To cite this version :

Application of fuzzy theory for identifying the required availability of an autonomous localization unit in European Train Control System

Khanh T. P. Nguyen[a] , Julie Beugin[b], Marion Berbineau[b], and Juliette Marais[b]

[a]Toulouse INP, LGP, Tarbes, France; [b]University Lille Nord De France, IFSTTAR, COSYS, Villeneuve-d'Ascq, France

ABSTRACT

According to the evolution tendency of the control decision process from a trackside to a train-borne system, various autonomous localization units for railway vehicles were developed. As recommended in railway standards, the design process of each system, here the autonomous localization units (LU), follows the V-model whose first step is to define its availability requirement in order to satisfy the global ETCS system requirements. The classical approach for assigning the subsystem availability is based on the assumption that failure parameters of other units are precisely known. This assumption is too restricted in reality due to the lack of information. In this paper, we propose a new approach that allows taking into account uncertainties in the dependability parameters of the ETCS components for identifying the upper threshold of the LU unavailability to reach ETCS availability requirements. Using fuzzy fault trees, the fuzzy unavailability of the ETCS without the autonomous LU is evaluated. Then, based on its membership function, we assess the satisfaction rate that an advanced ETCS with the autonomous LU can satisfy the ETCS availability target.

Introduction

The European Train Control System (ETCS) is designed to supervise train traffic and to ensure that a train does not travel further than a permitted place and does not exceed an allowed speed. For ETCS level 1 and level 2, the train integrity and the train localization or detection generally relies on trackside components such as: balises, track circuit or axle counters (Flammini, 2006). However, these methods lead to high maintenance costs and expensive investment costs for infrastructure deployment. In recent years, the evolution of the control process from a trackside to a train-borne system is a promising solution to solve this issue. Thus with the localization entirely performed onboard, no trackside infrastructure installation are required, and the onboard system's maintenance can be easily done during the frequent checks of the train, the maintenance and infrastructure costs can be reduced. In addition, such autonomous localization unit (LU) makes the train more intelligent. Indeed, as the localization can be more accurate and continuous, it can serve to perform several functions timely and autonomously, such as door opens,

lighting and speed limit controls, etc. In particular, what is the most beneficial with the improvement of the localization properties by an embedded equipment is the possibility to augment traffic capacity. The reason is that train movements will be no more constrained by trackside fixed installations that, currently, separate trains with long safety buffer. Thus, the autonomous LU becomes an important key for train fluidity and network rentability, especially for secondary networks. Therefore, to obtain an advanced ETCS, no more track circuits or axle counters will be necessary for the localization of the trains (Liefferinge & Paties, 2015) and the autonomous LU becomes an important key. Benefiting from the advantage of worldwide coverage of the Global Navigation Satellite System (GNSS), numerous research projects aimed at employing satellite-based autonomous localization into ETCS [GRAIL-2 (Marradi et al., 2012), EATS (Arrizabalaga et al., 2014), GaLoROI (Manz et al., 2015)].

The development process of new devices and especially the autonomous LU dedicated to safety operations requires the dependability parameters to be evaluated according to the European railway

standards: EN 50126-1,2, EN 50128, and EN 50129. These activities strive to assure the quality of the service delivered by the equipment. In fact, it is necessary to ensure that the autonomous LU availability permit to attain the desired overall ETCS availability. The two general methods that are widely used for this process are the "bottom-up" evaluation and the "top-down" apportionment approaches. For the "bottom-up" approach, the expected reliability and maintainability data of individual components are used to predict the overall system availability (Nguyen, Beugin, & Marais, 2013; Nguyen, Beugin, & Marais, 2015). This predicted value is compared to the requirement, and then the system design is adjusted if necessary to reach the goal. One of the principal drawbacks of this approach is the need for detailed information on the system, component data, and dynamic behaviors. This information is acquired with difficulty and often unknown in the development phase of a new system. These aspects are rather measured in the test phase. Therefore, in the development phase, the apportionment approach, which is a process where dependability requirements of a system are divided among the various subsystems, is preferred. However, for a large complex system when mutual effects between component operations exist, the availability goal cannot be decomposed straightforwardly from the overall system to subsystems (Qiu, Sallak, Schön, & Cherfi-Boulanger, 2014). Therefore, a hybrid approach that combines "bottom-up" and "top-down" evaluations is proposed in this paper. Furthermore, for handling the lack of information about component dependability parameters, we propose to use fuzzy numbers to characterize the parametric uncertainties.

This article is structured as follows: Firstly, we describe the ETCS operational principles and the evolution of the ETCS to an advanced-ETCS. Secondly, we propose a new hybrid approach to evaluate the unavailability requirement of a new autonomous LU and explains how to handle the parametric uncertainties. Next, the procedure to assess the fault tree top event using fuzzy parameters is presented. Then, the satisfaction curve of the LU unavailable values is presented. Finally, conclusions and prospects of the future works are discussed.

Evolution of the ETCS to an advanced ETCS

Nowadays, the adoption of the European Management System (ERTMS) is necessary to facilitate the rail traffic in European network. This European standard program allows to developing a common interoperable

system for railway stakeholders to be developed. It can be installed on conventional or high-speed lines with several possibilities of implementation. The third level of implementation of ERTMS is still at a conceptual stage and relies on the evolution of the ETCS sub-parts with the tendency to remove all the trackside equipment to implement their functionalities onboard.

Operational principles of the ETCS level 3

For the ETCS Level 3, the trains operate based on the "moving block" principle. In detail, the onboard equipment (OBU) determines the location of the entire train and transmits the train information to the radio block center (RBC) through the data communication system (DCS).

In this context, the RBC principal mission does not significantly change compared to the one in its first deployment in ETCS L2. The RBC receives information from the trains, monitors the railway area status that it controls and, based on this information, generates movement authority (MA) with route and speed restrictions data contained in its Computer Processing Unit (CPU).

Based on the received MA, the onboard unit determines the End of Authority (EOA) with velocity curve and presents them on the Driver Machine Interface (DMI). Considering the EOA and speed curve information, the onboard equipment will trigger the brakes when necessary, for example, when train exceeds the EOA.

The communication between the trains and the RBC are performed through a wireless data communication system (DCS). According to the ETCS development process, the wireless DCS role becomes more and more important as it offers continuous communications and therefore can improve train operations (Bo Ai et al., 2014). For details, the evolution of the ETCS and the DCS subsystems in interaction with the ETCS will be well considered in the next subsection.

Evolutions of the ETCS

The evolution of the ETCS is presented through the development process from the level 0 when the trackside equipment is non-ETCS compliant to the level 3 with a gradual migration of the trackside equipment toward an autonomous train-born system. For ETCS L3, the location for the train traffic control depends on the designed architecture will be provided by

onboard equipment, and therefore trackside train localization is optional (Ramdas & Bradbury, 2010):

- Hybrid architecture: The train localization is performed by both the onboard equipment or track circuits and axle counters. The local control and signaling functions provided by track circuits and axle counters may be considered as a redundant function of the RBC. This architecture can deliver increased operational performances but it enhances the complexity of the system and also the infrastructure and maintenance cost.
- Simple architecture: It eliminates all balises and depends totally on onboard based train localization. The infrastructure equipment consists only of a combined RBC with control and signaling functions. Therefore, the reliability of the onboard LU becomes significant and the RBC must takes into account various uncertainties involved. However, the advantage is to reduce the investment costs for infrastructure deployment and also the operation, maintenance cost.

The train integrity function, that is, the function that verifies that the train did not lose any wagen, could be also realized onboard in ETCS L3 using the localization function when it provides the head and the tail position of the train.

New technologies of DCS subsystems and autonomous LUs are envisaged in order to assure robustness and continuous services for the simple architecture of ETCS Level 3.

Long term evolution (LTE) technology for the wireless DCS

The ETCS L2 actually relies on continuous exchanges via GSM-R networks. However, (Sniady, 2015) showed the limitation of GSM-R, which cannot meet the user requirements when the accessibility, and the productivity of transport system increase. In detail, due to lacking comprehensible QoS features (such as end-to-end resource management), its potential to support a multi-service delivery network in critical environments is limited. Another problem with GSM-R is its insufficient capacity. In central stations, providing a sufficient number of channels to serve all the trains is a major problem, especially when new passenger services (such as multimedia entertainment applications for passengers) are deployed. In addition, the long handover procedure also limits the possibility of implementation of the ETCS for high-speed trains.

(Sniady et al., 2013) highlighted the benefits when deploying the LTE network for ETCS.

Because of the ability to support multi-service traffic (voice, video, data) that demands resilience or high bandwidth real-time capabilities, LTE offers an immense perspective to railway industry. In fact, with a low user plane latency, LTE leads to higher efficiency in train operation system. Through fast handover and global roaming procedure, it also meets the mobility requirements of high-speed train systems with targets up to 350 km/h. Moreover, QoS management mechanism built into LTE allows us to guarantee delivery of critical communication traffic over multi-service networks. With these features, (Ai et al., 2014) showed the tendency that all the railway services could be then gradually transferred to the LTE-R system according to the gradual maturity of LTE-R. The communication errors and the dependability parameters of such LTE-based DCS are analyzed in Nguyen, Beugin, Berbineau, and Kassab (2014, Nguyen, Beugin, Berbineau, & Kassab, 2015).

