applied sciences

MDPI

Article

Collision Risk Evaluation and Verification of GNSS-Based Train Integrity Detection

Kewei Ji [1], Linguo Chai [2,*], Sihui Li [3], Xiangyan Liu [2] and Xiu Pan [4]

[1] School of Traffic and Transportation, Beijing Jiaotong University, Beijing 100044, China; keweiji@bjtu.edu.cn
[2] School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing 100044, China; 17211275@bjtu.edu.cn
[3] Department of Transportation of Hebei Province, Shijiazhuang 050031, China; lisihui@bjtu.edu.cn
[4] Hebei Provincial Communication Planning and Design Institute, Shijiazhuang 050031, China; panxiu@waystone.top
* Correspondence: lgchai@bjtu.edu.cn

Abstract: To meet the demand for middle and low-density railway lines, a Global Navigation Satellite System (GNSS) based on a train integrity monitoring system (TIMS) is used for train integrity detection. Each system has to be analyzed before it is applied in practice. To evaluate the safety of the train integrity detection, a collision risk evaluation method is proposed based on the positioning errors and protection level, in which the Probability of dangerous Failure per Hour (PFH) is computed to quantify the the criteria of Safety Integrity Level (SIL). Then, an experiment-based simulation procedure is presented for safety verification. Statistics results have been obtained from field test data, and simulations are carried out using CPN and MATLAB to verify the collision risk of GNSS-based train integrity detection. The result showed that the GNSS-based train integrity detection satisfies the safety requirements in the system design phase for railway applications.

Keywords: Global Navigation Satellite System; train integrity; Colored Petri Net; safety verification

Citation: Ji, K.; Chai, L.; Li, S.; Liu, X.; Pan, X. Collision Risk Evaluation and Verification of GNSS-Based Train Integrity Detection. *Appl. Sci.* **2021**, *11*, 7764. https://doi.org/10.3390/app11167764

Academic Editor: Paola Pellegrini

Received: 14 July 2021
Accepted: 20 August 2021
Published: 23 August 2021

1. Introduction

In railway freight transport, there might be decoupling accidents that would seriously threaten a train's operation safety. As shown in Table 1, according to the analysis of train integrity-related accidents or events caused by train couplers and traction devices in the United States in the past 40 years (1975–2015) [1], coupler breakage, caused by acceleration, and fault of management or maintenance, leads to train vehicle separation. Without protection, the left behind train vehicles will lead to rear-end collision with the approaching train, which would cause severe casualties and economic loss. Train integrity detection means checking and reporting on train completeness in movement. The train integrity monitoring system (TMIS) is a signaling platform to ensure trains consistently remain intact. Once trains split unintentionally, TMIS will send alarms to the relevant personnel to take appropriate measures to avoid a collision.

A train integrity monitoring system based on on-board equipment is a low-cost solution for freight trains in middle and low-density railway lines. So far, there are train integrity solutions based on brake air pipe pressure, wireless sensor network, and GNSS as presented in reference [2–6]. In these systems, GNSS and other sensors are employed for self-localization and wireless communication. The risks of using GNSS are due to its inherent features [7], especially for safety relevant TIMS. It is necessary to point out the positioning faults or failures when the GNSS-based position is used in TIMS to ensure a safe and reliable position determination. So, a safety evaluation and verification in the system design phase should be done for the development of GNSS-based TIMS. CPN [8,9] has been successfully applied for the modeling and verification of safety-relevant systems, including risk analysis, accident modeling, and system verification [10–12]. Colored Petri

Net (CPN) is selected as the simulation of train positioning errors for the newly developed GNSS-based TIMS.

Table 1. Accidents or events related to train integrity caused by train coupler and traction devices.

Cause of the Accident	Quantity		Type of Accident		
	Count	Percentage	Collision	Derail	Other
Knuckle broken or defective	466	14	93	318	55
Coupler mismatch	387	11.6	41	302	44
Coupler draw head broken or defective	672	20.2	55	585	32
Coupler retainer pin/cross key missing	412	12.4	18	355	39
Draft gear/mechanism broke/defect	423	12.7	19	371	33
Coupler carrier broken/defective	209	6.3	24	175	10
Coupler shank broken/defective	125	3.7	5	110	10
Coupler shank broken/defectivel	11	0.3	-	10	1
Other coupler/draft system	622	18.7	97	446	79
Total	3327	100	352	2672	303

The paper is organized as follows. Firstly, system structure and train integrity detection logic of GNSS-based TIMS are introduced. Secondly, the safety of train integrity detection is evaluated based on the positioning errors and protection level using an indicator of Failure per Hour (PFH) to quantify the criteria of SIL, and an experiment-based Monte Carlo simulation verification procedure is proposed. Finally, simulations are carried out by CPN and MATLAB using the statistics from field tests.

2. GNSS-Based Train Integrity Detection

A typical GNSS-based TIMS consists of a ground monitoring center, Head-of-Train (HoT), and End-of-Train (EoT) units. An integrated train positioning system (in Figure 1), including a BDS, GPS, and inertial measurement unit (IMU), is employed to monitor the dynamic state of trains. EoT-HoT and train-ground communication are achieved by The General Packet Radio Service (GPRS) wireless channel. Messages from EoTs and HoTs are gathered by the train's integrity detection software in the ground monitoring center, where the train's integrity decisions are made.

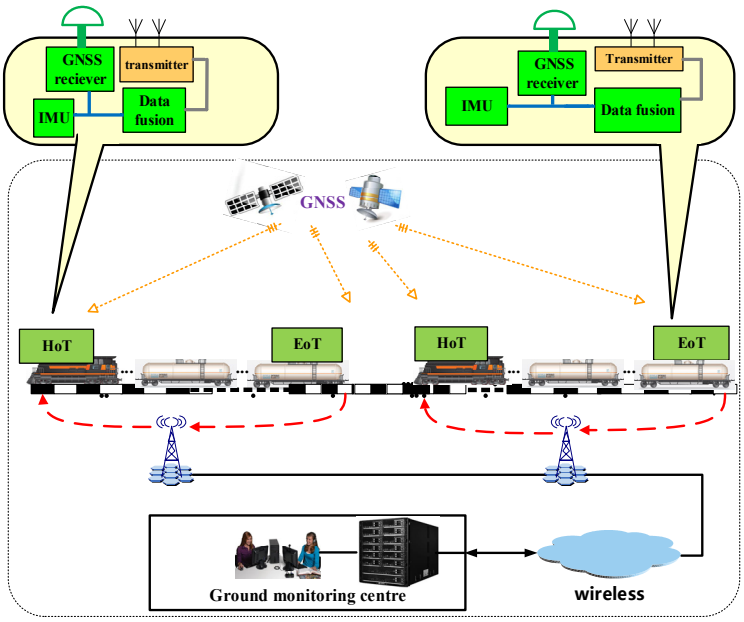


Figure 1. Structure of a typical GNSS-based TIMS.

