the proposed approach. Indeed, when considering another distribution for packet delay, such as gamma or logistic distribution [7], we only re-evaluate the probability that the transmission time is more than the obsolescence deadline [in Eq. (7) of the Section III-A]. Finally, a further work could consider distance management between trains to perform the sensitivity analysis of the dependability and the safety parameters of the TCS based on WCS.

REFERENCES

[1] B. Ai *et al.*, "Challenges toward wireless communications for high-speed railway," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 5, pp. 2143–2158, Oct. 2014.

[2] J. Moreno, J. M. Riera, L. D. Haro, and C. Rodriguez, "A survey on future railway radio communications services: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 10, pp. 62–68, Oct. 2015.

[3] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for LTE and LTE-A networks," *IEEE Commun. Surveys Tut.*, vol. 16, no. 1, pp. 283–302, 1st Quart. 2014.

[4] R. Alvarez and J. Roman, "ETCS L2 and CBTC over LTE—Convergence of the radio layer in advanced train control systems," presented at the IRSE Technical Meeting, Perth, WA, Australia, Oct. 2013.

[5] B. Ai, X. Cheng, L. Yang, Z. D. Zhong, J. W. Ding, and H. Song, "Social network services for rail traffic applications," *IEEE Intell. Syst.*, vol. 29, no. 6, pp. 63–69, Nov. 2014.

[6] B. Ai *et al.*, "Future railway services-oriented mobile communications network," *IEEE Commun. Mag.*, vol. 53, no. 10, pp. 78–85, Oct. 2015.

[7] J. Xun, B. Ning, K.-P. Li, and W.-B. Zhang, "The impact of end-to-end communication delay on railway traffic flow using cellular automata model," *Transp. Res. C, Emerg. Technol.*, vol. 35, pp. 127–140, 2013.

[8] B. Bu, F. Yu, and T. Tang, "Performance improved methods for communication-based train control systems with random packet drops," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 3, pp. 1179–1192, Jun. 2014.

[9] T. Xu and T. Tang, "The modeling and analysis of Data Communication System (DCS) in Communication Based Train Control (CBTC) with Colored Petri Nets," in *Proc. 8th ISADS*, Mar. 2007, pp. 83–92.

[10] A. Sniady, J. Soler, M. Kassab, and M. Berbineau, "Ensuring ETCS data integrity in LTE," *IEEE Veh. Technol. Mag.*, vol. 11, pp. 60–70, 2016.

[11] A. Khayat, M. Kassab, M. Berbineau, M. A. Abid, and A. Belghith, "Based communication system for urban guided-transport: A QoS performance study," in *Communication Technologies for Vehicles*, ser. Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 2013, pp. 197–210, doi: 10.1007/978-3-642-37974-1_16.

[12] L. Lei *et al.*, "Stochastic delay analysis for train control services in next-generation high-speed railway communications system," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 1, pp. 48–64, Jan. 2016.

[13] L. Xiaojuan and Z. Yanpeng, "A fast handoff algorithm with high reliability and efficiency for CBTC systems," in *Proc. TMEE*, 2011, pp. 1461–1464.

[14] L. Zhu, F. R. Yu, B. Ning, and T. Tang, "Handoff performance improvements in MIMO-enabled communication-based train control systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 2, pp. 582–593, Jun. 2012.

[15] M. Cheng, X. Fang, and W. Luo, "Beamforming and positioning-assisted handover scheme for long-term evolution system in high-speed railway," *IET Commun.*, vol. 6, no. 15, pp. 2335–2340, Oct. 2012.

[16] L. Zhu, F. R. Yu, B. Ning, and T. Tang, "Communication-Based Train Control (CBTC) systems with cooperative relaying: Design and performance analysis," *IEEE Trans. Veh. Technol.*, vol. 63, no. 5, pp. 2162–2172, Jun. 2014.

[17] *Railway Applications Communication, Signalling and Processing Systems Safety Related Electronic Systems for Signalling*, CENELEC European standard (European Committee for Electrotechnical Standardization), EN 50129, 2003.

[18] A. Zimmermann and G. Hommel, "Towards modeling and evaluation of ETCS real-time communication and operation," *J. Syst. Softw.*, vol. 77, no. 1, pp. 47–54, 2005.

[19] H. Zhao, T. Xu, and T. Tang, "Towards modeling and evaluation of availability of Communication Based Train Control (CBTC) system," in *Proc. IEEE ICCTA*, Oct. 2009, pp. 860–863.

[20] K. Nguyen, J. Beugin, M. Berbineau, and M. Kassab, "Modelling communication based train control system for dependability analysis of the LTE communication network in train control application," in *Proc. EMS*, Oct. 2014, pp. 320–325.

[21] T. Babczynski and J. Magott, "Dependability and safety analysis of ETCS communication for ERTMS level 3 using performance statecharts and analytic estimation," in *Proceedings of the Ninth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX, Poland*. Cham, Switzerland: Springer International Publishing, 2014, pp. 37–46, doi: 10.1007/978-3-319-07013-1_4.

[22] T. Babczynski and J. Magott, "New analytic estimation for dependability and safety of GSM-R communication in ERTMS level 3," in *Proc. 10th Symp. FORMS*, Braunschweig, Germany, Jan. 2014, pp. 146–155.