GNSS technology for the autonomous localization unit

The development of multi-constellations satellite such as the Russian GLONASS, the European Galileo, and the Chinese Compass offers an interoperable worldwide solution for navigation. In order to enhance the GNSS signal availability (Roongpiboonsopit & Karimi, 2009) presents a multi-constellations satellite selection algorithm (MCSSA) that allows a GNSS receiver to be able to couple satellites from all available constellations for positioning a user in the required time intervals. The issue is to analyze if the performances of GNSS systems satisfy the railway requirements, in particular for safety-related applications. In (Filip, Bazant, Mocek, & Cach, 2000), authors examined the performance of a standalone GPS/GLONASS satellite navigation system and also its combination with inertial navigation systems (INS) for safety-related applications in the railway industry. (Nguyen et al., 2013; Nguyen et al., 2015) evaluated the dependability of a GNSS & Eddy Current Sensors (ECS) based LU. In fact, numerous research projects such as GRAIL-2 (Marradi et al., 2012), EATS (Arrizabalaga et al., 2014), GaLoROI (Manz et al., 2015), had been launched and therefore highlighted the trend to employ the autonomous localization into ETCS. In this context, our work focuses on the ETCS with an autonomous LU and aims to identify the availability requirements for this autonomous LU.
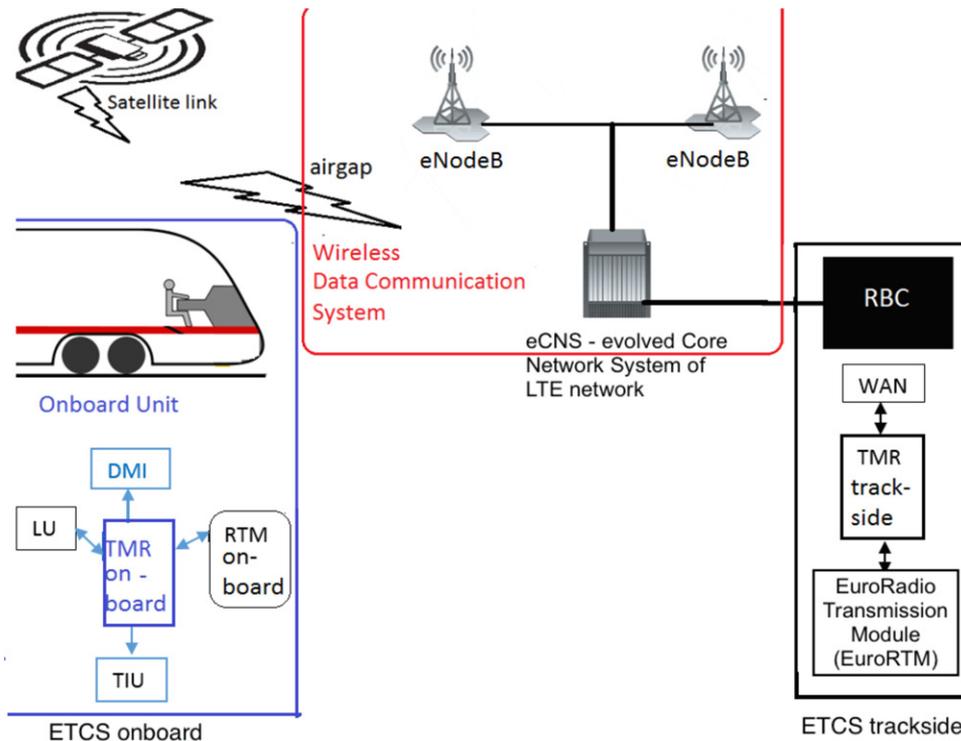
Figure 1. Simple architecture of the advanced ETCS in ERTMS L3. TIU: Train Interface Unit, RTM: Radio Transmission Module, DMI: Driver Machine Interface, LU: localization Unit, WAN: Wide Area Network, TMR: Triple Modular redundant architecture of calculation units (Flammini, 2006).

Advanced ETCS architecture

According to the current development tendency of the ERTMS/ETCS, an advanced ETCS is considered in this article. It supervises, controls train speed against an allowed speed profile (braking curve) which is automatically elaborated by the onboard equipment. No more track circuits or axle counters will be installed for the detection of the trains. The LTE technology and the autonomous LU are respectively recommended for the data communication system between trains and the RBC and for train localization. The simple architecture of an advanced ETCS is then presented in Figure 1.

New approach to identifying the unavailability requirement of a new autonomous LU

For determining the unavailability requirement of the LU, two general approaches can be adopted: the "top-down" apportionment approach or the "bottom-up" evaluation approach. However, when analyzing a particular sub-part in a more global and complex system (the ETCS), these two methods present issues that are presented in the following subsections. Therefore, we propose a procedure that allows to combine two above approaches and also to handle uncertain dependability parameters.

Issue of the "top-down" apportionment approach for Sub-systems, parts of a complex system

When considering a large complex system of system (SoS), the unexpected properties in the collective behavior of entities within their environment should be carefully considered. For example, the ETCS availability may become lower because of interactions of subsystems. Thus, the overall availability cannot be directly deduced by the sum of subsystems availability (Qiu et al., 2014). The overall availability should be evaluated at the SoS level in a determined context. In fact, EEIG ERTMS Users Group (1998) defined availability targets for ETCS according to different limited views of the system. Therefore, the availability apportionment cannot be decomposed straightforwardly from the overall system to subsystems, especially to the onboard LU on which focuses this article. It is necessary to identify the availability requirements of an autonomous LU from the SoS level.

Issue of the "bottom-up" approach for evaluating the ETCS dependability given parametric uncertainties

In the literature, numerous studies used "bottom-up" approach to assessing the reliability parameters of the

ETCS. In Flammini (2006), the author described several fault trees of different subsystems of ERTMS/ETCS L2 and based on them, evaluated the ETCS availability. Vernez and Vuille (2009) proposed to use the functional failure mode, effects and criticality analysis (FMECA) approach to address the dependability optimization of the ETCS L2. Yasuoka, Watabe, Hattori, and Matsumoto (2011) analyzed data of malfunctions of signaling operations within the Japanese railway east service area to evaluate the system reliability. Min, Chunhui, and Sen (2013) used Stochastic Reward Net for modeling the function and equipment structure of rail signaling system, and then based on it, evaluated its reliability. Morant, Larsson-Kråik, and Kumar (2016) analyzed the empirical data recorded on the corrective maintenance work orders of the Swedish railway signaling system for constructing a data-driven decision support model to study its maintenance performance. Qiu et al. (2014) proposed to use the statechart to evaluate the unavailability of the whole ERTMS L2.

In reality, it is difficult to estimate a precise value of failure, repair rates or unavailable probabilities of components due to lack of data. It is better to consider uncertainties associated with the dependability parameters to reflect the state of knowledge. Using Monte Carlo simulation (Qiu, Sallak, Schön, & Cherfi-Boulanger, 2013) examined the parametric uncertainty present in transition rates of a railway signaling system. However, the long simulation time is an issue. Besides, it requires much information and, moreover, it is not easy to propose an appropriate probability distribution for the epistemic parameter uncertainties. Among numerous uncertainty theories, the fuzzy set theory provides robust methodology to analyze the reliability and availability in the case of lacking or of inaccurate data (e.g. failure or repair rate of components; Kumar & Kumar, 2011). In fact, the fuzzy theory is recommended as a tool to model reality better than traditional probabilistic approaches because of improved results of empirical validation (Zimmermann, 2010).

Hybrid approach handling uncertain dependability parameters

To give an overview of the hybrid approach, its principles are first described with each feature chosen into the methodology and their advantages. The steps of the approach are then presented and detailed.

The top-down approach permits to identify the dependability (especially the availability) requirements of subsystems using an apportionment analysis from the dependability requirement of the overall system. In practice, when there are different interactions between components, such requirement cannot be straightforwardly decomposed. Contrarily, the bottom-up approach starts with the dependability parameters of components and then investigates their interactions to deduce the inference principles for evaluating the overall system dependability. However, this method requires precise information on the parameter values of the components, as well as the structure and behavior of the system. For new systems, there is no sufficient obtainable information. Therefore, we propose to integrate both methods in a hybrid apportionment procedure to determine the availability of sub-systems such as the LU in this article. Moreover, the main advantage of this new method compared to other classical methods is the ability to handle parameter value uncertainties. It leads to the satisfaction rate information corresponding to the uncertainty interval of the sub-system unavailability when considering the overall system dependability requirement. The approach is based on the following procedure steps described in next sub-sections.

- **First step:** preliminary allocation of the unavailability target to an advanced ETCS. We translate the ETCS availability goals defined by (EEIG ERTMS Users Group, 1998) into upper thresholds for the advanced ETCS unavailability caused by different failure types.
- **Second step:** analysis of the causes that lead to the advanced ETCS unavailability. Based on functional modeling of the overall system, the failure combinations in which the autonomous LU intervenes and that lead to system unavailability are analyzed. Fuzzy parameters will be employed to consider uncertain dependability values linked to the failure causes.
- **Third step:** identification of the satisfaction curve of the LU unavailability values to meet the advanced ETCS unavailability requirement. The autonomous LU unavailability target that allows the advanced ETCS unavailability targets to be achieved will be identified in the form of an uncertain unavailability. Therefore, the overall satisfaction curve, which presents the satisfaction rates to the ETCS requirements according to every unavailability value of the autonomous LU, will be deduced.

Preliminary allocation of the unavailability targets to an advanced ETCS

The causes of downtime during the train control system and subsystems operation can be classified into the following categories:
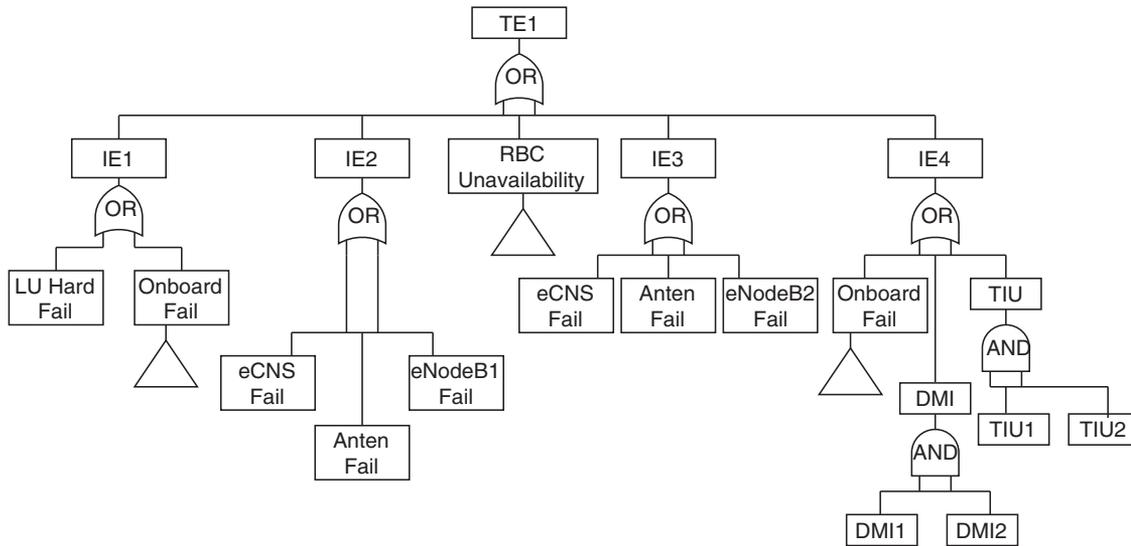
Figure 2. The advanced ETCS unavailability due to hardware failures (LU Hard: Localization Unit Hardware, eCNS: eLTE Core Network Access System, RBC: Radio Block Center, DMI: Driver Machine Interface, TIU: Train Interface Unit). TE1: Advanced ETCS unavailability due to Hardware failures, IE1: Unavailable message from train due to Hardware failures, IE2: Unavailable signal from train to RBC due to Hardware failures, IE3: Unavailable signal from RBC to train due to Hardware failures, IE4: Failed treatment of the received MA at train.