The ground monitoring center receives the train's location messages, such as traveling mileage, velocity, and direction, and the train's integrity and potential collision will be detected. Any warning would be sent to the managers and drivers to take safety action to avoid accidents. The TIMS should locate the train position, detect loss of train integrity (accidental train parting) and also point out the potential collision. The detailed timeline of a train's integrity detection under potential collision risk is illustrated in Figure 2.

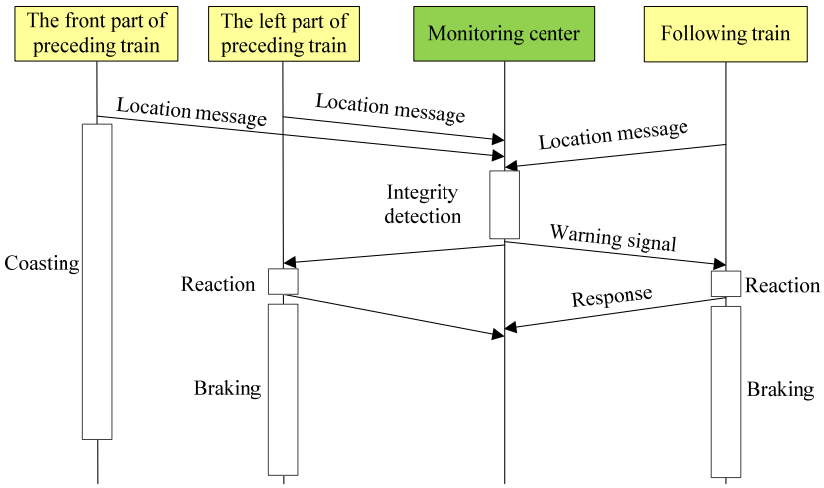


Figure 2. Timeline diagram of a train integrity detection under potential collision risk.

In the GNSS-based TIMS, an undetected train parting is a dangerous failure. When a limited safe time is exceeded, the undetected train breakage will lead to a rear-end collision. For the development of the safety-relevant GNSS-based TIMS, the safety evaluation and verification should be done based on a simulation in the system design phase.

TIMS is based on GPS/BDS and integrated with an IMU sensor to realize train localization. The GNSS-based train position error is the absolute difference between the estimated position and the actual position in two dimensional space [1,2], while the protection level (PL) is the uncertainty of location estimation, extending in a bounded domain under a certain confidence probability [13,14], bound to the horizontal PL with a probability derived from the integrity requirement (see Figure 3). Then we can form a safe train position description.

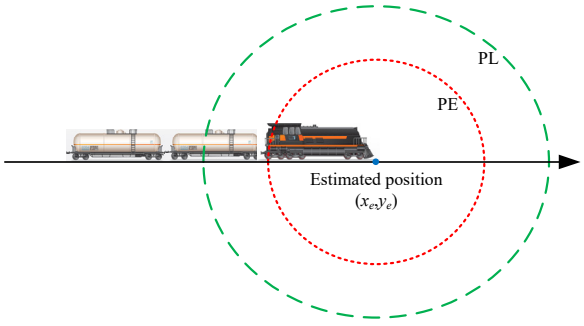


Figure 3. PE and PL in the GNSS-based train positioning.

3. Collision Risk Evaluation of Train Integrity Detection

The EN 50129 standard is a common basis for railway executives, recognizing and approving safety-relevant systems for signaling in railway applications [15]. EN 50129 and EN 50126 [16] can both quantitatively and qualitatively assess the risk. The IEC 61508 standard [17] thus defines quantitative safety requirements for each SIL. The quantitative requirements for the standard are summarized in Table 2, where the SILs are differentiated

by using the Probability of dangerous Failure per Hour (PFH), showing the quantitative SIL requirements with a minimal and maximal boundary.

Table 2. Quantitative SIL requirements.

Safety Integrity Level	Probability of Dangerous Failure per Hour (PFH)/h
SIL 4	$10^{-9} \leq \text{PFH} < 10^{-8}$
SIL 3	$10^{-8} \leq \text{PFH} < 10^{-7}$
SIL 2	$10^{-7} \leq \text{PFH} < 10^{-6}$
SIL 1	$10^{-6} \leq \text{PFH} < 10^{-5}$

Determining the probabilistic aspects of SIL for safety functions is performed differently [17]. The supplier designs the system safety and verifies these specifications using the dependability parameters of the components integrated in the system. The Probability of Failure on Demand (PFD) [17] is used to determine the PFH value related to a SIL (see Table 2). PFH is calculated during the system design analysis.

$$\text{PFH} = \frac{\text{PFD}(T_i)}{T_i} \tag{1}$$

In which T_i is the time interval between two proof tests, identical for the different subsystems.

A probabilistic analysis is about assessing the probability that a method is satisfying one or more performance criteria. It is up to the analyst to formulate what constitutes acceptable performance, or conversely failure, for the method under consideration. The limit state concept provides a unified framework for expressing the probability of failure definitions, which defines the boundary between the safe and unsafe regions of the design space. In terms of the detection threshold and measuring results, whether a system is safe or not is captured by one quantity, which is referred to as the performance function and is commonly denoted by Z. More generally, the performance function may be expressed in terms of all of the basic random variables in the problem:

$$Z = \Pr\left\{ \bigcap_{j=1}^{m} G_j(\Theta) < 0 \right\} \tag{2}$$

In which $\Pr\{\cdot\}$ stands for the probability of the random event in the bracket, and $\Theta = (\Theta_1, \Theta_2, \ldots \Theta_s)$ being the measurement variables. As shown in Figure 4, $G_j(\cdot)$ is the limit state function. The notation $G(\cdot) < 0$ denotes the failure region. Likewise, $G(\cdot) = 0$ and $G(\cdot) > 0$ indicate the failure surface and safe region, respectively.

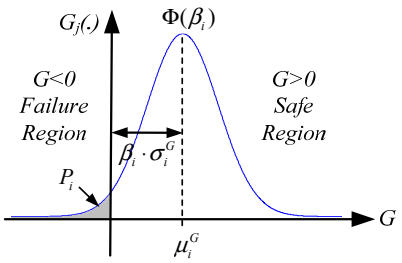


Figure 4. The probabilistic analysis method.

