Analysis of safe and effective next-generation rail signalling systems

Aoun, Joelle; Goverde, Rob M.P.; Nardone, Roberto; Quaglietta, Egidio; Vittorini, Valeria

DOI
10.1016/j.trc.2024.104573

Publication date
2024

Document Version
Final published version

Published in
Transportation Research Part C: Emerging Technologies

Transportation Research Part C 162 (2024) 104573

Contents lists available at ScienceDirect

Transportation Research Part C

journal homepage: www.elsevier.com/locate/trc

Analysis of safe and effective next-generation rail signalling systems

Joelle Aoun [a,*], Rob M.P. Goverde [a], Roberto Nardone [b], Egidio Quaglietta [a], Valeria Vittorini [c]

[a] Department of Transport and Planning, Delft University of Technology, Stevinweg 1, 2628 CN Delft, the Netherlands
[b] Department of Engineering, University of Naples "Parthenope", Centro Direzionale isola C4, 80143 Naples, Italy
[c] Dep. of Electrical Engineering and Information Technology, Univ. of Naples Federico II, Via Claudio 21, 80125 Naples, Italy

ARTICLE INFO

Keywords:
Moving Block
Virtual Coupling
Safety
Performance
Stochastic activity networks

ABSTRACT

Moving Block (MB) and Virtual Coupling (VC) rail signalling will change current train operation paradigm by migrating vital equipment from trackside to onboard to reduce train separation and maintenance costs. Their actual deployment is however constrained by the industry's need to identify configurations of MB and VC signalling equipment which can effectively guarantee safe train movements even under degraded operational conditions involving component faults. In this paper, we analyse the effectivity of MB and VC in safely supervising train separation under nominal and degraded conditions by using an innovative approach which combines Fault Tree Analysis (FTA) and Stochastic Activity Networks (SAN). An FTA model of unsafe train movement is defined for both MB and VC capturing functional interactions and cause-effect relations among the different signalling components. The FTA is used as a basis to apportion signalling component failure rates needed to feed the SAN model. Effective MB and VC train supervision is analysed by means of SAN-based simulations in the specific scenario of an error in the Train Position Report (TPR) for five rail market segments featuring different traffic characteristics, namely high-speed, mainline, regional, urban and freight. Results show that the thresholds of the design variables depend on the considered signalling system alternative and the investigated market segment. In particular, the TPR delay threshold allowed for MB is higher than for VC. This means that to ensure a safe train movement, VC cannot absorb a TPR delay of longer than 1.5 s, which corresponds to the mainline market segment. For MB instead, the results show that the maximum TPR delay can reach 3.9 s for high-speed and freight railways. In addition, results showed that the integration of an FTA in a SAN model can provide a better understanding of the safety-performance behaviour of a system where VC showed a higher number of braking indications with respect to MB for the same TPR error failure rate. This means that for VC to effectively supervise the train separation at the same safety level as MB, we would need to have a much higher reliability of the TPR. The overall approach can support infrastructure managers, railway undertakings, and rail signalling suppliers in investigating the effectiveness of MB and VC to safely supervise train movements in scenarios involving different types of degraded conditions

* Corresponding author.
E-mail addresses: J.Aoun@tudelft.nl (J. Aoun), R.M.P.Goverde@tudelft.nl (R.M.P. Goverde), Roberto.Nardone@uniparthenope.it (R. Nardone), E.Quaglietta@tudelft.nl (E. Quaglietta), Valeria.Vittorini@unina.it (V. Vittorini).

https://doi.org/10.1016/j.trc.2024.104573
Received 7 July 2023; Received in revised form 7 February 2024; Accepted 15 March 2024
Available online 26 March 2024

and failure events. The proposed method can hence support the railway industry in identifying effective and safe design configurations of next-generation rail signalling systems.

1. Introduction

Next-generation train-centric signalling systems like Moving Block (MB) and Virtual Coupling (VC) are currently being considered by the railway industry to meet strategic goals of increased network capacity and service efficiency. While MB reduces train separation to an absolute braking distance, VC would enable trains to move at a relative braking distance and potentially in synchronous fashion when forming radio-linked platoons. Both the concepts of MB and VC aim to migrate vital trackside equipment (e.g., track circuits, signals) to the onboard and remove the conventional track apportioning from open lines while still using interlocking at junctions/stations. A radio-based communication layer enables a trackside Radio Block Centre (RBC) to receive position reports from the trains and to send them Movement Authorities (MAs), i.e., the maximum distance that a train can safely cross. MAs are used by the onboard European Vital Computer (EVC) to dynamically supervise train separation while the Train Integrity Monitoring (TIM) checks that trains are integer, and no car is accidentally detached and stranded on the tracks. On top of such a complex system architecture, VC also features a Vehicle-to-Vehicle communication (V2V) -also known as train-to-train communication- layer by which trains inform each other on their current position, speed and acceleration to allow a separation shorter than an absolute braking distance or move synchronously in a platoon.