- Internal system weaknesses,
  - Software failure: unavailability generated by software defects in the deployed version.
  - Hardware failure: outages due to degradation mechanism in the devices.
- External influences,
  - Human errors: unavailability related to human operating errors.
  - Airgap failure: unavailability related to the operational environment, such those due to transmission errors.
  - Intentioned attacks: unavailability related to physical or cyber attacks.

Due to the properties of the ETCS unavailability that are present in a given view and not present in any other view (EEIG ERTMS Users Group, 1998) defined various mean availability targets for the ETCS relating to every given view. In this article, we are interested in the following two requirements, in which the autonomous LU intervenes:

R1: The ERTMS/ETCS quantifiable contribution to operational availability, due to hardware failures, shall be not less than 0.999854.

That means the advanced ETCS unavailability due to hardware failures is inferior to U_{R1} where $U_{R1} = 1.46E-4$. This unavailability target is linked to the top event of the Fault Tree (FT) presented in Figure 2. The FT structure will be explained in detail in next subsection.

R2: The ERTMS/ETCS quantifiable contribution to operational availability, due to hardware failures and transmission errors, shall not be less than 0.99984.

The R2 can be translated into the advanced ETCS unavailability due to hardware failures and transmission errors. This unavailability is then inferior to U_{R2}, where $U_{R2} = 1.6E-4$. This unavailability target is linked to the top event of the Fault Tree (FT) presented in Figure 3. The details of this FT will be discussed in next subsection.

Analysis of the causes that lead to the advanced ETCS unavailability

This section details the second step of the procedure, that is, it analyzes the failure combinations in which the autonomous LU intervenes and that lead to the advanced ETCS unavailability.

Figure 2 presents the hardware failure causes that lead to the advanced ETCS unavailability. It includes the following causes:

- IE1 - when the train "position report" message is unavailable due to hardware failures of the LU or of the onboard equipment, see details in Figure 4.
- when the train cannot send the message (IE2) or receive the message (IE3) due to hardware failures of transmission components, such as the eCNS, the eNodeB, and the receiving-transmitting antenna.
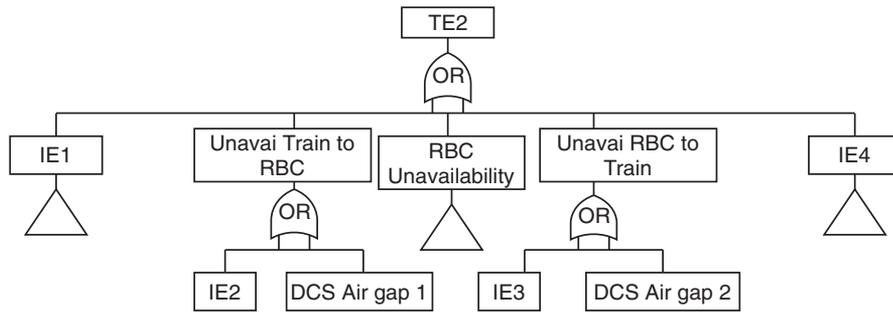
Figure 3. The advanced ETCS unavailability due to hardware failures and communication errors (TE2: Advanced ETCS unavailability due to hardware failures and communication errors, RBC: Radio Block Center, DCS: Data Communication System).
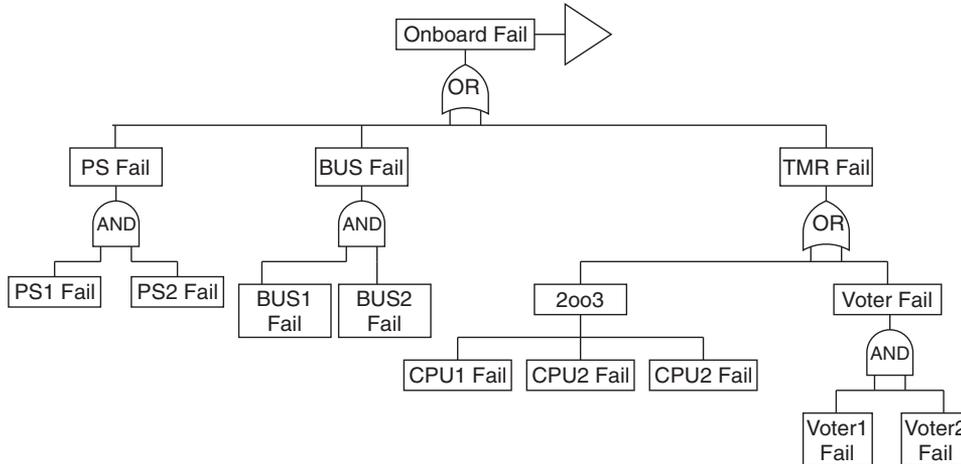
Figure 4. The onboard equipment failures (PS: Power System, CPU: Computer Processor Unit, TMR: Triple Modular Redundancy).
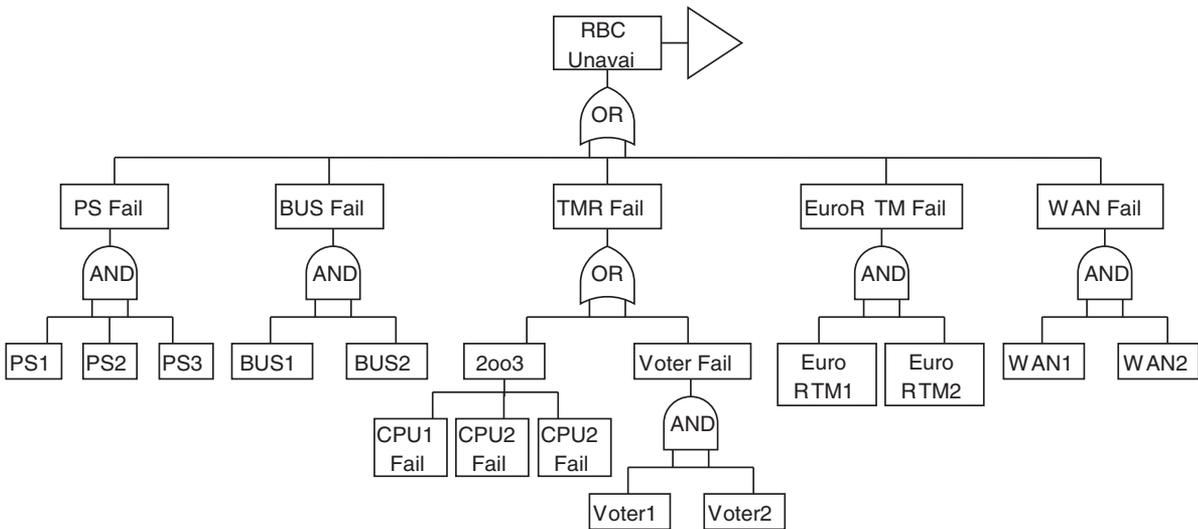
Figure 5. The RBC unavailability (RBC: Radio Block Center, PS: Power System, TMR: Triple Modular Redundancy, EuroRTM: EuroRadio Transmission Module, CPU: Computer Processor Unit, WAN: Wide Area network).

- when there exist hardware failures in the RBC. The RBC unavailability is well analyzed in Figure 5.
- when the MA cannot be correctly treated at the train due to hardware failures of the onboard equipment, the driver machine interface (DMI), or

the train interface unit (TIU). The DMI (served to provide onboard interaction with the train driver) and the TIU (used to make the interface between TIU and train-borne equipment, e.g. the brakes) have each of them one redundant unit (Flammini,

2006). Therefore, the DMI (or TIU) is considered as unavailable when both units, DMI1 and DMI2 (or TIU1 and TIU2) are failed.

Figure 3 presents the advanced ETCS unavailability due to hardware failures and communication errors. Compared with Figure 2, the fault tree in this case also takes into account the data communication system unavailability due to air gap unavailability (DCS air-gap 1 for the signal from the train to the RBC, and DCS air-gap 2 for the signal from the RBC to the train).

The air gap failures are related to connection losses due to network coverage and service quality of the communication system. Following the study on the impact of the radio deployment on ETCS presented in (Sniady, 2015), the LTE delay performance is significantly better than GSM-R, and furthermore, no data loss was observed. In other words, the negative contribution of the LTE service quality can be negligible when evaluating the steady state availability of the DCS. In this article, only connection loss due to network coverage is considered in the DCS air gap failure.

The onboard equipment fault tree

In the advanced ETCS, the onboard unit structure is similar to the one presented in Flammini (2006), but the train localization is only performed by itself. Therefore, the balise transmission module is removed, and the odometer is replaced by the autonomous LU that should to ensure accurate, continuous, and reliable localization results.

The onboard fault tree is then presented in Figure 4. Its top event happens when the redundant components are failed. These components are the power system (PS), or bus (BUS), or CPU, or voter, that is, component linked to the 2 out of 3 (2oo3) architecture realizing the majority vote strategy. Their redundant configurations are explained in detail in (Flammini, 2006).

The LU presented in this article is considered as a black box. We are only interested in its hardware unavailability.

The radio block Centre fault tree

The RBC structure in the advanced ETCS is similar to the traditional RBC structure in ERTMS L2. Then, the RBC fault tree is described in Figure 5 following

(Flammini, 2006). Its top event occurs when one of the following critical events happens:

- The three PS components connected in parallel are failed.
- The two redundant buses, for interconnecting system peripherals, are failed.
- The Triple Modular Redundancy (TMR) architecture of CPU (2oo3 voting logic) is unavailable.
- EuroRTM (EuroRadio Transmission Module) that helps the RBC is connected to the DCS is failed. Its interface technology depends on the data communication system technology (e.g., WIFI, GSM-R or LTE, etc.).
- The redundant configuration of 2 WAN (Wide Area Network) used to connect the RBC and other ETCS-trackside components is failed.

The procedure to evaluate the top event of these FT using fuzzy parameters will be presented in next section.

Procedure to evaluate the fault tree top event using fuzzy parameters

In this section, we firstly present the common formulas used for calculating the unavailability of a system made of different combined components with constant failure and repair rates. The fuzzy numbers are used to handle the uncertainty of these values. Thus, the basic theoretical background on fuzzy numbers and their combination are reminded. Finally, we explain how to introduce fuzzy numbers into a fault tree.