For the GNSS-based train integrity detection, the limit-state indicates the margin of safety between the detection threshold and the estimated train positioning results. The limit state function $G_j(\cdot)$ can be described as:

$$G_j(\Theta_j) = D - \Theta_j \tag{3}$$

where

$D = L_d$ is the train integrity detection threshold;

Θ_j, $j = 1, 2$ are the positioning results. As Figure 5 shows, $\Theta_1 = L_e$ is the estimated train length and $\Theta_2 = L_p$ is the train protection length.

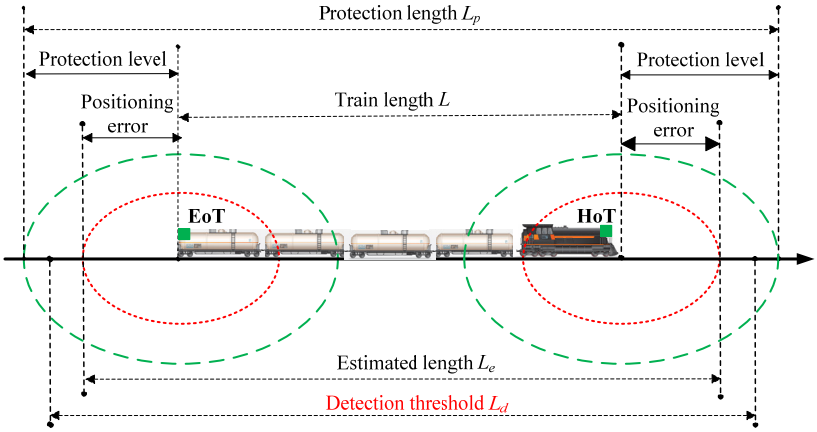


Figure 5. The distributed structure of the train integrity detection.

We assume in GNSS-based positioning that PE and PL are normally distributed $\Theta_j \sim N(\mu_{\Theta_j}, \sigma_{\Theta_j})$. The mean and standard deviation of the limit-state, $G(\cdot)$, can be determined from the elementary definition of the mean and variance, $G \sim N(\mu_G, \sigma_G)$. Where $\mu_G = \mu_D - \mu_\Theta$ is the mean. μ_D and μ_Θ are the means of D and Θ_j, respectively. $\sigma_G = \sqrt{\sigma_D^2 + \sigma_\Theta^2 - 2\rho_{D\Theta}\sigma_D\sigma_\Theta}$ is the standard deviation. Thus, the probability of failure is

$$R_\Theta = \int_{-\infty}^{0} f_G(G)dG = 1 - \Phi(\beta) = \Phi(-\beta) \tag{4}$$

where

$\beta_i = \frac{\mu_i^G}{\sigma_i^G} = \frac{\mu_i^R - \mu_i^S}{\sigma_i^R + \sigma_i^S}$ is defined as the safety index. Values of β for typical values of $G(\cdot)$ are shown in [18].

$\Phi(\cdot)$ is the standard normal cumulative distribution function.

Kalman filter (KF) is employed to solve the Bayesian filtering problem and obtain the state estimation results in GNSS-based train position estimation. Variation of PL is determined by relevant information from the Kalman filtering process. Besides, an efficient way is to project the test statistic to the position domain by using the uncertainty of position estimation.

The first step for identifying PL is to carry out the state estimation by fusing information with the system model and sensor measurement. Assume that h_k denotes the state vector at instant k that describes the dynamic state of a train moving along the track; the system model for fusion is:

$$\begin{aligned} h_k &= A_{kt}h_{k-1} + \eta \\ y_k &= B_k h_k + w \end{aligned} \tag{5}$$

where A_k is the active transition matrix at time k; B_k is the active emission matrix at time k. η and w are the independent Gaussian transitions and observation noises, and y_k is the observation vector with instant sensor measurement. As the definition of filtering state, the horizontal position uncertainty of PL can be calculated as

$$\mathrm{PL} = \gamma_k \cdot \sigma_k \tag{6}$$

where γ_k is the factor determined to reflect the probability of missed detection of PL, and the value γ_k = 6.18 indicates a probability of missed detection of 5×10^{-9} [19]. σ_k is the is the estimation residual in KF [14].

For GNSS-based train localization, the probability of failure, risk of GNSS integrity monitoring, which indicates the positioning error exceeding PL, can be calculated as:

$$R^f = \Phi\left(\frac{-\mathrm{PL} - \mu}{\sigma}\right) + 1 - \Phi\left(\frac{\mathrm{PL} - \mu}{\sigma}\right) \tag{7}$$

where μ and σ are the mean and variance of the position estimation error $\hat{h}_k$.

Then we can work out the safety risk of train integrity. As shown in Figure 5, there are two different situations in train integrity monitoring:

- $L_e < L_p < L_d$

The detection threshold L_d is lower than the measured train length L_e and protection length L_p. Then, $R_k = \Pr\{G_1(\Theta) < 0 \cup G_2(\Theta) < 0\} = \Pr\{G_2(\Theta) < 0\}$ and the PFD can be derived as:

$$\mathrm{PFD}_k = \Pr\{G_2(\Theta) < 0\} = R^f \times R_{\Theta_2} \tag{8}$$

- $L_e < L_d < L_p$

The detection threshold L_d is bigger than the measured train length L_e and lower than the protection length L_p. Then $R_k = \Pr\{G_1(\Theta) < 0 \cup G_2(\Theta) < 0\} = \Pr\{G_1(\Theta) < 0\}$, and the PFD can be derived as:

$$\mathrm{PFD}_k = \Pr\{G_1(\Theta) < 0\} = R_{\Theta_1} \tag{9}$$

If the train parting is still not detected in the limited safe time, a rear-end collision will occur. Then we can get the safety risk for collision in GNSS-based train integrity detection:

$$\mathrm{PFH} = \frac{3600}{m} \sum_{k=1}^{m} \mathrm{PFD}_k \tag{10}$$

where m is the limited safe time. In the train control system, the time interval between the adjacent two trains is greater than the train braking time, as illustrated in Table 3 [20]. There are differences in the train coasting time and braking coefficient between full-service braking and emergency braking. In this paper, the limited safe time m is chosen as the same as the full-service braking time according to the velocity, and on the assumption that the following train shares the same velocity with the preceding train.

Table 3. Train braking time in train control system.

Velocity (km/h)	300~0	250~0	200~0	160~0	100~0
Emergency braking time (s)	74.2	60.6	47.1	37.5	23.2
Full-service braking time (s)	113.1	88.1	63.6	48.1	31.3

4. Experiments Based Simulation for Collision Risk Verification

For each specific scenario in GNSS-based TIMS constructed from the attributes of the operating situation (both GNSS positioning situation and train motion situation), the probability of a specific event in a scenario depends on the frequency range assigned to the safety function [21].