The railway industry is focusing on comprehensively assessing the implementation of MB and VC technologies, particularly emphasizing their impact on effectiveness and safety as the foremost important factor in authorizing operations. Safety-critical factors and constraints emphasize the need to understand and manage risks associated with cutting-edge technologies. Shubinsky et al. (2023) mention safety–critical control/command systems and their required Safety Integrity Level (SIL). The factors that necessitate the highest safety levels relate to the supervision of maximum permitted speed, train integrity supervision, driverless train control, trackside systems, and transmission and implementation of vital commands. In Aoun et al. (2023), the critical components for the deployment of VC include the interlocking and control technology, communication structures, and the cooperative train protection and operation of convoys. Quaglietta et al. (2022) consider five safety–critical factors for VC that need to be included in the computation of a dynamic safety margin. These factors include the train positioning errors, the communication update delays, the train control delays, the emergency braking application of the leader train, and exogenous factors such as peculiar weather or track conditions. ASTRail (2019) developed an analysis for MB system hazards by looking at the causes and effects. The critical factors of the top hazards that lead to collisions and/or derailments include communication failures, lost messages, errors in position integrity monitoring or the RBC, and a wrong TPR. Flammini et al. (2019) consider the communication as a critical factor by stating that VC over MB "will make communication issues even more critical". Other mentioned safety–critical factors include the evaluation of the performance of novel large bandwidth communication technologies against bit errors, faults and latency by means of appropriate stochastic models to assess the safety of VC against hazardous scenarios and critical failures.

Previous studies have evaluated the safety of MB with qualitative analyses in European projects such as ASTRail (2019) and X2Rail-1 (2019), by proposing hazard mitigation measures and updates to signalling requirements and engineering rules. Zafar et al. (2012) conducted a quantitative formal analysis of MB safety properties to prevent collisions/derailment in interlocking areas. Aoun et al. (2021) reported a preliminary qualitative safety assessment for both MB and VC based on expert interviews. However, several gaps remain in quantitatively analysing the effectiveness of MB and VC in ensuring safe train separation under various operational conditions, considering the influence of component failures and their cascading effects on the overall signalling system capabilities. To bridge these gaps, this paper proposes a novel approach that integrates Fault Tree Analysis (FTA) and Stochastic Activity Networks (SAN) to evaluate the effectiveness of MB and VC in supervising train movements, accounting for the complexity of interactions among signalling components, and the variable faults across these components. The proposed approach is crucial given the need to ensure safe and effective operations on existing railway networks, an aspect often overlooked in existing literature. Additionally, the study aims to determine the thresholds of design variables, to ensure effective and safe train movement, alongside evaluating VC's maximum failure rate through sensitivity analysis. The methodology is particularly applied on the example of a TPR network delay, while conducting a sensitivity analysis on the TPR error to evaluate VC's maximum failure rate for comparable technological maturity with MB.

Aoun et al. (2021) showed that among eight criteria assessed through a hybrid Delphi-Analytic Hierarchy Process (Delphi-AHP) approach, the safety criterion was evaluated as the most relevant with a weight of 45 %. Results also revealed that VC can outperform MB if both signalling alternatives reach the same level of technological maturity, i.e., safety. In addition, findings in MOVINGRAIL (2020) and Aoun et al. (2023) showed that the Reliability Availability Maintainability and Safety (RAMS) analysis and a Risk Assessment according to the Common Safety Method (CSM-RA) are attributed to a high priority and are critical step-changes towards the deployment of VC.

After an extensive literature review on various safety and performance methods, we found that combining FTA and SAN is an effective approach in dealing with system's complexities and behaviour to better understand the impact of faults on safety and performance. The methodology is further explained in Section 3.

An FTA is defined for modelling components' interactions and cause-effect relationships which could lead to unsafe train movements in both MB and VC. The FTA is then used to apportion a Safety Integrity Level (SIL) 4 failure rate across the different MB and VC signalling components. The resulting component failure rates are then used as input to a SAN-based simulation for assessing safe train supervision effectiveness of MB and VC in an example of a Train Position Reporting (TPR) error. Supervision effectiveness of a train-