Mathematical background

Common unavailability assessment

Consider a component i whose the lifetime and repair time are exponential with failure rate λ_i, and repair rate ν_i, the component unavailability in steady state is given by (Rausand & Hoyland, 2004):

$$U_i = \frac{\lambda_i}{\nu_i + \lambda_i} \qquad (1)$$

In this article, assuming that

- failed components receive repair services right away no matter how many components are failed,
- working components are normally subjected to their failures when other components or systems are down, the output probability of the OR-gate, AND-gate and K-out-of-N gate of the FT are evaluated similarly to the unavailability of systems

connected in series, parallels or K-out-of-N structures, following (Li, Zuo, & Yam, 2006):

- *when n components are connected in series having availability Ai, failure rate λi and repair rate νi, then the system unavailability (or in other words, the OR-gate output) is given by:*

$$U_S = 1 - \prod_{i=1}^{n} A_i = 1 - \prod_{i=1}^{n} \frac{\nu_i}{\nu_i + \lambda_i} \qquad (2)$$

- *when the system is composed of n identical components in parallel having failure rate λ and repair rate ν, then the system unavailability (or in other words, the AND-gate output of identical inputs) is given by:*

$$U_S = \prod_{i=1}^{n} (1 - A_i) = \frac{(\lambda)^n}{(\nu + \lambda)^n} \qquad (3)$$

- *when the system has a redundant configuration of K-out-of-N identical components having failure rate λ and repair rate ν, then the system unavailability (or in other words, the KooN-gate output of identical inputs) is given by:*

$$U_S = \frac{\lambda^n}{(\lambda + \nu)^n} \sum_{r=0}^{k-1} \left(\frac{\nu}{\lambda} \right)^r \qquad (4)$$

Then, the unavailability in the case of a 2oo3 system (i.e the 2oo3-gate output) is given by:

$$U_S = \frac{3\lambda^2\nu + \lambda^3}{(\nu + \lambda)^3} \qquad (5)$$

Fuzzy number and fuzzy arithmetic

Depending on the available knowledge, the failure or repair rate of a component can be modeled by a precise value or by typical values, a distribution, or an interval. In reality, when only little knowledge is available, the failure or repair rate's value can simply be represented by an interval from a lower bound a to an upper bound c. Although there may not be sufficient information in between a and c to construct a whole distribution, often in practice, there is some preference for a more probable value $b \in [a, c]$. This preference can stem from one or a few past cases, previous experience, or knowledge of experts. The context calls for the use of a fuzzy number, which is an imprecise quantity dedicated to taking into account such inherent uncertainty (Zimmermann, 2010). That is the reason why in this paper, we extend the representation of dependability parameters to fuzzy numbers. In detail, we prefer a triangular fuzzy number over a triangular probabilistic distribution since the
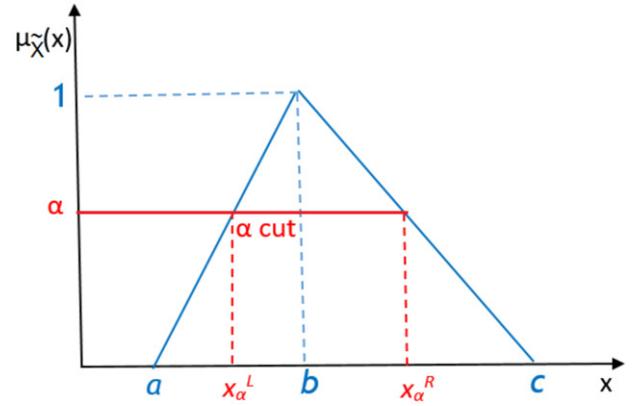

Figure 6 Illustration of one α-cut set of a fuzzy triangular number.

latter requires much richer historical information or background data to define its shape.

Definition 0.1. Fuzzy number

Let X be a universal set, then a fuzzy number $\tilde{X}$ is a convex normalized fuzzy set $\tilde{X}$, defined by its membership function: $\mu\tilde{X} : X \rightarrow [0, 1]$, called the grade of membership of x in $\tilde{X}$. This membership function assigns a real number $\mu\tilde{X}(x)$ in the interval $[0, 1]$ to each element $x \in X$.

Definition 0.2. α-cut set

Given a fuzzy set $\tilde{X}$ in X and any real number $\alpha \in [0, 1]$, then the α-cut set of $\tilde{X}$, denoted by $\tilde{X}_\alpha$, is an interval defined by: $\tilde{X}_\alpha = \{x \in X, \mu\tilde{X}(x) \geq \alpha\}$, see Figure 6.

Definition 0.3. Fuzzy arithmetic with α-cut sets

Let $[x_\alpha^L, x_\alpha^R]$ and $[y_\alpha^L, y_\alpha^R]$ are respectively the α-cut interval of $\tilde{X}$ and $\tilde{Y}$ with the corresponding α value, then the α-cut interval of $\tilde{Z} = f(\tilde{X}, \tilde{Y})$ is defined as $[z_\alpha^L, z_\alpha^R]$ where:

$$\begin{cases} z_\alpha^L = \min_{\left\{x \in [x_\alpha^L, x_\alpha^R], y \in [y_\alpha^L, y_\alpha^R]\right\}} f(x, y) \\ z_\alpha^R = \max_{\left\{x \in [x_\alpha^L, x_\alpha^R], y \in [y_\alpha^L, y_\alpha^R]\right\}} f(x, y) \end{cases} \qquad (6)$$

From Eq. (6), the following α-cuts of functions of positive fuzzy numbers can be easily derived:

$$\tilde{Z} = \tilde{X} + \tilde{Y}; \quad \tilde{Z}_\alpha : \left[x_\alpha^L + y_\alpha^L, x_\alpha^R + y_\alpha^R\right] \qquad (7)$$

$$\tilde{Z} = \tilde{X}.\tilde{Y}; \quad \tilde{Z}_\alpha : \left[x_\alpha^L.y_\alpha^L, x_\alpha^R.y_\alpha^R\right] \qquad (8)$$

$$\tilde{Z} = 1 - \tilde{X}; \quad \tilde{Z}_\alpha : \left[1 - x_\alpha^R, 1 - x_\alpha^L\right] \qquad (9)$$

Evaluation of the fault tree top event using fuzzy parameters

An overview of concepts and applications of the fuzzy fault tree analysis was discussed in Mahmood, Ahmadi,

Verma, Srividya, and Kumar (2013). Let $\tilde{P}_i$ $(i = 1, 2 \ldots n)$ represent the fuzzy probability of event i, the α-cut set of the output gate's probability is given by:

$$\tilde{P}^L_{AND_\alpha} = \prod_{i=1}^{n} \tilde{P}^L_{i_\alpha}; \qquad \tilde{P}^R_{AND_\alpha} = \prod_{i=1}^{n} \tilde{P}^R_{i_\alpha} \qquad (10)$$

$$\tilde{P}^L_{OR_\alpha} = 1 - \prod_{i=1}^{n} \left(1 - \tilde{P}^L_{i_\alpha}\right); \qquad \tilde{P}^R_{OR_\alpha} = 1 - \prod_{i=1}^{n} \left(1 - \tilde{P}^R_{i_\alpha}\right) \qquad (11)$$

The following Lemma allows us to consider the membership function's shape of the probability of the OR/AND-gate output.

Lemma 1. *Let $\tilde{X}_i$ be the fuzzy number whose $x^L_{i_\alpha}$ is non-decreasing and $x^R_{i_\alpha}$ is non-increasing in α, $\tilde{Z}$ be the AND/OR-gate output of n fuzzy numbers $\tilde{X}_i$, then z^L_α is non-decreasing and z^R_α is non-increasing in α.*

Next, we evaluate the α-cut set of the gate output when the unavailability of a basic component indirectly evaluated through the corresponding fuzzy failure rate ($\tilde{\lambda}_i$) and fuzzy repair rate ($\tilde{\nu}_i$).

Lemma 2.
1. *Let $\tilde{Z}$ be the unavailability of the component i, then the α-cut set of $\tilde{Z}$ is given by:*

$$z^L_\alpha = \frac{\lambda^L_{i_\alpha}}{\nu^R_{i_\alpha} + \lambda^L_{i_\alpha}}; z^R_\alpha = \frac{\lambda^R_{i_\alpha}}{\nu^L_{i_\alpha} + \lambda^R_{i_\alpha}} \qquad (12)$$

2. *Let $\tilde{Z}$ be the output of the OR-gate, the α-cut set of $\tilde{Z}$ is given by:*

$$z^L_\alpha = 1 - \prod_{i=1}^{n} \frac{\nu^R_{i_\alpha}}{\nu^R_{i_\alpha} + \lambda^L_{i_\alpha}}; z^R_\alpha = 1 - \prod_{i=1}^{n} \frac{\nu^L_{i_\alpha}}{\nu^L_{i_\alpha} + \lambda^R_{i_\alpha}} \qquad (13)$$

3. *Let $\tilde{Z}$ be the output of the AND-gate, the α-cut set of $\tilde{Z}$ is given by:*

$$z^L_\alpha = \prod_{i=1}^{n} \frac{\lambda^L_{i_\alpha}}{\nu^R_{i_\alpha} + \lambda^L_{i_\alpha}}; z^R_\alpha = \prod_{i=1}^{n} \frac{\lambda^R_{i_\alpha}}{\nu^L_{i_\alpha} + \lambda^R_{i_\alpha}} \qquad (14)$$

4. *Let $\tilde{Z}$ be the output of the 2oo3-gate, then the α-cut set of $\tilde{Z}$ is given by:*

$$\begin{cases} z^L_\alpha = \dfrac{\left(\lambda^L_\alpha\right)^3 + 3\left(\lambda^L_\alpha\right)^2 \nu^R_\alpha}{\left(\lambda^L_\alpha + \nu^R_\alpha\right)^3} \\[2ex] z^R_\alpha = \dfrac{\left(\lambda^R_\alpha\right)^3 + 3\left(\lambda^R_\alpha\right)^2 \nu^L_\alpha}{\left(\lambda^R_\alpha + \nu^L_\alpha\right)^3} \end{cases} \qquad (15)$$

Lemma 3. *Considering a component having fuzzy failure rate $\tilde{\lambda}$ and fuzzy repair rate $\tilde{\nu}$ where $\lambda^L_\alpha, \nu^L_\alpha$ are non-decreasing in α and $\lambda^R_\alpha, \nu^R_\alpha$ are non-increasing in α,*

then its unavailability, $\tilde{Z}$ is a fuzzy number whose z^L_α is non-decreasing and z^R_α is non-increasing in α.