To consider the influence of the environment along train routes, it is obviously impossible to describe a limited number of representative geometries to cover all situations of signal visibility. Environmental configurations along the train itinerary present identical geometry features. The area around this itinerary constitutes a "typical" environment. Safety results can then give representative characteristics for the different typical environments observed [21]. The GNSS-based positioning system can be decomposed as a state to help

identify the system performance level. These states of GNSS in TIMS are related to location measurements. So from the GNSS receiver perspective, three states are defined for the GNSS receiver locations. These three states [21] are upstate, degraded state, and faulty state, as shown in Figure 6.

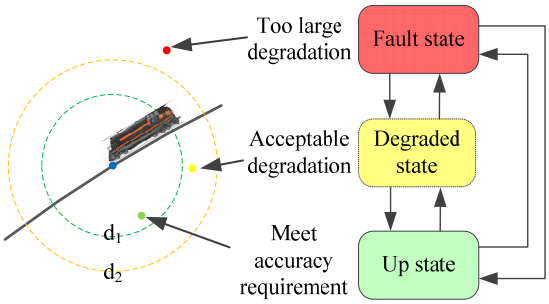


Figure 6. State of train positioning.

The measured position of the GNSS-based positioning unit is the most important factor for train parting incident detection. So, a hazardous event is more likely to occur when the localization function reaches the degraded state and fault state. A train, which has been wrongly positioned, can lead to unexpected estimated train length and false detection results. This situation can lead to a rear-end collision. Safety activities on a GNSS-based TIMS concentrate on these states of GNSS-based localization.

The Monte Carlo simulation is a numerical process that is able to generate both GNSS positioning errors and train parting sequences composed of dependent situations where failure frequencies are subject to uncertainty [22]. Several possible evolutions in the life of the system (i.e., the dynamic transitions of the GNSS positioning system in an up or degraded state) can be obtained with a Monte Carlo simulation. In GNSS-based applications in railways, we use an Experience Statistics (ES) methodology [7] to obtain an efficient procedure capable of managing a huge quantity of data in order to evaluate the safety properties of GNSS-based positioning. This approach follows the usual steps that we have here adapted to the GNSS localization.

To determine the accuracy of an estimated position, a reference is needed. The inertial navigation sensors and other technical solutions-based reference systems can provide an accurate reference for measurement data evaluation. Figure 7 illustrates the proposed ES-based Monte Carlo simulation procedure, which begins with this data collection and continues with several processing steps:

- Step 1, a selection is carried out by the amount of collected data stemming from receiver output files. They constitute raw data that are unworkable for a safety evaluation. Useful data leading to the position estimation are extracted at each sampling instant. Then the useful data are processed to obtain information related to correct and hazardous states. To determine if there is a failure or not, a position has to be compared with the true position (the reference). The obtained information leads to quantitative values that can be subsequently analyzed statistically in order to get safety results
- Step 2, the typical testing scenarios can be simulated by different probabilities from Step 1. The system states of GNSS-based positioning in each scenario will be defined and transformed to each other. Aligned with time, states, and scenarios, positioning errors are obtained with the normal distribution, of which the mean and variant can be found from the statistics.
- Step 3, the train motion of both the preceding train and following train will be simulated with different velocities and accelerations. Integrated with positioning errors, the train movement state can employ a Kalman filter to compute the protection level. With different train operation situations, the limited safety time, simulation time, and detection time can be found. Based on the detection threshold, a limit-state-based prob-

ability method will be applied to get the PFD and PFH. Finally, the SIL of GNSS-based TIMS in the design phase are achieved.

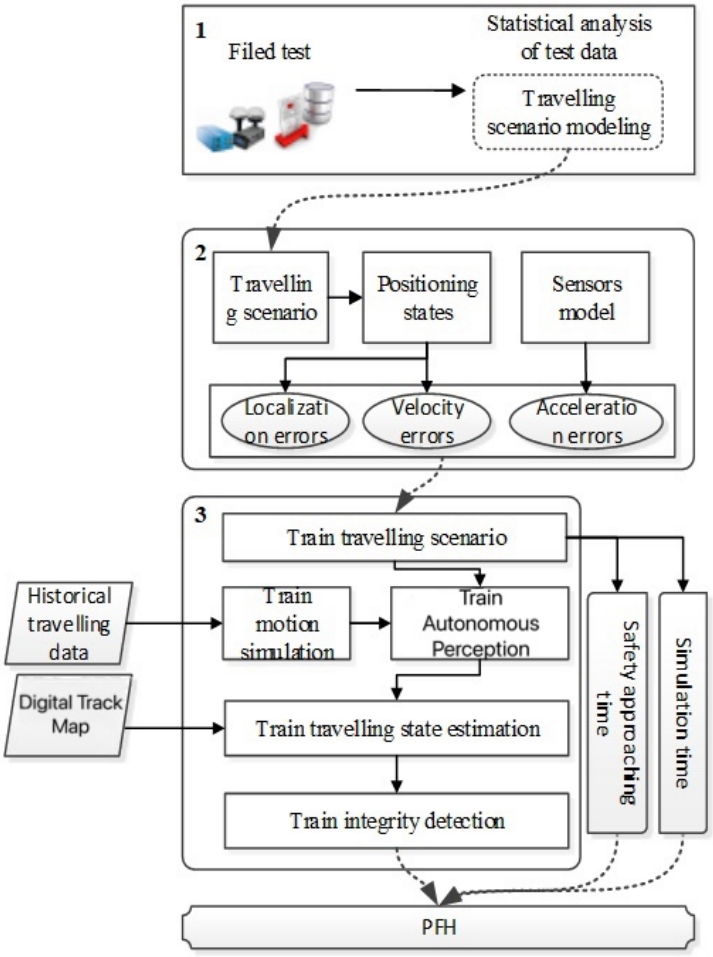


Figure 7. Verification procedure based on the analysis of experiments data.

5. Simulation and Results

To obtain different scenarios and positioning states, raw data are collected as follows: the runs of a train equipped with a GPS receiver and reference system are tested in order to evaluate the positioning errors. The GNSS and the reference location data were collected along the High Tatra Mountain railway line from May 2008 to February 2009 (see Figure 8) [23–26], and the deviation between GNSS receiver and reference locations is calculated for performance evaluation.

Figure 8. Map of the field data.