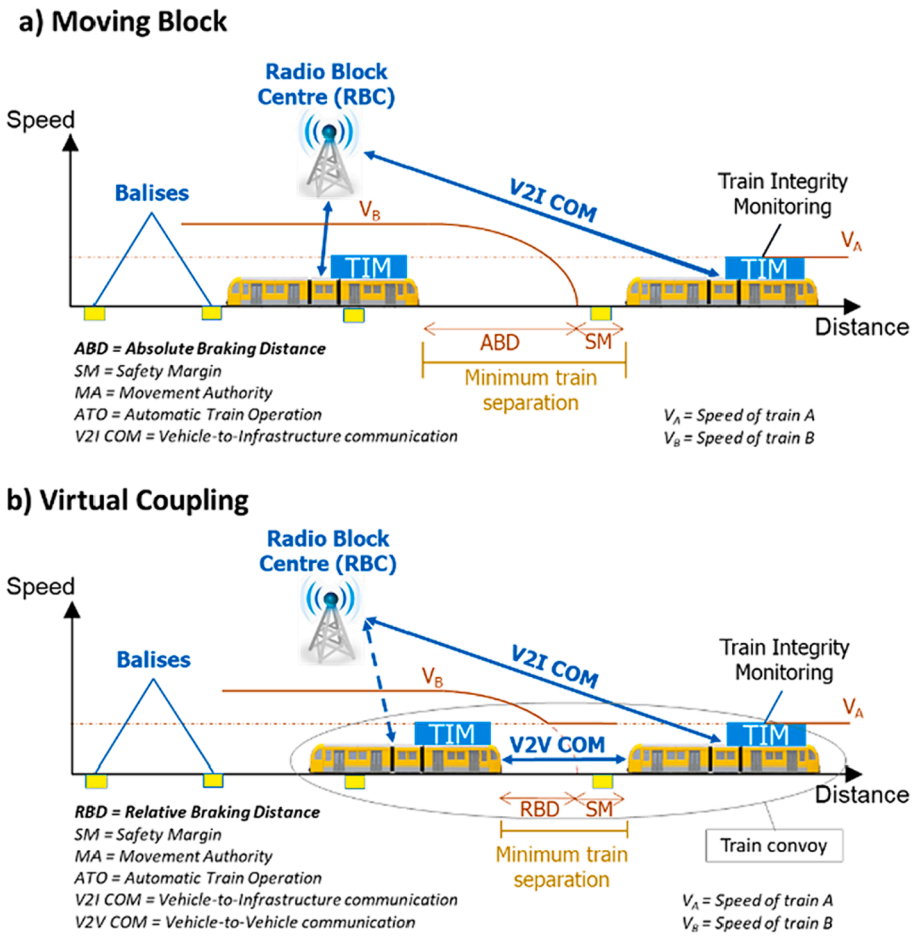

Fig. 1. Schematic architecture of train-centric signalling systems: (a) Moving Block and (b) Virtual Coupling.

centric signalling system is here intended as the capability of supervising the required safe train separation by smooth application of service braking, without triggering warning or emergency braking interventions, which might raise safety risks beside discomfort for both passengers and staff onboard of the trains. According to this definition, an effective train movement supervision would allow trains to maintain safe separations just by relying on the permitted braking curve, even in case of degraded or emergency situations. Although in real-life operations it is not always possible to avoid warning or emergency braking interventions, the provided definition aims at setting the theoretical basis to assess ideal conditions of an effective train movement supervision under MB and VC. For this latter signalling system in particular, we analyse the impact on signalling supervision effectiveness of the dynamic safety margin, introduced in Quaglietta et al. (2022), which considers an additional distance to allow trains in a VCTS to safely stop by smoothly using the service brakes even in case of sudden emergency braking application of the train in front. The assessment of signalling supervision effectiveness is hence measured in terms of the number of unplanned service braking applications of a train to avoid triggering a warning or emergency braking intervention. The used KPI is a safety-related measure indicating the capability of the signalling system to safely supervise the train within the given movement authority while avoiding overshooting of the warning braking curve and/or the triggering of emergency braking interventions. A large number of braking indications provided by a signalling system under nominal undisturbed traffic conditions, might signify potential system's issues such as challenges in hazard detection, latencies in communication of vital information or reduced reliability of signalling components which can directly affect operation safety. Especially for train-centric systems like MB and VC where supervised train separations are shorter, the escalation of braking indications might be challenging to manage given the reaction times of train drivers and/or the ATO, and lead to critical overshooting of the warning braking curves or even to emergency braking applications. The main contributions in this work are:

(i) Identifying the effects of signalling component failures on the effectivity of MB and VC in safely supervising train operations for five railway market segments.
(ii) Proposing a novel approach which combines FTA and SAN for a quantitative analysis of signalling system configurations.
(iii) Defining a key performance indicator (KPI) for the evaluation of effective signalling supervision of safe train movements.

(iv) Determining practical implications for MB and VC component configurations which could support the railway industry in investment and design decisions.

The paper is structured as follows. Section 2 highlights the MB and VC concepts and the main safety and operational challenges for implementing VC. It also provides a literature review on the SAN modelling formalism. Section 3 describes the FTA-SAN methodology adopted in this paper. A description of the FTA and SAN models for MB and VC is provided in Section 4. Finally, Section 5 outlines the results followed by conclusions in Section 6.

2. Literature review and background

To achieve the contributions defined in Section 1, there is a need first to understand next-generation railway signalling systems and the purpose of combining FTA and SAN models. This section provides the reader with a better understanding of the systems and concepts that are used in this paper as well as the proposed approach for developing a novel framework that aims at evaluating the safe and effective behaviour of advanced transportation technologies, with particular focus on the railways field. It must be noted that the number of times the train brakes according to the permitted braking curve which uses a service braking rate –hereafter referred as braking applications– is used in this paper as an indicator for safety. Therefore, we do not focus on accidents that relate to collisions or derailments but rather on the failures of the railway signalling system functionalities that lead to the undesired event of an unsafe train movement.

2.1. Next-generation railway signalling systems

In the past decades, research has focused on investigating different aspects of next-generation train-centric signalling systems like MB and VC in terms of capacity evaluation and hazards identification. Fig. 1 gives a schematic view of the MB and VC concepts. Both MB and VC provide a chance to increase capacity at reduced costs due to less trackside equipment since the train separation in both systems is no longer based on fixed blocks where the rule is that a block section cannot be occupied by more than one train at a time. In addition, lineside signals are removed, and trackside track-vacancy detection equipment is migrated to onboard TIM (Aoun et al., 2021). The TIM verifies that a train is complete while it is in operation. It also guarantees a safe train-rear position for dynamic braking curve supervision. In MB (Theeg and Vlasenko, 2009), such as proposed in the European Rail Traffic Management System/European Train Control System Level 3 (ERTMS/ETCS L3), the train separation depends on Train Position Reports (TPRs) which are regularly sent from train to trackside, i.e., the RBC. It must be noted that according to the latest TSI on CCS, ETCS Level 3 has lost its state as an independent ETCS standard and is now considered a variant within ETCS Level 2, where train detection and integrity checks could be performed by the trackside equipment beyond the scope of ERTMS or managed within the scope of the ERTMS system (European Commission, 2023; EUAR, 2023). The RBC sends movement authorities (MAs) to the trains to indicate the maximum distance that a train can safely run represented by the End of Authority (EoA). In MB, the train separation is reduced to an absolute braking distance which is needed by a train to brake to standstill. VC can reduce further the separation between the trains to a relative braking distance by taking into account the braking characteristics of the train ahead. VC can therefore allow trains to move efficiently in platoons by forming a virtually coupled train set (VCTS) or convoy where trains communicate with each other by means of V2V and cooperative train control to ensure a safety margin. The highest capacity benefits for VC are in the case of trains running in a virtually coupled state where a safety margin would be sufficient between the trains in the VCTS. The Global System for Mobile Communication Railways (GSM-R) is used for the bi-directional exchange of messages between an onboard EVC and the RBC represented by the vehicle-to-infrastructure communication (V2I) in Fig. 1. GSM-R V2I applies to both MB and VC while the additional functionality of the V2V is specific for the VC technology and requires (5G) low-latency high-availability communication. It must be noted that even for the V2I communication (which currently relies on GSM-R), more advanced communication systems are planned to be implemented in the future such as the Future Railway Mobile Communication System (FRMCS) 5G-systems (RailEngineer, 2023; UIC, 2023; RailTech, 2022). Therefore, the study in this paper is not restricted to GSM-R and can be generalized to newer communication systems. As the sight reaction time of a human driver would not be safe in the setup of a very short train separation among trains, Automatic Train Operation (ATO) becomes essential for VC.