Theorem 1. *Considering a series/parallel system that includes components having fuzzy dependability parameters $\tilde{X}_i$ where $x^L_{i_\alpha}$ is non-decreasing and $x^R_{i_\alpha}$ is non-increasing in α, the unavailability of this system is also a fuzzy number $\tilde{Z}$ whose $z^L_{i_\alpha}$ is non-decreasing and $z^R_{i_\alpha}$ is non-increasing in α.*

It is also true for the 2oo3 system with identical components.

In summary, FT having fuzzy input parameters is evaluated by Procedure 1. On other hand, from Theorem 1, the membership function of the top event probability, $\mu\tilde{Z}(z)$, has the left side being monotone non-decreasing in z and the right side being monotone non-increasing in z. Based on these results, in next section, the approach to evaluate the satisfaction curve for unavailability of the autonomous LU will be presented.

Procedure 1: Evaluating the FT with fuzzy parameter inputs
1: Set $\alpha = 0$
2: **while** $\alpha \leq 1$ **do**
3: Determine α-cut set for all input fuzzy numbers.
4: Calculate the α-cut set for all gate outputs (by Eqs. (15–19)) until the α-cut set of the top event is obtained.
5: $\alpha = \alpha + \Delta$, where Δ is a small amount (e.g 10^{-4}).
6: **end while**
7: Construct the membership function of the top event by aggregation of all α-cut sets.

Evaluation of the satisfaction curve of the unavailability of the autonomous localization unit

Principles to obtain a satisfaction curve

The satisfaction curve of the autonomous LU's unavailability values will be identified for every requirement of the advanced-ETCS unavailability. Without loss of generality, we present in this section the principles to determine the satisfaction curve according to the requirement R1. Those principles apply also for requirement R2.

The FT presented in Figure 2 can be evaluated by minimal cuts represented in Figure 7. Let U_{LU} and U_1 characterizing respectively the autonomous LU's fuzzy unavailability and the fuzzy probability of the event IU1 of the fault tree.
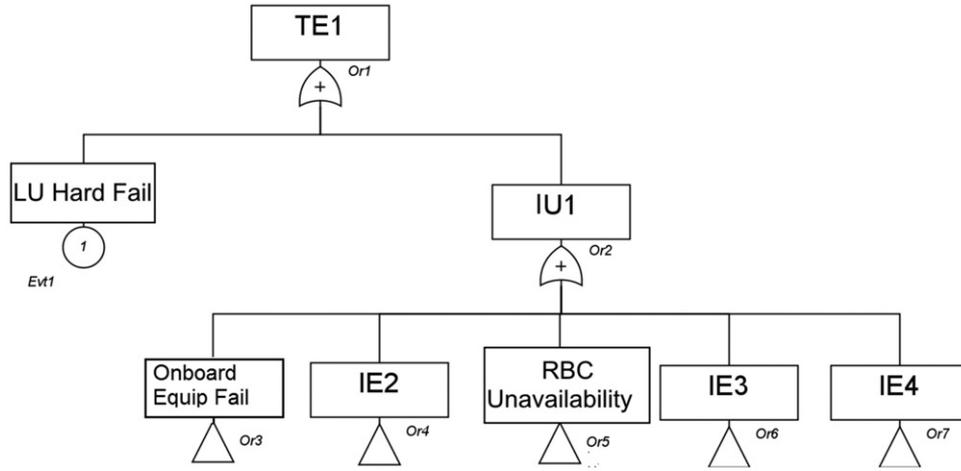
Figure 7. Deduced view of the fault tree of the advanced ETCS due to hardware failures (RBC: Radio Block Center, LU: Localization Unit, IE2: Unavailable signal from train to RBC due to Hardware failures, IE3: Unavailable signal from RBC to train due to Hardware failures, IE4: Failed treatment of the received MA at train, TE1: Advanced ETCS unavailability due to Hardware failures).
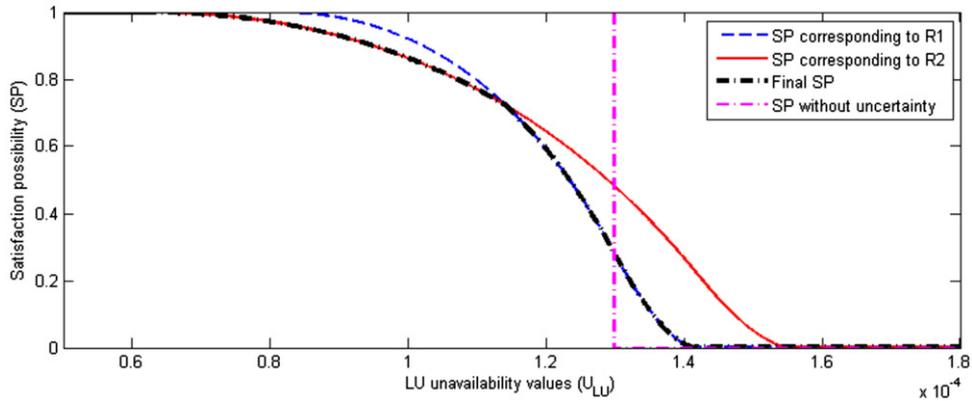

Figure 8. Illustration of the satisfaction area.

The membership function, $\mu_{\tilde{U}_1}(U_1)$, is assessed by Procedure 1 that describes the evaluation approach for such FT with fuzzy parameter inputs. It is then represented by the blue line in Figure 8. In order to satisfy the requirement R1 ($P_{TE1} \leq U_{R1}$), the upper threshold of $\tilde{U}_1$ is: $U_{R1} - U_{LU}$. This threshold is characterized by the red vertical line in Figure 8 when U_{R1} and U_{LU} are precise numbers. Then, we consider the satisfaction rate, which represents the satisfaction percentage (SP) of the advanced ETCS unavailability with the ETCS requirement R1. It can be calculated by the fraction of the gray area (S_{GA}) over the surface $S_{\mu(U_1)}$ created by the membership function $\mu_{\tilde{U}_1}(U_1)$ and the horizontal ax, see Figure 8. If the red line is outside (on the right) of the blue curve, that is, $U_{\alpha=0}^R \leq (U_{R_1} - U_{LU})$, the requirement R1 is statisfied with all possible value of U_1. Contrarily, the satisfaction percentage (SP) is given by:

$$SP = \frac{S_{GA}}{S_{\mu(U_1)}} \qquad (16)$$

In order to determine the exigence for the LU unavailability (U_{LU}) according to the ETCS requirement (R1), we have to evaluate the SP values in function of U_{LU} values:

- If $U_{LU} \leq U_{R1} - U_{1_{\alpha\ 0}}^R$, $SP = 100\%$.
- If $U_{LU} > U_{R1} - U_{1_{\alpha\ 0}}^L$, $SP = 0\%$.
- If $U_{R1} - U_{1_{\alpha\ 0}}^R < U_{LU} \leq U_{R1} - U_{1_{\alpha\ 0}}^L$, SP is identified by Procedure 2. This procedure incluses two phrases. Firstly, we evaluate the set of values of the satisfaction percentage SP for all U1 values, where $U_1 \in [U_{1_{\alpha\ 0}}^L, U_{1_{\alpha\ 0}}^R]$. Finally, corresponding to every value of U_{LU} we find the maximal value of SP (in the set of SP values given by the first phase) such as this value is inferior than $U_{R1} - U_{LU}$. This procedure will applied for the case study and its result will be presented in Figure 9.

Procedure 2: identifying the satisfaction curve of the LU unavailability values

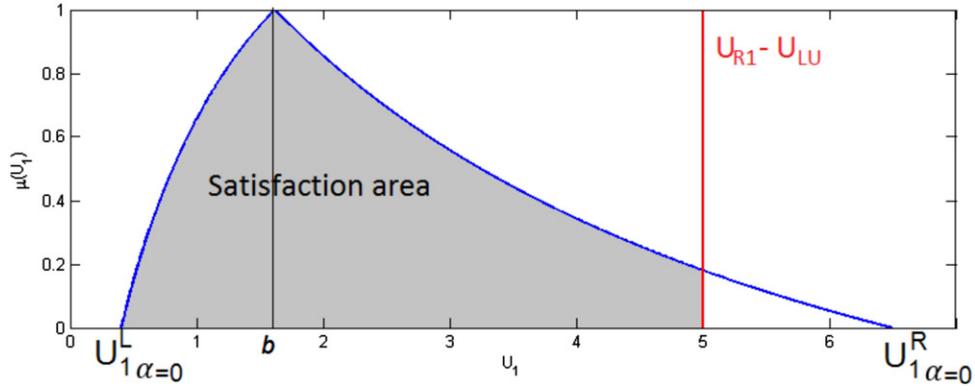1: **procedure Evaluate the satisfaction percentage, SP**

Figure 9. Satisfaction curves of the LU unavailability values.

2:    Let d be the length of the vector B including obtained values of U_1 that is evaluated by Procedure 1. We have: $B = \{U_{1_{\alpha \; 0}}^L, U_{1_{\alpha \; i\Delta}}^L, U_{1_{\alpha \; 1}}, U_{1_{\alpha \; i\Delta}}^R, U_{1_{\alpha \; 0}}^R\}$, where $(i = 1, 2, ..., n-1)$.