The High Tatra Mountain railway line is 29.1 km long from Poprad to Smokovec until Strbske Pleso. There are open areas and forests but no tunnels or railway bridges. The thresholds for the required train localization function are set as an upstate threshold of 10 m, and the positioning deviations bigger than 10 m and lower than 20 m are set as the degraded state. A faulty state is defined when the deviation is bigger than 20 m, which indicates it ceases to be a localization function and is no longer available as a resource for the localization function. Then, the statistics of positioning errors in different scenarios (open area and forest) and localization states (upstate, degraded state and fault state) are found out [27], as shown in Table 4. Since the mean and variance of deviation normal distribution in upstate from the test run are chosen, the mean and variance of the other two states are set depending on the thresholds.

Table 4. Statistics of GNSS positioning errors.

Scenarios		**Open Area**			**Forest**		
Percentage		98%			2%		
States		Upstate	Degraded State	Fault State	Upstate	Degraded State	Fault State
Percentage		95.78%	3.26%	0.96%	73.69	7.92%	18.39%
Positioning error	μ(m)	6.84	16.84	26.84	8.96	18.96	28.96
	σ(m)	24.11	24.11	24.11	29.71	29.71	29.71

Not only the localization states but also the transitions between the states are considered here. The mean time of the six transitions can be found out from the measured individual time span staying in one state to another. The mean times from one state transition to another are categorized, and the results [27] of all six transitions are estimated in Table 5.

Table 5. Distribution of Each Transition and Parameters.

Transition	**Mean Time (s)**	**Corresponding in CPN Model**
upstate to degraded state transition	15.31	UP_DE
degraded state to upstate transition	2.46	DE_UP
upstate to faulty state transition	20.79	UP_FA
faulty state to upstate transition	5.91	FA_UP
degraded state to faulty state transition	2.88	DE_FA
faulty state to degraded state transition	6.71	FA_DE

The procedure is based on the statistically processed fieldmeasurements. One scenario is a sequence constituted of a succession of states associated with the localization function. The transition between the different states is also associated with time. Figure 9 illustrates scenarios (open area with white color and forest with grey color) in which states (upstate with green color, degraded state with yellow color, and fault state with red color) are distinguished at each sampling instant using unit steps and colors.

Because of the timed and stochastic nature of the GNSS-based positioning system, formal and simulation-based verification are combined to generate the GNSS positioning errors. The CPN model of the GNSS positioning errors is shown in Figures 10 and 11. In order to evaluate the existing or planned systems, a performance analysis is conducted. In CPN, each token can be parameterized with the required meaning, which is not available in low-level Petri Nets. By adapting values to corresponding quantities, the system can be easily understood and changed, then described in executable code. During simulation-based performance analysis, data is collected from the occurring binding elements, and the markings reached [15]. With the data obtained from the model, performance measures of the GNSS-based TIMS are available.

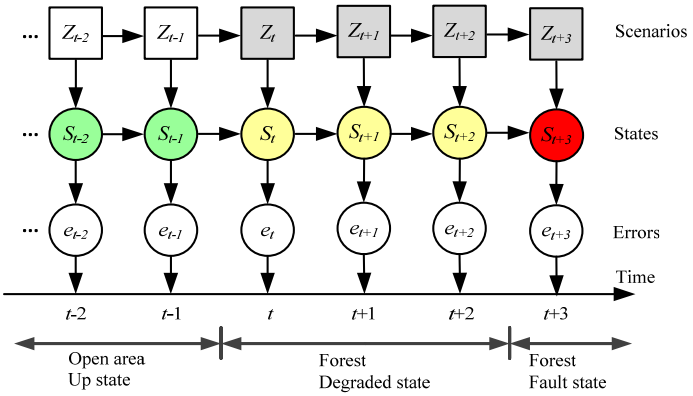


Figure 9. Test scenarios and transition.

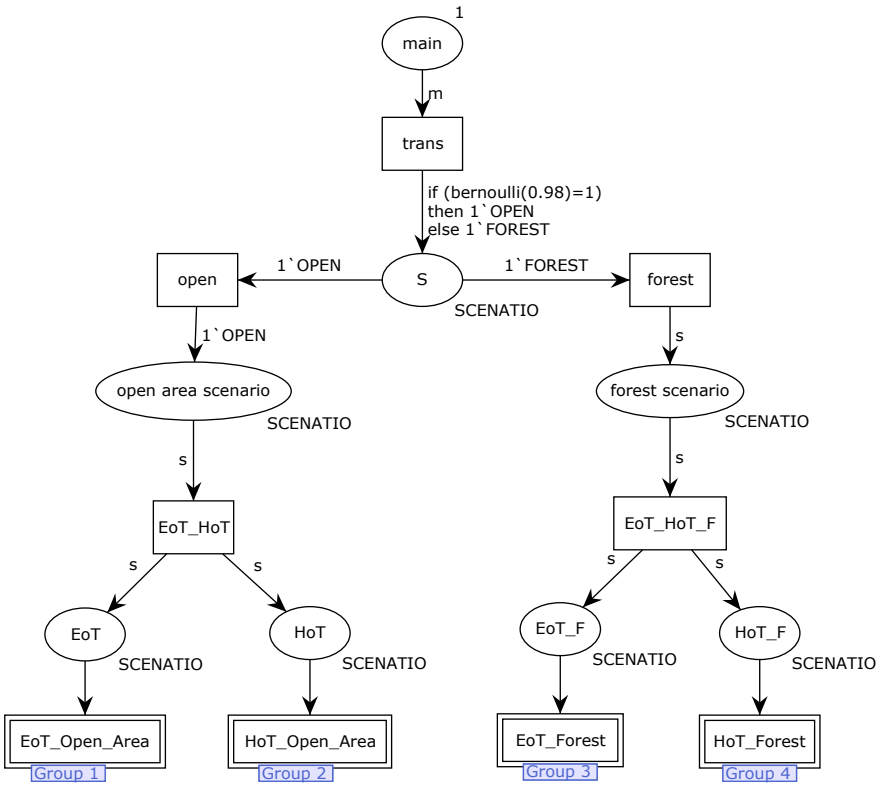


Figure 10. First layer CPN model of scenario in detail.

The model is divided into two layers; the first layer (see Figure 10) includes EoT and HoT in open area scenarios and forest scenarios. As shown in Figure 11, the second layer described each scenario in detail; parameterization was done in this layer (EoT_Open_Area, HoT_Open_Area, EoT_Forest, and HoT_Forest share the same model structure in Figure 11, different parameters according to Table 4). Relative time and distributions characteristics are involved in the second layer; position error data can be extracted from up_data, degraded_data, and faulty_data.