Biagi et al. (2017) evaluate emergency stops in ETCS L3 due to communication failures using stochastic parameters, with some changes that reflect the amendments introduced in the evolution of the ERTMS/ETCS specification. Flammini et al. (2019) proposed a quantitative model to analyse the effects of introducing VC according to the extension of the current ETCS L3 standard, by maintaining the backward compatibility with the information exchanged between trains and the trackside infrastructure. Di Meo et al. (2019) studied operational principles and communication configurations of VC in several stochastic scenarios related to the transitions between different VC operating modes by using a numerical stability analysis of the closed-loop system to study platooning in the automotive field. Quaglietta et al. (2020) developed a train-following model to describe train operations under VC and assess capacity performance under different operational settings. In Aoun et al. (2020), several challenges for the implementation of VC have been discussed particularly related to safety, technology, operation, infrastructure and business. Aoun et al. (2021) found that the safety criterion weighs almost the same as seven other criteria together, namely infrastructure capacity, system stability, lifecycle costs, energy consumption, travel demand, public acceptance and regulatory approval. In addition, Aoun et al. (2023) found that the most critical step-changes towards the deployment of VC are the longitudinal motion control systems within convoys and the integrated traffic management and cooperative train operation. This is because there is a need to guarantee a safe distance between trains before being able to develop the concept of operations, as well as the train positioning and the switch technology. To guarantee a safe relative

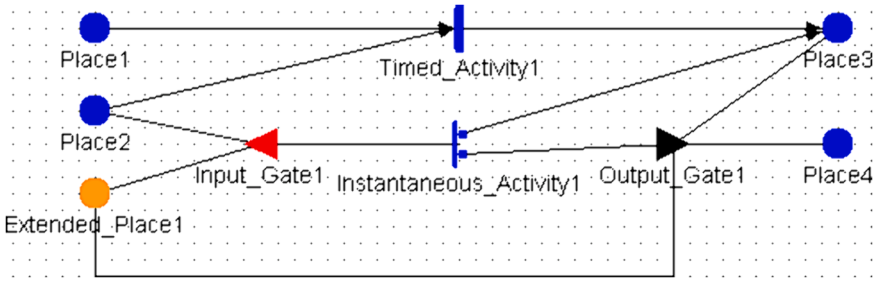

Fig. 2. Simple example of a SAN model.

distance, several issues need to be solved. They can relate to the frequency of the V2V layer. For instance, if dynamic information about braking control of the leader in a convoy is not timely sent and received by the trains behind, then train collisions might occur. Another constraint can potentially arise from the heterogeneity of braking characteristics of different trains moving in a convoy which could also raise collision risks if for instance the train ahead within a convoy has a higher braking rate. In addition, an accurate dynamic safety margin (Quaglietta et al., 2022) needs to be considered between the trains based on the speed, a friction factor, the RBC and V2V latencies, the control delay or ATO reaction time, and the location inaccuracy.

The train separation principle and safety requirements in railway systems are vital for ensuring efficient and secure train operations. Previous research has extensively focused on various aspects of train separation principles and safety, aiming to enhance the overall safety and efficiency of railway networks. European projects such as X2Rail-3 (2018) and MOVINGRAIL (2018) have been investigating safe operational principles, scenarios and reliable communication architectures for the feasibility of VC. Fenner (2016) presented steps and scenarios for closer running, i.e., VC, with the aim of safely operating trains closer together at their permitted speeds to deliver increased flexibility and capacity to meet predicted demands. Felez et al. (2019) developed a preliminary Model Predictive Control approach for virtually coupled trains using a predecessor-following information structure that minimizes a function of desired safe relative distance, the speed of the predecessor train and the jerk. In railways, the V2V communication is particularly beneficial when trains move synchronously together in a platoon, and consequently a safety margin would be sufficient between the trains in a VCTS (Quaglietta et al., 2022). Additionally, an accurate dynamic safety margin needs to be considered between the trains based on the speed, a friction factor, the RBC and V2V latencies, the control delay or ATO reaction time, and the location inaccuracy. Based on Aoun et al. (2020, 2021, 2022, 2023), safety requirements relate to the longitudinal motional control systems within convoys. Other safety requirements relate to diverging junctions at which the trains in a VCTS should be decoupled and have sufficient distance to move and lock the point, abstaining derailment risks. Furthermore, the route locking and (sectional) release principle should guarantee that switches stay locked during the passage of all virtually coupled trains in a VCTS. The frequency of the V2V communication layer is also crucial because if dynamic information about deceleration controls of the leader in a convoy is not timely broadcast and received by the train(s) behind, then potential train collisions might occur. Additionally, the train separation between trains in a VC convoy is based on relative braking distances plus a dynamic safety margin (as introduced in Quaglietta et al., 2022), which aims at preventing train collisions in case of risk factors such as latencies in train control and communication or sudden emergency braking applications of the train in front. Finally, a thorough investigation of the safety margin shall be made, taking into account optimal design configurations that encompass speed profiles, friction, V2V communication latency, and positioning/location inaccuracy.