3:    **for** $i = 2 : 1 : d$ **do**

4:       Calculate $S_{\mu(U_1)}$, that is a vector having d elements, by the numerical integral following the trapezoidal rule: $S_{\mu(U_1)}(i) = S_{\mu(U_1)}(i-1) + 0.5 * [B(i) - B(i-1)] * (\alpha_{B(i)} + \alpha_{B(i \; 1)})$

5:    **end for**

6:    Evaluate vector SP: $SP = \frac{S_{\mu(U_1)}}{S_{\mu(U_1)}(d)}$

7: **end procedure**

8: **procedure Identifying $SP_{U_{LU}}$**

9:    Set i = 1

10:    **while** $(d \neq i + 1)$ **do**

11:    h = round$((i + d)/2)$

12:    **if** $U_{R1} - U_{LU} < B(h)$ **then**

13:       d = h

14:    **end if**

15:    **if** $U_{R1} - U_{LU} > B(h)$ **then**

16:       i = h

17:    **end if**

18:    **if** $U_{R1} - U_{LU} = B(h)$ **then**

19:       i = h; d = h

20:       Break

21:    **end if**

22: **end while**

23:    $SP_{U_{LU}} = \frac{SP(i) + SP(d)}{2}$

24: **end procedure**

Case study: identifying the satisfaction curve of the autonomous LU unavailability values

The input parameters for the case study are presented in Table 1. For equipment of the RBC and the OBU, the most probable failure rate values are chosen according the values presented in Flammini (2006). The upper and lower values of their failure rates are chosen arbitrarily +100% and –50% of the most probable values. On the other hand, as the Mean Time To ReStore (MTTRS) of the OBU equipment and the RBC equipment are respectively 1.737 and 0.896 hours (EEIG ERTMS Users Group, 1998), the most probable values of their repair rates are 0.58 and 1.12, respectively. Furthermore, EEIG ERTMS Users Group (1998) described that the standstill time of the OBU equipment and the RBC equipment are respectively less than 4 hours and 2 hours. Then the lower bounds of repair rates of all OBU and RBC equipment are respectively 0.25 and 0.5. In summary, the repair rates of the RBC and OBU equipment are chosen as follows: $\tilde{\nu}_{OBU(e)} : [0.25, 0.58, 1.2]$ and $\tilde{\nu}_{RBC(e)} : [0.5, 1.12, 2.2]$ (/h).

Regarding the DCS, although the antenna is considered as a DCS equipment but is implemented on the train, its repair rate is considered like the repair rate of other onboard equipment. The most probable value of the antenna failure rate is chosen according to the MTBF of train antenna presented in the test report (Comp, A., 2015. Certification of test report-MTBF-OmPlecs-TOP 200 AMR.). For the eNodeB and eCNS, the most likely values of their repair rates and failure rates are chosen according to the values presented in the commercial product descriptions (Huawei Technology Company. LTE3.1 DBS3900 LTE Product Description; Huawei eLTE3.3 eCNS210 product description). The upper and lower values are chosen arbitrarily +100% and −50% of the corresponding most probable value. Following Zimmermann and Hommel (2005), the connection loss rate and reconnection rate are respectively $\tilde{\lambda}_{CL} : [10^{\;4}, 10^{\;3}, 10^{\;2}], \tilde{\nu}_{CL} : [600, 1200, 2400]$ (/h).

The satisfaction percentages corresponding to requirement R1 (noted SP_{R1}) are then evaluated by Procedure 2. It is represented by the blue dash line in Figure 9. Similarly, corresponding to requirement R2, the SP_{R2} are characterized by the red line. The final satisfaction possibility SP is evaluated by:

$SP = \min(SP_{R1}, SP_{R2})$. We find that if the LU unavailability is inferior to $6.17E-5$, the SP is 100%, while the ETCS requirements cannot be satisfied when the LU unavailability is superior to $1.42E-4$. When $6.17E-5 \leq U_{LU} \leq 1.42E-4$, the satisfaction possibility follows the black dash line represented in Figure 9.

To compare with the traditional methodology, we perform similar calculations using non-fuzzy algebra for evaluating the classical FT. The most probable values of the input parameters are used to assess the probability U_1. The results describe that the LU unavailability must be inferior or equal to $1.3E-4$ to satisfy both requirements R1 and R2. That means the ETCS requirement is also satisfied when unavailability value of the autonomous LU is $1.3E-4$. However, when using our methodology, taking into account parametric uncertainties, the corresponding satisfaction possibility of this value is only 28.53%. That means we have to bear the high risk that the ETCS does not meet the availability requirements. Contrarily, if we consider the pessimist cases of input parameters, the traditional approach result could lead to unnecessary expenses for the development of the LU, and furthermore, could be difficult to achieve in practice.

Discussion about the impact of components and their parametric uncertainties on the satisfaction curve

Let D be the set of the LU unavailability values whose the SP corresponds to the ETCS requirements we want to consider. The impact of component i on the LU satisfaction curve is examined by the critical importance measure (CIM_i). It is evaluated by the difference between the LU satisfaction curve when the component i is working and when the component i is failing.

$$CIM_i = \sqrt{\sum_{U_{LU} \in D} \left(SP_{U_{LU}|(i \text{ working})} - SP_{U_{LU}|(i \text{ failing})} \right)^2}$$

(17)

Similarly, the impact of parameter uncertainty on the LU satisfaction curve is examined by the uncertainty importance measure (UIM_j) of parameter j. It is evaluated by the difference between the LU satisfaction curve when the parameter j is precisely measured and the one when the parameter j is fuzzy.

$$UIM_j = \sqrt{\sum_{U_{LU} \in D} \left(SP_{U_{LU}|(j \text{ precise})} - SP_{U_{LU}|(j \text{ fuzzy})} \right)^2} \quad (18)$$

Table 2 presents the critical component ranking and the parameter uncertainty impact ranking when

Table 1. Summary of the input parameters.

Parameter	Lower	Most Probable	Upper
λ_{PS}	9.1E 6	1.82E 5	3.64E 5
λ_{BUS}	2.2E 6	4.4E 6	8.8E 6
λ_{CPU}	3.7E 6	7.4E 6	1.48E 5
λ_{Voter}	1.5E 6	3E 9	6E 9
λ_{RTM}	5E 7	1E 6	2E 6
λ_{DMI}	5E 8	1E 7	2E 7
λ_{TIU}	5E 8	1E 7	2E 7
λ_{WAN}	5E 8	1E 7	2E 7
λ_{eCNS}	1.55E 6	3.1E 6	6.2E 6
λ_{eNodeB}	3.25E 6	6.5E 6	1.3E 5
λ_{Anten}	3.05E 8	6.1E 8	1.22E 7
λ_{CL}	1E 4	1E 3	1E 2
$\nu_{RBC(e)}$	0.5	1.12	2.2
$\nu_{OBU(e)}$ & ν_{Anten}	0.25	0.58	1.2
ν_{eCNS} & ν_{eNodeB}	0.5	1	2
ν_{CL}	600	1200	2400

considering the satisfaction curve of the LU unavailability values from $5E-5$ to $1.8E-4$. We find that the components related to the data communication system (DCS) such as the eNodeB, eCNS, air gap and the antenna are respectively the most critical components because their status directly affects on the advanced ETCS unavailability. On the other hand, the impact of the voter component can be negligible thanks to its redundant configuration and its reliable characteristic. Considering the ranking of the uncertainty importance measure (UIM), we find that the impact of parametric uncertainties of the DCS components on the satisfaction curve is also the most important compared with other parameters. Therefore, they must have more precise value than other parameters.

Discussion of the practical application and benefits of the proposed methodology

In numerous recent articles (Milakis, van Arem, & van Wee, 2017; Ran, Jin, Boyce, Qiu, & Cheng, 2012; Shladover, 2017), the authors highlight perspectives of future transportation research, in which the entire system becomes more connected and automated. In fact, the adoption of an autonomous LU in ETCS is encouraged by numerous European Commission research projects. These projects aim to explore and promote the use of satellites as a low-cost signaling solution and the ERTMS Regional, in particular, is used in the highest level of ETCS (level 3). An overview of these projects is provided in Marais, Beugin, and Berbineau (2017) in which the authors emphasized a promising perspective of introducing the GNSS in railway mentalities, especially in the ETCS application. In fact, the potential gains achievable by the combination of ETCS signaling and train dispatching systems were highlighted in Goverde, Corman, and D'Ariano (2013, 3). In Smith, Majumdar, and Ochieng (2012), the authors

Table 2. Ranking of the components CIM and the input parameters UIM.

Component *CIM*	Ranking
eNodeB	1
eCNS	2
Airgap	3
Anten	4
PS	5
CPU	6
BUS	7
RTM	8
DMI	9
TIU	9
WAN	10
Voter	11
Parameter *UIM*	**Ranking**
ν_{eCNS} & ν_{eNodeB}	1
λ_{eNodeB}	2
λ_{CL}	3
ν_{CL}	4
λ_{eCNS}	5
$\nu_{OBU(e)}$ & ν_{Anten}	6
λ_{Anten}	7
λ_{PS}	8
λ_{CPU}	9
$\nu_{RBC(e)}$	10
λ_{BUS}	11
λ_{RTM}	12
λ_{TIU} & λ_{DMI}	13
λ_{WAN}	14
λ_{Voter}	15

investigated the technical and procedural challenges relevant to the safe introduction of ERTMS into European railway systems. The road map for the introduction and exploitation of GNSS technologies in the train control system based on the ERTMS architecture was described in Senesi (2012). One of the principal challenges is to verify that the performances obtained correspond to the ETCS requirements including safety-related ones. In particular, it is necessary to prove that the new solution satisfies dependability and safety conditions using especially RAMS requirements as defined in the three European railway standards (i.e. EN50126, EN50128, and EN50129). Traditional RAMS evaluation approaches, including simulation and experimental campaigns, are not adequate for wireless systems and GNSS-based positioning systems in particular. In fact, it is difficult to precisely obtain detailed information on the system, component dependability parameters or operation environments for simulations in the development phase of a new system. On the other hands, for on-sites-experimental campaigns, it requires a large investment cost and, furthermore, it is quite impossible to control all test conditions, for example possibility to change the constellation and anticipation of future systems, such as the complete Galileo.

In this context, our new methodology could be used to identify the specification of the LU according to ETCS requirements. Thanks to the combination between the hybrid apportionment procedure and the fuzzy theory, it offers the ability to handle unknown information about new sub-systems and the uncertainties of its component dependability parameters. In particular, it provides managers with satisfaction rate information corresponding to the uncertainty interval of the sub-system dependability when considering the overall system requirement. Considering the case study, the classical approach specifies that the LU maximal unavailability should be $1.3E - 4$ to satisfy the ETCS availability requirement. However, our new approach shows that if this value is used when developing a new LU, the satisfaction possibility according to the ETCS requirement is quite small, only 28.53%. That means we have to bear the high risk that the ETCS does not meet the availability requirements. Contrarily, if we consider the pessimistic cases of input parameters (i.e., the highest values of failure rates and lowest values of repair rate), the traditional approach result describes a low value of the LU unavailability. This requirement could lead to unnecessary expenses in the development of the LU, and furthermore, could be difficult to achieve in practice. Using the new method, the obtained satisfaction curve provides more information to analysts about the satisfaction rate corresponding to every value of the LU unavailability. This information reinforces the decision flexibility of managers. They could opt either for an additional investment to improve the LU availability or an acceptance of the low satisfaction rate to reduce expenses.