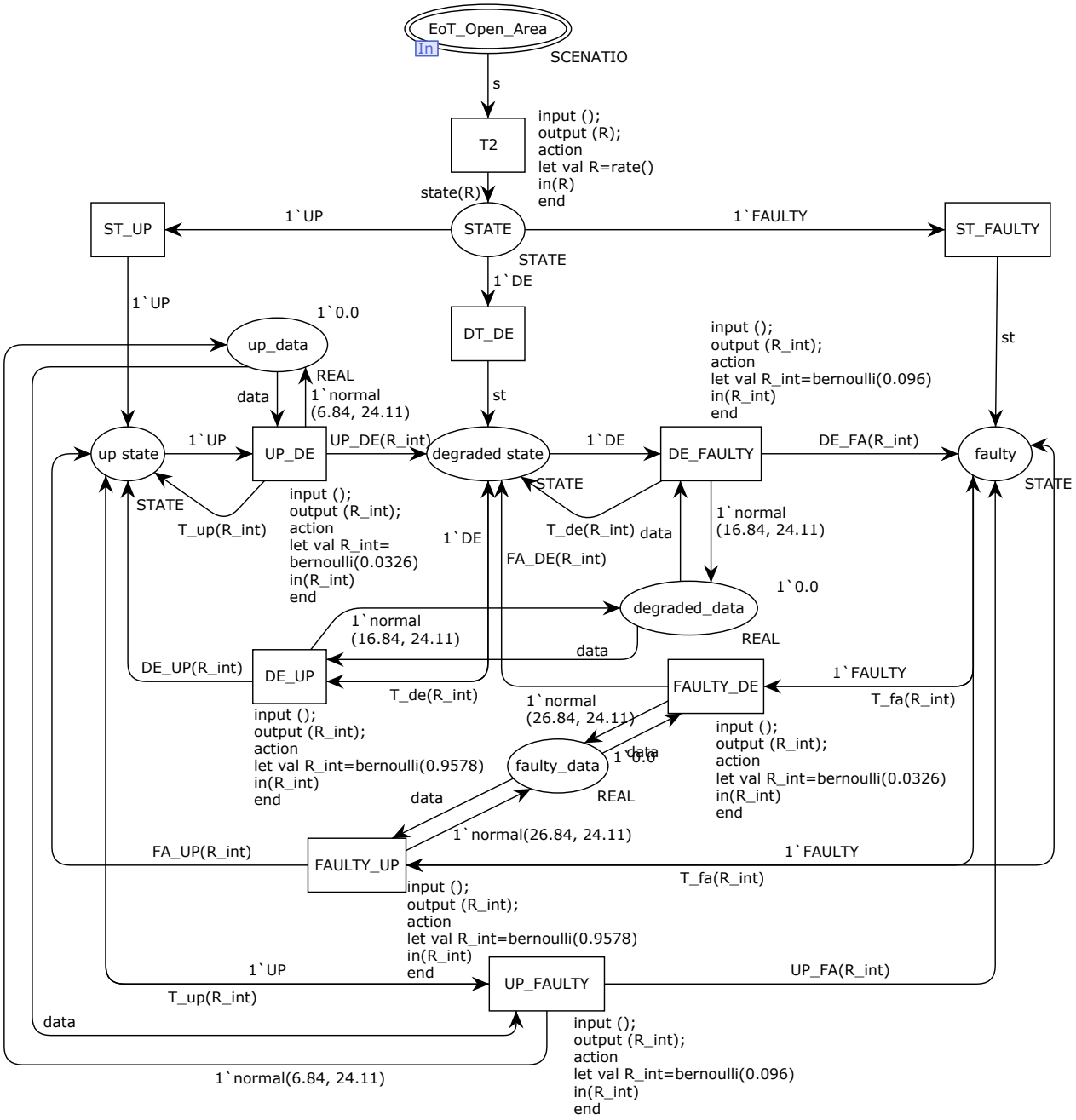
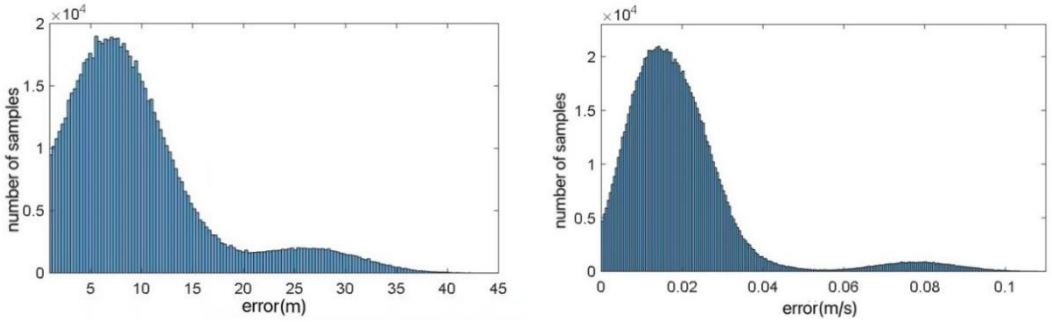


Figure 11. Second layer CPN model of scenario in detail.

The off-line data positioning errors (see Figure 12) aligned to simulation time from CPN tools are imported into MATLAB and integrated with the train motion simulation. The train motion simulation generates kinematic data (i.e., position, velocity, and acceleration) of both HoT and EoT. Train parting events are so rare that they do not provide enough information for statistical analysis, and we cannot have a true experiment yet. To take into account each parameter subject to failure, train parting processes are simulated with different relative distances, velocities, and accelerations over a mission time to provide an interval of time-dependent probabilities for the train integrity detection. Hence in this Monte Carlo process, the system states evolve, while the operating context remains the same and experiences all the possible GNSS localization and train operation scenarios and states.



(**a**) simulated positioning error (**b**) simulated velocity error

Figure 12. Simulated positioning error and velocity error.

The autonomous positioning error of offline data corresponding to the simulation time from the CPN tool (see Figure 5) are imported into MATLAB and combined with the simulation data of train motion characteristics to generate kinematic data (i.e., position, speed, and acceleration) for evaluating hot and EoT. Due to the severity and contingency of train separation accidents, they cannot provide enough measurement information for a statistical analysis, and it is difficult to carry out corresponding field tests. In order to consider the parameters of each safety failure model, different relative distances, speeds, and accelerations are used to simulate the train separation process in order to provide the time-dependent probability interval of train integrity detection. Therefore, through the Monte Carlo simulation process of multi-level state transition, train integrity detection results of all simulation operation scenarios, environment scenarios, train positioning status, train integrity status, and other system's multi-level state evolution can be completed.