2.2. *The SAN modelling formalism*

Stochastic Activity Networks (SANs) are a stochastic extension of Petri Nets (PNs). They provide a high-level modelling formalism and enable the specification of performance, dependability and performability models (Meyer et al., 1985; Sanders and Meyer, 2001). Therefore, SANs have been widely used for dependability and performability evaluation of complex systems (Sanders and Malhis, 1992; Bertolino et al., 2011; Fantechi et al., 2022). A modular approach to modelling of complex systems is possible by leveraging hierarchical specification of models.

In the following, the main notations and concepts used in the paper are introduced. SANs consist of four primitives: places/extended places, activities (with or without cases), input gates and output gates, as illustrated in Fig. 2. *Places* represent the state of the modelled system, they can contain a number of *tokens*. The number of tokens in a place represents the *marking* of that place. The distribution of tokens over places in the model is the *marking of the network* and represents the state of the model. *Extended places* differ from 'ordinary' places for the type of tokens they may contain: the tokens in a place do not provide any kind of information, instead in the extended places they can represent atomic variables or data structures. Extended places cannot be connected directly to an activity, but only to its input and output gates; their names are referred by the definition of the associated input gate predicates and output gate functions. Therefore, the arcs between extended places and the input/output gates can be omitted to keep simple the graphical representation of a complex model.

Activities represent actions in the modelled system, they are of two types: *timed* and *instantaneous*. Timed activities represent time-consuming actions, instantaneous activities represent logic conditions or actions that complete in a negligible amount of time. Places and activities are connected through arcs so that an activity may have a set of input places and a set of output places. *Cases* are used to

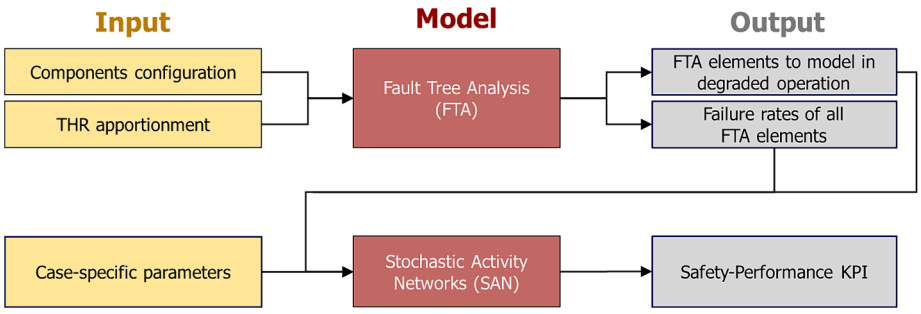

Fig. 3. FTA-SAN methodology framework.

model uncertainty associated to the completion of an activity: each case represents a possible different outcome. Each activity has a probability distribution (*the case distribution*) associated with its cases. The case distribution may be dependent on the marking of the model at the activity completion, if no cases are present a default with a probability equal to one is assumed. Graphically, cases are represented as circles on the right side of an activity (see Fig. 2). Each timed activity has an *activity time distribution function* associated with its duration, which can be associated to general distributed random variables (e.g., exponential, normal, binomial) and can be marking dependent.

The dynamics of the model is provided by the firing of the activities according to the *enabling and completion rules.* The firing of an activity models the execution of the activity and causes a state change in the SAN producing a new marking (hence it represents a state change in the modelled system): tokens are removed from the input places of the transition and generated in the output places according to the completion rule.

Input and output gates are introduced to allow greater flexibility in defining enabling and completion rules. Only enabled activities may fire, input gates control the enabling of the activities and define the marking changes when the activities complete. An *input gate*, if present, is placed between the activity and its input places and connected by arcs where *an enabling predicate* and an *input gate function* are defined. *An activity is enabled* when the predicates of all input gates connected to the activity are evaluated to true, and each 'ordinary' place connected to the incoming arcs contains at least one token. The input gate function specifies how the marking of the input places changes upon the completion of the activity. In case an activity is directly connected to an input place, the activity is enabled if there is at least one token in that input place and the marking of the place is decremented when the transition fires. An *output gate*, if present, is placed between the activity and its output places and connected by arcs to the cases of the activity and to the output places. An *output gate function* is defined which specifies how the marking of the output places changes upon the completion of the activity. In case an activity is directly connected to an output place, the firing of the activity increments the marking of the place.

In Fig. 2, the timed activity *Timed_Activity1* is enabled by tokens in places *Place1* and *Place2*. When the activity fires, a new token is added in *Place3*. At the bottom of the figure, the instantaneous activity *Instantaneous_Activity1* is enabled by the predicate of *Input_Gate1*, which, in turn, is evaluated with respect to the marking of *Place2* and *Extended_Place1*. When the activity fires, two cases are possible. If selected, the first case adds a token to *Place3*; alternatively, the second case enables the execution of the output gate *Output_Gate1*, which, in turn, updates the marking of *Place4* and *Extended_Place1* according to the output function associated with the activity. It must be noted that the arcs between *Extended_Place1* and the gates *Input_Gate1 Output_Gate1* could be omitted for sake of clarity.