[23] ETCS/GSM-R Quality of Service Operational Analysis EEIG ERTMS Users Group, Brussels, Belgium, Oct. 2005.

[24] K. Nguyen, J. Beugin, M. Berbineau, and M. Kassab, "Analytical approach for evaluating LTE communication errors in train control application," in *Proc. IEEE ICCW*, Jun. 2015, pp. 2369–2374.

[25] "Commission decision on the technical specification for interoperability relating to the control-command and signalling subsystem of the trans-European rail system," Official J. Eur. Union, T. E. Comm., Brussels, Belgium, Under Doc. C (2012) 172, vol. 55, Dec. 2012.

[26] E. Serpedin and Q. M. Chaudhari, *Synchronization in Wireless Sensor Networks: Parameter Estimation, Performance Benchmarks and Protocols*. New York, NY, USA: Cambridge Univ. Press, 2009.

[27] S. Kangude, "Lecture MAC—HARQ & scheduling. EETS 8316, wireless," SMU Eng., Dallas, TX, USA, 2013.

[28] L. Zhu, F. R. Yu, and B. Ning, "Availability improvement for WLAN-based train-ground communication systems in Communication-Based Train Control (CBTC)," in *Proc. IEEE 72nd VTC—Fall*, Sep. 2010, pp. 1–5.

[29] T. Murata, "Petri nets: Properties, analysis, and applications," *Proc. IEEE*, vol. 77, no. 4, pp. 541–580, Apr. 1989.

Khanh T. P. Nguyen received the B.E.E. degree from Ho Chi Minh City University of Technology, Ho Chi Minh City, Vietnam, in 2008; the M.Sc.Tech. degree in system optimization and security from University of Technology of Troyes (UTT), Troyes, France, in 2009; and the Ph.D. degree in automation and production engineering from École Centrale de Nantes, Nantes, France, in 2012.

From March 2013 to December 2015, she was a Postdoctoral Researcher with the French Institute of Science and Technology for Transport, Development and Networks (IFSTTAR). She has been part of the European project GaLoROI in the field of global-navigation-satellite-system-based solutions embedded in train control applications and the SySTUF project in the field of long-term-evolution-based wireless communication links used in communications-based train control applications. Since 2016, she has been an Assistant Professor with UTT. Her research interests include system reliability, maintenance optimization, stochastic modeling, and safety assessment of railway safety-related systems.

Julie Beugin received the B.Eng. degree from National School of Engineering in Computer Science, Automation, Mechanics and Electronics (ENSIAME), Valenciennes, France, in 2002; the M.Eng. degree in automation engineering from University of Valenciennes, Valenciennes, in 2002; and the Ph.D. degree in automation engineering in 2006.

Her Ph.D. dealt with the safety assessment of railway safety-related systems using risk concepts and reliability, availability, maintainability and safety (RAMS) evaluation methods. During these research works, she has been part of European projects in the field of urban guided transportations (UGTMS and MODUrban). Since 2007, she has been a Researcher with the French Institute of Science and Technology for Transport, Development and Networks. Her research interest is in dependability and safety evaluation of complex guided transportation systems. Part of her activities addresses RAMS demonstration issues of global-navigation-satellite-system-based solutions embedded in train control applications and were developed through the GaLoROI and the QualiSar European projects and through the Tr@in-MD project. Her recent activities address, in addition, the dependability analysis of long-term-evolution-based wireless communication links used in communications-based train control applications inside the SySTUF project.

Marion Berbineau received the M.Eng. degree in electronics, automatic and metrology from Polytech Lille, Lille, France, in 1986 and the Ph.D. degree in electronics from University of Lille, Lille, in 1989.

In 1989, she joined the French Institute of Science and Technology for Transport, Development and Networks as a Researcher in wireless telecommunications for transports. From 2002 to July 2013, she was the Director of the LEOST Laboratory. She is currently the Research Director and the Deputy Director of the Components and Systems Department that consists of 12 laboratories. She was involved in several national projects (CORRIDOR, MOCAMIMODYN, SYSTUF, and VEGAS) and European projects (MOSTRAIN, LOCOPROL, ESCORT, INTEGRAIL, BOSS, and GALOROI). She is currently involved in the ROLL2RAIL (H2020) project. She previously took part in the Global System for Mobile Communications—Railway (GSM-R) development in several European projects (MORANE) and is active as an expert in GSM-R deployment. She is an author and a coauthor of several publications and patents. Her fields of expertise are electromagnetic propagation and modeling, channel characterization and modeling for transport and complex environments particularly in tunnels, signal processing for wireless communication systems in multipath environments, multiple-input–multiple-output systems, and cognitive radio for intelligent transport systems and for railway applications including control command, video surveillance, and passenger information.

Mohamed Kassab received the B.Eng. degree in computer sciences and the M.Sc. degree in computer networks from National School of Computer Studies, Manouba, Tunisia, in 2003 and 2004, respectively, and the Ph.D. degree in computer sciences from Telecom Bretagne, Brest, France, in 2008.

From 2009 to 2013, he was a Postdoctoral Fellow with the French Institute of Science and Technology for Transport, Development and Networks. In January 2014, he joined University of Monastir, Monastir, Tunisia, as an Assistant Professor. His research interests include wireless network architecture, quality-of-service management and mobility management in wireless networks, machine-to-machine communication, and software-defined networks. He is particularly interested in the study of these issues in transportation contexts.