For accelerometers, the sensor error includes three parts: bias, temperature drift, and random interference. Taking the measurement result of the x-axis of the accelerometer as an example, the error model [28] is as follows:

$$\hat{a} = (1 + S)a + B_f + n \tag{11}$$

The meaning of each symbol in the formula is as follows: $\hat{a}$ is the measured value of acceleration; a is the actual acceleration; S is the scale factor error; B_f is the zero bias error; n is the random noise error.

In order to verify the performance of the proposed train integrity detection based on autonomous perception, this paper takes the actual operation of the Ge NJ2 train on Qinghai Tibet Railway as an example and uses the combination of measured data and numerical simulation data to verify the performance of the train operation state estimation, train integrity detection and collision risk evaluation and verification. See Table 6 for the main parameters of the Ge NJ2 train.

Table 6. Main parameters of NJ2.

Performance Parameter Category	Parameter Characteristics
Locomotive length	21 m
Maximum operating speed	120 km/h
Brake type	CCBII
Maximum acceleration	7.2 km/h/s
Maximum deceleration	14.4 km/h/s
Dead-weight	13.8 t

The simulated train operation time of the train parting process in every single simulation is 100 s. Every set of simulation tests include 2700 simulation tests, in which the velocity increases from 0 to 50 m/s (almost the maximum velocity that a freight train can reach) by 1 m/s and the acceleration from 0 to 0.54 m/s^2 (maximum traction acceleration)

by 0.01 m/s^2. Kalman filtering is employed to smooth the data and compute the protection level. Based on the positioning errors and protection level (see Figure 13), the train integrity detection threshold is set to be 50 m. Then a safety evaluation procedure is launched, and plenty of PFDs in different simulations are computed. As presented in Figure 14, a set of simulation tests with all the train motion situations show the calculated PFD. The results show that the PFD varies from 10^{-20} to 10^{-50}, and higher PFD's have smaller velocity and acceleration.

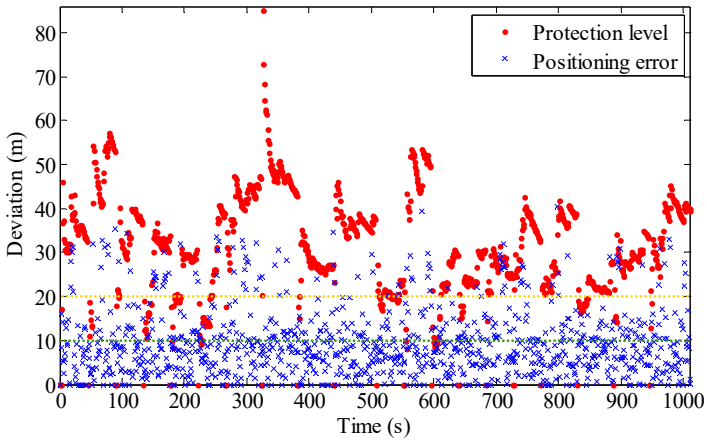


Figure 13. Simulated positioning error and protection level.

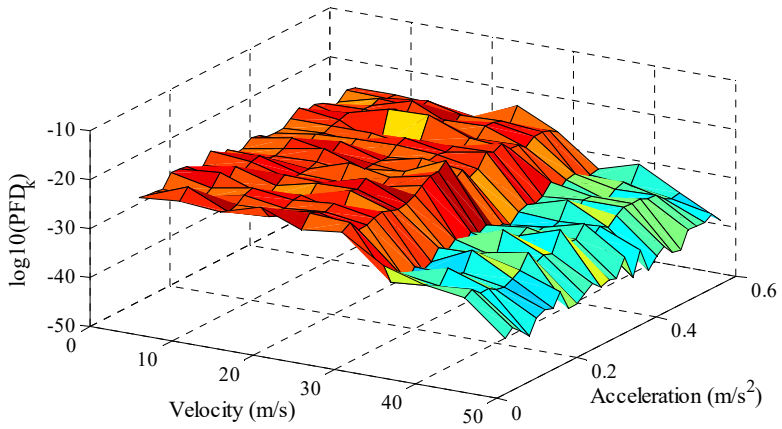


Figure 14. Collision risks in one simulation test.

Due to the limit of computing performance, 50 sets of simulation tests are carried out, and the total simulated train operation time is 1.35×10^{-7} s. Plenty of PFD in both different GNSS localization scenarios and states and train motion states are calculated and followed by the PFH with simulated train operation time. The calculated PFH (see Figure 15) in the 50 sets of simulation range from 10^{-23} per hour to 10^{-35} per hour.

An average PFH = $10^{-25.1482}$ is found, in reference to the corresponding relationship of SIL and PFH, the value of the PFH goes into SIL4. Additionally, in the simulated 3750 h of train operation, no collision accidents happen. Consequently, GNSS technologies can be applied in safety-related TIMS. Yet it is worth more time to verify, since the results of SIL quantities were gained over a limited time period. To improve the performance of GNSS-based train integrity detection, an innovative method should be offered.

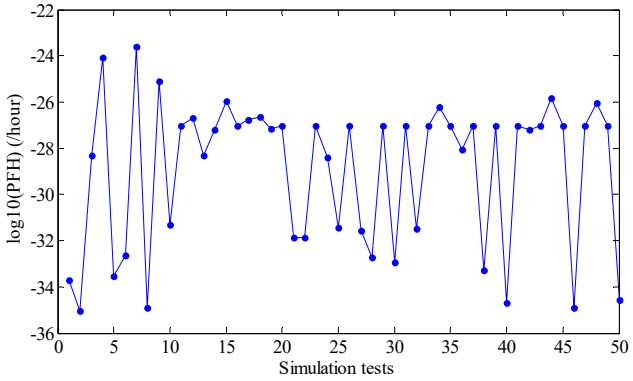


Figure 15. The PFH in 50 sets of simulation tests.

6. Conclusions

This paper proposed methods of formal and Monte Carlo simulation-based collision risk evaluation and verification of GNSS-based Train integrity Monitoring Systems. When GNSS in applied in TIMS, the positioning error is the uncertain factor in train integrity detection. Based on the positioning errors and protection level from the filtering, the collision risk evaluation method is proposed by using PFH to quantity the SIL. To verify the collision risk of GNSS-based TIMS, an experiment-based Monte Carlo simulation procedure is presented. In the simulation, GNSS localization statistics are found from the field test in the High Tatra Mountain railway line. The CPN is employed to simulate the positioning errors based on the testing scenarios and states, then the protection level is computed in MATLAB, and the PFH is derived. The simulation results show that the GNSS-based TIMS satisfies the safety requirements in the system design phase for railway applications.