With the aim of dealing with complex system models, a hierarchical specification of SAN is possible through the *replicate and join* operations. The Replicate/Join formalism allows to build composed models from sub-models called *SAN atomic models*. The atomic models are composed through place superposition. The replicate operation generates more instances of an atomic model, and the join operation composes different types of atomic models. In both cases, the sub-models communicate by sharing the global variables represented by the common (superposed) places.

SAN models are developed and solved by using the multi-formalism multi-solvers tool Möbius (Sanders, 1999; Clark et al., 2001). Da Silva et al. (2021) mention that Möbius is the only available mature tool that can edit and solve SAN models, and integrates both analytical solvers and a discrete event simulator.

In Möbius some of the primitives of the SAN models are based on the C++ programming language, specifically the types used to define the extended places, and the functions and distributions associated to the activities and to the input and output gates are written in C++.

To accurately evaluate the effects of VC in terms of network safety, realistic conditions need to be considered such as the minimum headway times and the type of rolling stock. Recent studies (Flammini et al., 2021) indicated that the SAN can be used to effectively evaluate the safety of VC. The authors used SAN to represent all performance and dependability aspects of interest for the analysis of railway VC in real-world scenarios. Based on their results, they proposed to extend their research to reliability, safety and security modelling due to the modularity of the adopted SAN approach.

3. Methodology

In this section, we introduce a novel methodological framework (Fig. 3) on the integration of an FTA with a SAN approach (Section

Table 1
Model variables.

Model Name	Description	Min. Value
RBCprocessingTime	Computation by the RBC	0.2 s
EVCprocessingTime	Onboard translation of received MA into speed profile and speed indication computation by the EVC	1.5 s
TPRnetDelay	Communication time from the train to the RBC (TPR broadcasting time)	0.5 s
MAnetDelay	Communication time from the RBC to the train (MA broadcasting time)	0.5 s
V2VcommDelay	Communication delay in V2V communication	0.1 s
TPRupdatePeriod	Train position and integrity reporting time including GSM-R and GNSS	4 s
driverReactionTime	Includes the onboard translation of received MA into speed indication, i.e. visualization by the EVC, and the time for the driver to interpret and react to the indication	4 s
ATOreactionTime	Includes the onboard translation of received MA into speed profile performed by the ATO, and the speed indication computation by the EVC.	0.5 s

2.2). The FTA is a deductive, structured methodology to determine the potential causes of an undesired event (Khakzad et al., 2011; Limnios, 2007; NASA, 2002). Mahboob and Straub (2011) define the FTA method as a common technique used for logical representation of a technical system for the purpose of safety and reliability analysis. In this deductive method, an undesired event –called Top Event (TE)– is postulated and the scenarios leading to the TE are identified. They originate from basic events and are described by a series of logical operators and intermediate events leading to the TE.

In this paper, we provide an aggregated high-level FTA for modelling the causes of unsafe train movement. We then integrate the failure rates derived from the developed FTA in the cases of activities in the SAN models by conducting a sensitivity analysis on the failure rate to analyse the effect of perturbations on the train movement in degraded operations. These degraded operational conditions relate to potential faults in the design variables of MB and VC railway signalling. The perturbations refer to the number of violations of ETCS braking applications, while the goal is to maintain a safe separation (minimum headway) and to avoid an emergency stop in case of faults in the values of the design variables. A variable is defined as an element, feature or factor that is liable to vary or change. A design variable is a numerical input that is allowed to change during the design process or optimization. In this paper, we vary the values of the variables that allow the design of train-centric signalling systems (Table 1). These values were initially derived from experts' experiences, who participated in the European Shift2Rail PERFORMINGRAIL project (PERFORMINGRAIL, 2020).

To develop an FTA, the system components are first identified and evaluated based on their corresponding functionalities and interdependencies. Then, a cascading sequence of system component failures and cause-effect relationships are analysed to understand how a failure or fault in one component impacts the other components. We used a Tolerable Hazard Rate (THR) apportionment (see Section 4.1.2) to compute the failure rates of all the elements of the fault tree. Part of the detailed FTA developed for MB and VC can be found in Aoun et al. (2022).

Two simulation analyses are described in this paper and performed in Section 5. Within the SAN modelling tool, Möbius, a sensitivity analysis on different design variables that constitute the investigated system is performed while taking into account the minimum headway between trains. The purpose of both analyses is to find configurations that allow a safe train movement based on a specific safety-performance KPI. The first analysis about the TPR net delay has been performed for a given train headway by varying the value of the TPR according to a uniform distribution defined in a given range of values. This analysis aims at identifying the max TPR value as the threshold beyond which trains start activating service braking to stay within safe train separations. The idea is that trains moving at the minimum headway should operate without unnecessary service braking applications. The value of this threshold is thus dependent on the chosen KPI, which is the number of braking applications according to the permitted braking curve (which uses a service braking rate). Therefore, above this threshold, the train would need to brake. In addition, we do not look solely at the safety component but also at the performance aspect because if the train needs to frequently brake, the passengers might experience discomfort and the train driving strategies might be inefficient and energy-consuming. From a safety perspective, the use of this KPI is to ensure that the trains do not run into warning or emergency braking conditions which besides discomfort might raise safety risks for passengers onboard. In this paper, we particularly focus on the TPR delay design variable which is the communication time from the train to the RBC (TPR broadcasting time).