On the other hand, thanks to the development of the Galileo constellation, the localization could be achieved by simultaneous multi-constellation management algorithms. Therefore, it allows improving the availability of the LU. For an extension of this work, considering environmental effects when assessing the ETCS availability requirement, the proposed method could provide a satisfaction curve on the ETCS requirement for the LU unavailability values due to missing satellite signals. Based on that, the analyst could consider the possibility of using the multi-constellation to improve the LU availability and therefore obtain a higher satisfaction rate. Moreover, this methodology could also be applied in different practical situations to determine the requirements of a such new subsystem according to overall system requirements. For examples, to identify specifications of a new LTE based data communication system, an overall ETCS fuzzy FT could be constructed by investigating internal system failures and external influences, which are difficult to precisely evaluated. Therefore, managers can balance investment cost with desired

performances thanks to the advantage of this approach regarding uncertainties handling.

Conclusion

In this article, we have discussed the current trend of the ETCS towards integrating onboard autonomous localization. For the development process of this new equipment, it is necessary to allocate required availability values in order to meet ETCS requirements. Therefore, we proposed a new approach for evaluating the satisfaction rate of the LU unavailability to the defined ETCS requirements. This method allows taking into account parametric uncertainties to evaluate the fuzzy unavailability of systems in series/parallels or K-out-of-N structures. The performance of our procedure has been illustrated by a case study of an advanced ETCS integrating LTE-based data communication system and an onboard LU. The results showed that the upper threshold of the LU unavailability obtained by the classical method (using the most probable parameter values) only corresponds to a satisfaction rate of 28.53% when taking into account parametric uncertainty. The new quantitative method provides more information to analysts about the satisfaction rate corresponding to every value of the LU unavailability. It reinforces the flexibility of manager decisions in practice: opt either for an additional investment to improve the LU availability or an acceptance of the low satisfaction rate to reduce expenses. On the other hand, we highlighted the importance of the DCS components when evaluating the critical importance measures (*CIM*). We also highlighted their parametric uncertainties impact on the satisfaction curve of the LU unavailability when considering the uncertainty importance measure (*UIM*).

The methodology is generic in nature and can be specifically tailored to determine the LU availability requirements according to different ETCS availability requirements. For examples, the internal system weaknesses and external influences could be taken into account in an overall fuzzy FT. This is especially the case for the environmental effects on the localization (e.g. on GNSS signals) for which it is difficult to obtain precise parameter values. In this case, managers can benefit from the advantage of this approach handling uncertainties, to balance ETCS life cycle cost with desired performances. However, the evaluation time of a large fuzzy FT could be an issue when considering a general case taking into account all types of internal and external failures. Therefore, an efficient algorithm to reduce the evaluation time should be developed in the future.

In further works, using the new qualitative method presented in this article, we could allocate the RAM requirements to localization equipment. Furthermore, according to the V-model, when a new system is completed, the operational test or virtual certification processes should be performed to prove its satisfaction rate.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

ORCID

Khanh T. P. Nguyen http://orcid.org/0000 0001 8184 8238

References

Arrizabalaga, S., Mendizabal, J., Pinte, S., Sanchez, J., Gonzalez, J., Themostokleous, M., & Lowe, D. (2014). Development of an advanced testing system and smart train positioning system for etcs applications. In Transport research arena 2014, Paris.

Ai, B., Cheng, X., Kurner, T., Zhong, Z. D., Guan, K., He, R. S., … Briso Rodriguez, C. (2014). Challenges toward wireless communications for high speed railway. *IEEE Transactions on Intelligent Transportation Systems*, 15(5), 2143 2158. doi:10.1109/TITS.2014.2310771

EEIG ERTMS Users Group. (1998). ERTMS/ETCS RAMS Requirements specification.

Filip, A., Bazant, L., Mocek, H., & Cach, J. (2000). GPS/ GNSS based train position locator for railway signalling. In Computers in Railways VII.

Flammini, F. (2006). *Model based dependability evaluation of complex critical control systems* (Doctor Thesis). University of Naples Federico II, Naples, Italia.

Goverde, R. M., Corman, F., & D'Ariano, A. (2013). Railway line capacity consumption of different railway signalling systems under scheduled and disturbed conditions. *Journal of Rail Transport Planning & Management*, 3, 78 94. doi:10.1016/j.jrtpm.2013.12.001

Kumar, K., & Kumar, P. (2011). Fuzzy availability modeling and analysis of biscuit manufacturing plant: a case study. *International Journal of System Assurance Engineering and Management*, 2(3), 193 204. doi:10.1007/s13198 011 0076 3

Li, X., Zuo, M. J., & Yam, R. C. M. (2006). Reliability analysis of a repairable k out of n system with some

components being suspended when the system is down. *Reliability Engineering & System Safety*, *91*(3), 305 310. doi:10.1016/j.ress.2005.01.010

Liefferinge, M. V., & Paties, L. (2015). Preparing the com munication system for ERTMS. *European Railway Review*, *21*(1).

Mahmood, Y. A., Ahmadi, A., Verma, A. K., Srividya, A., & Kumar, U. (2013). Fuzzy fault tree analysis: A review of concept and application. *International Journal of System Assurance Engineering and Management*, *4*(1), 19 32. doi:10.1007/s13198 013 0145 x

Manz, H., Schnieder, E., Stein, D., Spinder, M., Lauer, M., Baudis, C., ... Marais, J. (2015). GaLoROI. Satellite based localization in railways. In International Congress on Advanced Railway Engineering. Istanbul, Turquie.

Marais, J., Beugin, J., & Berbineau, M. (2017). A survey of GNSS based research and developments for the European railway signaling. *IEEE Transactions on Intelligent Transportation Systems*, *18*(10), 2602 2618. doi:10.1109/TITS.2017.2658179

Marradi, L., Galimberti, A., Foglia, L., Zin, A., Pecchioni, C., Doronzo, M., ... Lekchiri, M. (2012). GNSS for Enhanced Odometry: The GRAIL 2 results. Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing, (NAVITEC), 2012 6th ESA Workshop (pp. 1 7). doi:10.1109/NAVITEC.2012.6423069

Milakis, D., van Arem, B., & van Wee, B. (2017). Policy and society related implications of automated driving: A review of literature and directions for future research. *Journal of Intelligent Transportation Systems*, *21*(4), 324 348. doi:10.1080/15472450.2017.1291351

Min, Y., Chunhui, Y., & Sen, Z. (2013). Reliability model for control center of railway signalling system based on SRN. In *Fourth International Conference on Digital Manufacturing and Automation (ICDMA)*, 2013, (pp. 987 990). doi:10.1109/ICDMA.2013.231

Morant, A., Larsson Kråik, P. O., & Kumar, U. (2016). Data driven model for maintenance decision support: A case study of railway signalling systems. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, *230*(1), 220 234. doi:10.1177/0954409714533680

Nguyen, K., Beugin, J., Berbineau, M., & Kassab, M. (2014). Modelling Communication Based Train control system for dependability analysis of the LTE Communication network in train control application. In European Modelling Symposium. Pise, ITALIE.

Nguyen, K., Beugin, J., Berbineau, M., & Kassab, M. (2015). Analytical approach for evaluating LTE communication errors in train control application. In 1st IEEE ICC 2015 Workshop on Dependable Vehicular Communications. Londres, ROYAUME UNI.

Nguyen, K., Beugin, J., & Marais, J. (2013). Dependability evaluation of a GNSS and ECS based localisation unit for railway vehicles. In 13th International Conference on ITS Telecommunications.

Nguyen, T. P. K., Beugin, J., & Marais, J. (2015). Method for evaluating an extended Fault Tree to analyse the depend ability of complex systems: Application to a satellite based railway system. *Reliability Engineering & System Safety*, *133*, 300 313. doi:10.1016/j.ress.2014.09.019

Qiu, S., Sallak, M., Schön, W., & Cherfi Boulanger, Z. (2014). Availability assessment of railway signalling sys tems with uncertainty analysis using Statecharts. *Simulation Modelling Practice and Theory*, *47*, 1 18. doi:10.1016/j.simpat.2014.04.004

Qiu, S., Sallak, M., Schön, W., & Cherfi Boulanger, Z. (2013). Epistemic parametric uncertainties in availability assessment of a Railway Signalling System using Monte Carlo simulation. In European Safety and Reliability Conference, ESREL 2013. Amsterdam, Netherlands.

Ramdas, V. & Bradbury, T. (2010). ERTMS L3 Risks and Benefits to UK railways (Client final report No. CPR798 PPCA09094). Transportation Research laboratory.

Ran, B., Jin, P. J., Boyce, D., Qiu, T. Z., & Cheng, Y. (2012). Perspectives on future transportation research: Impact of intelligent transportation system technologies on next generation transportation modeling. *Journal of Intelligent Transportation Systems*, *16*(4), 226 242. doi:10.1080/15472450.2012.710158

Rausand, M., & Hoyland, A. (2004). *System reliability the ory: Models, statistical methods, and applications*. Wiley Series in Probability and Statistics Applied Probability and Statistics Section. Hoboken: Wiley.

Roongpiboonsopit, D., & Karimi, H. A. (2009). A multi constellations satellite selection algorithm for integrated global navigation satellite systems. *Journal of Intelligent Transportation Systems*, *13*(3), 127 141. doi:10.1080/15472450903084238

Senesi, F. (2012). Satellite application for train control sys tems: The Test Site in Sardinia. *Journal of Rail Transport Planning & Management*, *2*(4), 73 78. doi:10.1016/j.jrtpm.2013.08.001

Shladover, S. E. (2017). Connected and automated vehicle systems: Introduction and overview. *Journal of Intelligent Transportation Systems*, *22*, 190 200.

Smith, P., Majumdar, A., & Ochieng, W. Y. (2012). An over view of lessons learnt from ERTMS implementation in European railways. *Journal of Rail Transport Planning & Management*, *2*(4), 79 87. doi:10.1016/j.jrtpm.2013.10.004

Sniady, A. (2015). *Communication Technologies Support to Railway Infrastructure and Operations* (Doctor Thesis). Technical University of Denmark, Denmark.

Sniady, A., Soler, J., & Berbineau, M. &. (2013). Performance of LTE in high speed railway scenarios. In *Communication Technologies for Vehicles* (pp. 211 222). Lecture Notes in Computer Science. Berlin: Springer.