Future research will concentrate on the more complex scenarios of both GNSS localization and TIMS operation for simulation. In the next phase of system development, more real system operation data should be collected and analyzed to further evaluate the train integrity detection performance.

Author Contributions: Collision Risk Evaluation, K.J.; train integrity, L.C.; colored Petri Net, S.L.; safety verification, X.L.; simulation procedure, X.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by National Key Research and Development Program of China (2018YFB1600600), National Natural Science Foundation of China (61903024), S&T Program of Hebei(20310801D), Beijing Natural Science Foundation (L191013).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Federal Railroad Administration Office of Safety Analysis. Available online: http://safetydata.fra.dot.gov/OfficeofSafety (accessed on 12 November 2016).
2. Pacific Southwest Railway Museum Association. Available online: http://www.sdrm.info/faqs/brakes/history/ (accessed on 5 October 2015).
3. Scholten, H.; Westenberg, R.; Schoemaker, M. Trainspotting, a WSN-based train integrity system. In Proceedings of the ICN 2009—International Conference on Networks, Le Gosier, France, 1–6 March 2009; pp. 226–231.
4. Oh, S.; Yoon, Y.; Kim, K.; Kim, Y. Design of train integrity monitoring system for radio based train control system. In Proceedings of the ICCAS 2012—12th International Control, Automation and Systems Conference, JeJu Island, Korea, 17–21 October 2012; pp. 1237–1240.
5. Acharya, A.; Sadhu, S.; Ghoshal, K. Train localization and parting detection using data fusion. *Transp. Res. C-Emerg. Technol.* **2011**, *19*, 75–84. [CrossRef]

6. Li, S.; Cai, B.; Shangguan, W.; Schnieder, E.; Toro, F.G. Switching LDS detection for GNSS-based train integrity monitoring system. *IET Intell. Transp. Syst.* **2017**, *11*, 299–307. [CrossRef]
7. Beugin, J.; Marais, J. Simulation-based evaluation of dependability and safety properties of satellite technologies for railway localization. *Transp. Res. C-Emerg. Technol.* **2012**, *22*, 42–57. [CrossRef]
8. Jensen, R.G.; High-Level, K. *Petri Nets: Theory and Application*; Springer: Berlin/Heidelberg, Germany, 1991.
9. Jensen, K. *Coloured Petri Nets. Basic Concepts, Analysis Methods and Practical Use*; Springer: Berlin/Heidelberg, Germany, 1992.
10. Vernez, D.; Buchs, D.; Pierrehumbert, G. Perspectives in the use of coloured Petri nets for risk analysis and accident modelling. *Saf. Sci.* **2003**, *41*, 445–463. [CrossRef]
11. Fanti, M.P.; Giua, A.; Seatzu, C. Monitor design for colored Petri nets: An application to dead lock prevention in railway networks. *Control Eng. Pract.* **2006**, *14*, 1231–1247. [CrossRef]
12. Son, H.S.; Seong, P.H. Development of a safety critical software requirements verification method with combined CPN and PVS: A nuclear power plant protection system application. *Reliab. Eng. Syst. Saf.* **2003**, *80*, 19–32. [CrossRef]
13. ICAO. Annex 10 (Aeronautical Telecommunications) to the Convention on International Civil Aviation, 2006. Volume I—Radio Navigation Aids, International Standards and Recommended Practices (SARPs). In *ICAO Doc. AN10-1*, 6th ed.; ICAO: Montreal, QC, Canada, 2006.
14. Liu, J.; Tang, T.; Cai, B.G.; Wang, J.; Chen, D.W. Integrity assurance of GNSS-based train integrated positioning system. *Sci. China Technol. Sci.* **2011**, *54*, 1779–1792. [CrossRef]
15. European Committee for Electrotechnical Standardization. *CENELEC, EN 50129. Railway Applications: Safety Related Electronic Systems for Signalling*; European Committee for Electrotechnical Standardization (CENELEC): Brussels, Belgium, 1998.
16. European Committee for Electrotechnical Standardization. *CENELEC EN 50126: Railway Applications—The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*; CENELEC: Brussels, Belgium, 2007.
17. International Electrotechnical Commission. *IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems (IEC 61508-1 to 7)*; IEC: Geneva, Switzerland, 2000.
18. Cornell, C.A. A probability-based structural code*. *ACI J. Proc.* **1969**, *66*, 974–985.
19. Diesel, J.; Luu, S. GPS/IRS AIME: Calculation of thresholds and protection radius using Chi-square methods. In Proceedings of the 8th International Technical Meeting of the Satellite Division of the Institute of Navigation, Palm Springs, CA, USA, 12–15 September 1995; pp. 1959–1964.
20. Ning, B.; Tang, T.; Li, K.C. *Transportation Bureau of MOR, System Requirements Specification for CTCS-3 Train Control System (v1.0)*; China Railway Publishing House: Beijing, China, 2009.
21. Lu, D.; Schnieder, E. Performance Evaluation of GNSS for Train Localization. Intelligent Transportation Systems. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 1054–1059.
22. Beugin, J.; Renaux, D.; Cauffriez, L. A SIL quantification approach based on an operating situation model for safety evaluation in complex guided transportation systems. *Reliab. Eng. Syst. Saf.* **2007**, *92*, 1686–1700. [CrossRef]
23. Jonáš, M. GNSS integrity for railway transportation. *Trans. Transp. Sci.* **2011**, *4*, 183–192. [CrossRef]
24. Poliak, J. Validierung von Satellitenbasierten Eisenbahnortungssystem. Ph.D. Thesis, Technische Universität Braunschweig, Braunschweig, Germany, 2009.
25. Lemmer, K.; Schnieder, E.; Stiller, C. *Entwicklung eines Demonstration für Ortungsaufgaben mit Sicherheitsverantwortung im Schienengüterverkehr: DemoOrt. Abschlussbericht der Phasen 1 und 2*; DLR: Braunschweig, Germany, 2009.
26. Becker, U.; Poliak, J.; Geistler, A.; Hasberg, C.; Hörste, M.M. DemoOrt repositions trains with satellite. *EURAILmag Bus. Technol.* **2008**, *18*, 216–219.
27. Lu, D. GNSS for Train Localisation Performance Evaluation and Verification. Ph.D. Thesis, Technische Universität Braunschweig, Braunschweig, Germany, 2014.
28. Paul, D.G. *Principle of GNSS, Inertial and Multisensor Integrated Navigation Systems*; Artech House: London, UK, 2008.