The main reason for using the TPR as an example is the highly relevance of this variable when designing signalling systems and its significant role in the developed FTA for both MB and VC (see Section 4.1 and Fig. 5). Therefore, we believe that the usage of other design variables would not affect the validity of the proposed methodology that aims at the evaluation of a defined KPI to ensure the effectivity and safety of systems. A detailed SAN analysis of MB to other design variables like the MA net delay and the RBC processing time can be found in PERFORMINGRAIL (2020).

In the second analysis, the same process is followed to address the sensitivity of service braking applications to different TPR error failure rates. The applied sensitivity analysis on the failure rates in the FTA was introduced in the cases of the activities in the SAN models, and the failure rates were drawn according to a uniform distribution from a given range of failure rate values. For each value of the range, a SAN-based simulation was performed to assess the resulting number of service braking applications. The focus of this paper is on analysing the failure rate of the TPR error for both MB and VC in a way that guarantees a similar level of maturity between both systems. In both analyses, the objective is to search for a threshold variation of the design configuration before leading to a violation of the permitted braking curve, so to evaluate an effective and safe deployment of MB and VC.

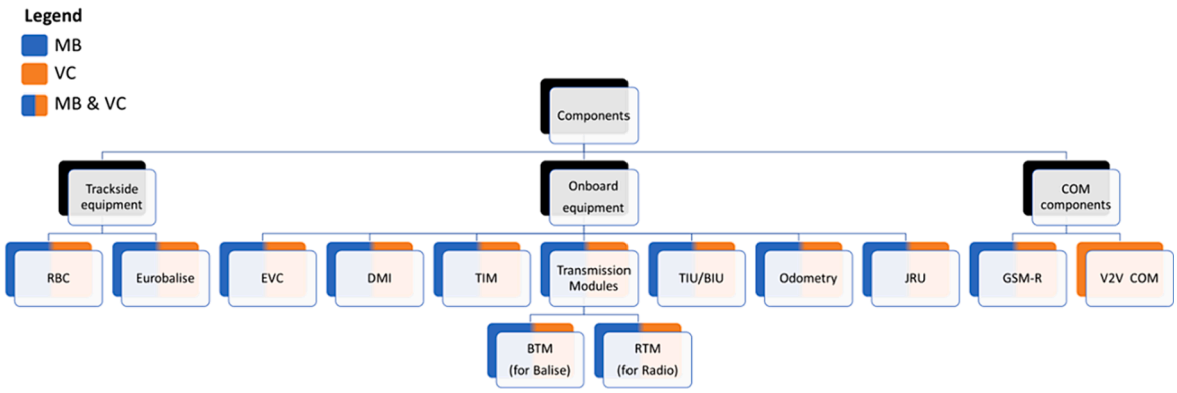

Fig. 4. Components' breakdown structure of Moving Block (MB) and Virtual Coupling (VC).

It is well known that the application of formal modelling methods and tools to complex systems can pose limitations primarily linked to three factors: *(i)* the expressive power of the employed formalism, which must be capable of modelling the specific characteristics of the studied system; *(ii)* the difficulty of analysing models, especially in the presence of state space explosion phenomena; and *(iii)* the availability of sufficiently mature model development and analysis tools for use in not only research but also industrial contexts. The approach proposed in the paper combines two formalisms to address all these factors. On one hand, fault trees have limited expressive power but are solely used for fault analysis. Large fault trees can be solved with established tools and techniques. On the other hand, the system's behaviour modelling is delegated to SANs, supported by a mature analysis tool and capable of modelling any complex behaviour. SANs do not require an analytical solution but are addressed through a simulation approach, making them highly flexible and efficient in presence of a very large state space. Therefore, the proposed innovative approach utilizes complementary formalisms, and their combination can help model and analyse practical scenarios and different types of railway systems.

The combination of FTA and SAN offers a comprehensive approach that leverages the strengths of both methodologies, providing a more holistic understanding of system safety and performance. By integrating FTA, which is adept at analysing system failures and identifying potential risks, with SAN, which excels in modelling complex dynamic systems with probabilistic elements, a more accurate assessment of system behaviour can be achieved. This combined approach enables the evaluation of not only potential failure scenarios but also the probabilistic impacts and interactions of various system components, by integrating the failure rates coming from the FTA to SAN. Therefore, the proposed method contributes to a more thorough analysis of system effectiveness and safety under diverse operational conditions, and the synergy between FTA and SAN leads to a novel framework that enhances the overall comprehensiveness of the assessment process.

4. Modelling for Moving Block and Virtual Coupling

4.1. FTA modelling of unsafe train movement for Moving Block and Virtual Coupling

4.1.1. System components and functions

The first step in developing an FTA is to define the scope of the study. This is achieved by defining the systems' components and identifying their related functions. Fig. 4 illustrates the breakdown structure of the components that constitute MB or ETCS L3 (blue colour) and VC (orange colour). The elements that have both the blue and orange colours are applicable to both MB and VC.

As ETCS L3 is built upon ETCS L2, previous analyses for building fault trees of ETCS L2 (UNISIG, 2019) have been used as an inspiration to build the fault tree for ETCS L3. This is because several MB components are also included in ERTMS/ETCS Level 2 systems. At this level of abstraction, the main differences between ETCS L2 and the MB systems are the following: 1) the onboard system includes a new component, TIM, 2) the trackside track-clear detection is no longer necessary as in fixed-block signalling; 3) trackside functions are new or modified. All the trackside and onboard equipment are common to both MB and VC. However, VC is characterised by the additional V2V component.