Vernez, D., & Vuille, F. (2009). Method to assess and opti mise dependability of complex macro systems: Application to a railway signalling system. *Safety Science*, *47*(3), 382 394. doi:10.1016/j.ssci.2008.05.007

Yasuoka, K., Watabe, A., Hattori, T., & Matsumoto, M. (2011). The policy of applying RAMS to evaluate railway signalling systems for reliable transportation. In E. Schnieder & G. Tarnai (Eds.), *FORMS/FORMAT 2010* (pp. 55 63). Berlin: Springer.

Zimmermann, A., & Hommel, G. (2005). Towards modeling and evaluation of ETCS real time communication and operation. *Journal of Systems and Software.*, *77*(1), 47 54. doi:10.1016/j.jss.2003.12.039 doi:10.1016/j.jss.2003.12.039

Zimmermann, H. J. (2010). Fuzzy set theory. *Wiley Interdisciplinary Reviews: Computational Statistics*, *2*(3), 317 332. doi:10.1002/wics.82

Appendix A

Proofs of lemmas and theorems

Lemma 1. *Considering $\alpha_1 < \alpha_2$, we have: $x_{i_{\alpha_1}}^L \leq x_{i_{\alpha_2}}^L$ and $x_{i_{\alpha_1}}^R \geq x_{i_{\alpha_2}}^R$, then:*

1. $\prod_{i=1}^n x_{i_{\alpha_1}}^L \leq \prod_{i=1}^n x_{i_{\alpha_2}}^L$ and $\prod_{i=1}^n x_{i_{\alpha_1}}^R \geq \prod_{i=1}^n x_{i_{\alpha_2}}^R$.
2. *As the AND gate output probability calculated by Eq.(10), Lemma 1 is obtained.*
3. $\prod_{i=1}^n (1 - x_{i_{\alpha_1}}^L) \geq \prod_{i=1}^n (1 - x_{i_{\alpha_2}}^L)$ *and* $\prod_{i=1}^n (1 - x_{i_{\alpha_1}}^R) \leq \prod_{i=1}^n (1 - x_{i_{\alpha_2}}^R)$.

$$\Rightarrow \begin{cases} 1 - \prod_{i=1}^n \left(1 - x_{i_{\alpha_1}}^L\right) \leq 1 - \prod_{i=1}^n \left(1 - x_{i_{\alpha_2}}^L\right) \\ 1 - \prod_{i=1}^n \left(1 - x_{i_{\alpha_1}}^R\right) \geq 1 - \prod_{i=1}^n \left(1 - x_{i_{\alpha_2}}^R\right) \end{cases}$$

As the OR gate output probability calculated by Eq. (11), Lemma 1 is obtained.

Lemma 2. *1. From Eq. (1), the partial derivatives of z_α with respect to λ_{i_α} and ν_{i_α} can be obtained:*

$$\frac{\partial z_\alpha}{\partial \nu_{i_\alpha}} = -\frac{\lambda_{i_\alpha}}{\left(\nu_{i_\alpha} + \lambda_{i_\alpha}\right)^2}; \; \frac{\partial z_\alpha}{\partial \lambda_{i_\alpha}} = \frac{\nu_{i_\alpha}}{\left(\nu_{i_\alpha} + \lambda_{i_\alpha}\right)^2}$$

As ν_i, $\lambda_i > 0$, then $\frac{\partial z_\alpha}{\partial \nu_{i_\alpha}} < 0$ and $\frac{\partial z_\alpha}{\partial \lambda_{i_\alpha}} > 0$. Therefore, from Eq. (6), we derive Eq. (12).

2. The partial derivatives of z_α (from Eq. 2) with respect to $\lambda_{j_\alpha}, \nu_{j_\alpha}$, we obtain:

$$\frac{\partial z_\alpha}{\partial \nu_{j_\alpha}} = -\frac{\lambda_{j_\alpha}}{\left(\nu_{j_\alpha} + \lambda_{j_\alpha}\right)^2} \prod_{i=1, i/j}^n \frac{\nu_{i_\alpha}}{\nu_{i_\alpha} + \lambda_{i_\alpha}}$$

$$\frac{\partial z_\alpha}{\partial \lambda_{j_\alpha}} = \frac{\nu_{j_\alpha}}{\left(\nu_{j_\alpha} + \lambda_{j_\alpha}\right)^2} \prod_{i=1, i/j}^n \frac{\nu_{i_\alpha}}{\nu_{i_\alpha} + \lambda_{i_\alpha}}$$

As failure and repair rates are positives, then $\frac{\partial z_\alpha}{\partial \nu_{j_\alpha}} < 0$ and $\frac{\partial z_\alpha}{\partial \lambda_{j_\alpha}} > 0$. Therefore, from Eq. (6), we derive Eq. (13).

3. Similar to the OR gate case, we easily derive $\frac{\partial z_\alpha}{\partial \nu_{j_\alpha}} < 0$ and $\frac{\partial z_\alpha}{\partial \lambda_{j_\alpha}} > 0$ after evaluating the partial derivative of z_α with respect to $\lambda_{j_\alpha}, \nu_{j_\alpha}$. Therefore, from Eq. (6), we derive Eq. (14).

4. Similarly, from Eq. (5), we get the partial of derivatives of z_α with respect to λ_α and ν_α, we then easily deduce $\frac{\partial z_\alpha}{\partial \nu_{j_\alpha}} < 0$ and $\frac{\partial z_\alpha}{\partial \lambda_{j_\alpha}} > 0$. Therefore, from Eq. (6), we derive Eq. (15).

Lemma 3. *Considering $\alpha_1 < \alpha_2$, we have:*

$$\begin{cases} \frac{\lambda_{\alpha_1}^L}{\lambda_{\alpha_2}^L} \leq 1 \\ \frac{\nu_{\alpha_1}^R}{\nu_{\alpha_2}^R} \geq 1 \end{cases} \Rightarrow \frac{\lambda_{\alpha_1}^L}{\lambda_{\alpha_2}^L} \leq \frac{\nu_{\alpha_1}^R}{\nu_{\alpha_2}^R} \Rightarrow \lambda_{\alpha_1}^L \nu_{\alpha_2}^R \leq \lambda_{\alpha_2}^L \nu_{\alpha_1}^R$$

$$\Rightarrow \frac{\lambda_{\alpha_1}^L \nu_{\alpha_2}^R - \lambda_{\alpha_2}^L \nu_{\alpha_1}^R}{\left(\nu_{\alpha_1}^R + \lambda_{\alpha_1}^L\right)\left(\nu_{\alpha_2}^L + \lambda_{\alpha_2}^R\right)} \leq 0 \Rightarrow \frac{\lambda_{\alpha_1}^L}{\nu_{\alpha_1}^R + \lambda_{\alpha_1}^L} \leq \frac{\lambda_{\alpha_2}^L}{\nu_{\alpha_2}^R + \lambda_{\alpha_2}^L}$$

Hence, from Eq. (12) we have: $z_{\alpha_1}^L \leq z_{\alpha_2}^L$.

Similarly, we can deduce $z_{\alpha_1}^R \geq z_{\alpha_2}^R$.

Theorem 1. *Firstly, from Lemma 1 and Lemma 3, if fuzzy dependability parameters (such as unavailability probabilities,*

failure/repair rates) of components, noted $\tilde{X}_i$, have non decreasing $x_{i_\alpha}^L$ and non increasing $x_{i_\alpha}^R$ in α, then, the AND/OR gate's output is also a fuzzy number, $\tilde{Z}$ where $z_{i_\alpha}^L$ is non decreasing and $z_{i_\alpha}^R$ is non increasing in α. In other words, the unavailability of the series/parallel system is also a fuzzy number $\tilde{Z}$ whose $z_{i_\alpha}^L$ is non decreasing and $z_{i_\alpha}^R$ is non increasing in α.

Secondly, we prove that it is also true for 2oo3 structure. In fact, from Eq. (15), we have:

$$z_{\alpha_1}^L - z_{\alpha_2}^L = \left[\lambda_{\alpha_1}^L \nu_{\alpha_2}^R - \lambda_{\alpha_2}^L \nu_{\alpha_1}^R\right] \cdots$$

$$\frac{\left[3\left(\lambda_{\alpha_1}^L \nu_{\alpha_2}^R + \lambda_{\alpha_2}^L \nu_{\alpha_1}^R\right)\left(\lambda_{\alpha_1}^L \lambda_{\alpha_2}^L + \nu_{\alpha_1}^R \nu_{\alpha_2}^R\right) + 8\lambda_{\alpha_1}^L \lambda_{\alpha_2}^L \nu_{\alpha_1}^R \nu_{\alpha_2}^R + \left(\lambda_{\alpha_1}^L \nu_{\alpha_2}^R + \lambda_{\alpha_2}^L \nu_{\alpha_1}^R\right)^2\right]}{\left(\nu_{\alpha_1}^R + \lambda_{\alpha_1}^L\right)^3 \left(\nu_{\alpha_2}^R + \lambda_{\alpha_2}^L\right)^3}$$

As we have: $\nu > 0, \lambda > 0$ and $\lambda_{\alpha_1}^L \nu_{\alpha_2}^R \leq \lambda_{\alpha_2}^L \nu_{\alpha_1}^R$, then $z_{\alpha_1}^L - z_{\alpha_2}^L \leq 0$

Similarly, we can deduce $z_{\alpha_1}^R \geq z_{\alpha_2}^R$ as $\nu > 0, \lambda > 0$ and $\lambda_{\alpha_1}^R \nu_{\alpha_2}^L \geq \lambda_{\alpha_1}^L \nu_{\alpha_2}^R$.

Appendix B

List of Abbreviations

CPU	Computer Processor Unit,
DCS	Data Communication System,
DMI	Driver Machine Interface,
eCNS	eLTE Core Network Access System,
ERTMS	European Management System,
ETCS	European Train Control System,
EuroRTM	EuroRadio Transmission Module,
GNSS	Global Navigation Satellite System,
GSM R	Global System for Mobile Communications Railway,
LU Hard	Localization Unit Hardware,
LTE	Long Term Evolution,
MA	Movement Authority,
IE1	Unavailable message from train due to Hardware failures,
IE2	Unavailable signal from train to RBC due to Hardware failures,
IE3	Unavailable signal from RBC to train due to Hardware failures,
IE4	Failed treatment of the received MA at train,
OBU	Onboard Equipment Unit,
PS	Power System,
RBC	Radio Block Center,
TE1	Advanced ETCS unavailability due to Hardware failures,
TE2	Advanced ETCS unavailability due to hardware failures and communication errors,
TIU	Train Interface Unit,
TMR	Triple Modular Redundancy,
UIM	Uncertainty Importance Measure,
WAN	Wide Area Network