Intuitively, the fewer number of trackside components may increase the system reliability and decrease costs, as it is also envisioned by the European rail initiatives Shift2Rail and EU-Rail. On the other hand, the introduction of new components has to be considered. In the following, a brief description of the components introduced in Fig. 4 is given.

Both MB and VC systems have RBCs and Eurobalises as trackside equipment. The RBC is a computer-based system that elaborates the messages that need to be sent to the trains. A main goal of the RBC is the management of the MA. The MA provides the maximum distance that a train can safely cross without colliding with another train on the route. In VC, the MA associated to VC, MA_{VC}, combines information from both the RBC and the V2V communication channel, and the speed associated to the End of Authority for VC (EoA_{VC}) is either equal to the speed of the train ahead (if trains are running in a coupled stage), or zero (if trains are decoupled). The Eurobalise is a transmission device placed between the rail tracks. It is defined as a trackside transponder or electronic beacon acting as a fixed geographical reference point. The main functions of the Eurobalise are to report the train position and to provide the up-link for sending messages to the train onboard system.

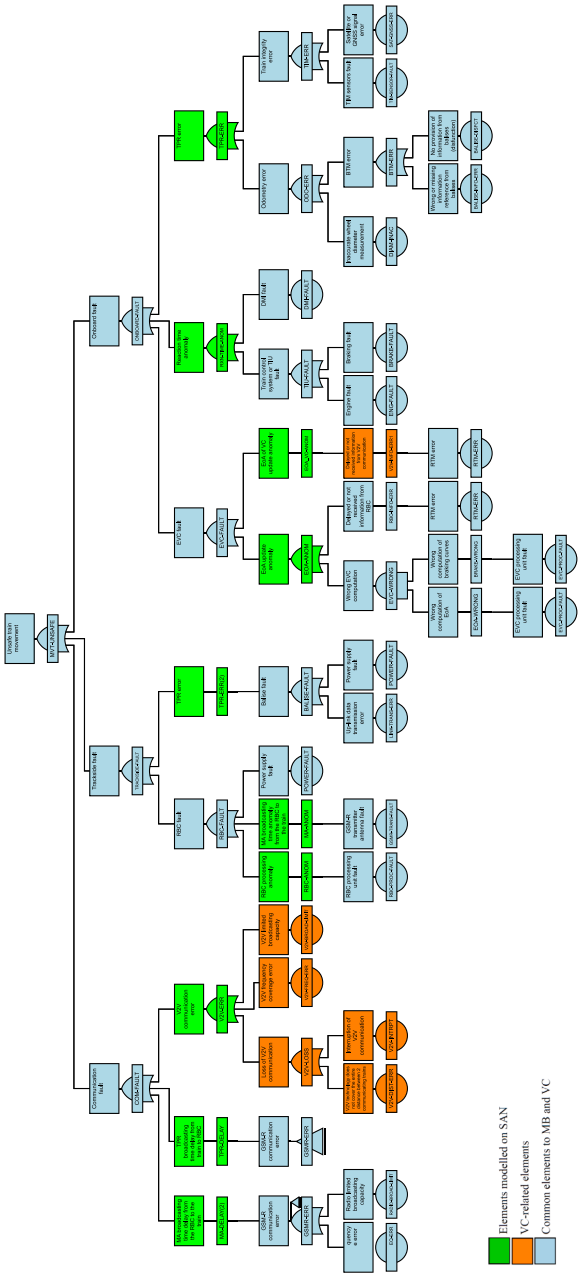

Fig. 5. FTA for modelling an unsafe train movement for Moving Block and Virtual Coupling.

The ERTMS/ETCS onboard system is a computer-based system that supervises the movement of a train, on basis of the information exchanged with the trackside system. It is composed of the European Vital Computer (EVC) where kernel functions are stored, the Driver Machine Interface (DMI), the Balise Transmission Module (BTM), the Train Integrity Monitoring (TIM), the Radio Transmission Module (RTM), the Train/Brake Integrity Unit (TIU/BIU), odometry and the Juridical Recording Unit (JRU). The EVC monitors continuously the train location by means of an onboard odometer that is regularly calibrated any time the train crosses a balise. It also elaborates MA messages and supervises in real-time a dynamic speed profile including braking curves that ensures that the train does not overrun the EoA. However, in the case of VC, further functions of the EVC are implemented by considering the supervision of both the EoA_{vc} and the standard EoA (in the operational state of an (un)intentional decoupling). In addition, the EVC for VC predicts the distance traversed by the leader during a certain coordination time that is required by the follower to catch up with the leader's speed at the location indicated by the EoA_{vc} within a certain safety margin from the latter's rear. The DMI provides a bi-directional interface with the train driver and displays relevant information and instructions to the driver. The TIM verifies that a train is complete while it is in operation. It also guarantees a safe train-rear position.

The BTM detects the presence of a balise and processes the up-link and down-link data. The BTM is interfaced with the ERTMS/ETCS kernel and onboard antenna unit (i.e., Global System for Mobile communications-Railway (GSM-R)). The RTM provides a bi-directional interface with the trackside. The TIU and BIU are used as interfaces with the EVC to the train and/or the locomotive for submitting commands or receiving information. The BIU is used for implementing braking instructions. The odometry represents the entire process of measuring the train's movement (speed and distance) during a journey along the track. The JRU is used as a device to record defined data relating to the train's movements for legal purposes. The recorded data shall allow analysing the cause of an accident, incident, or hazardous situation.

The communication components include the GSM-R onboard which applies to both MB and VC and the additional functionality of the V2V communication that is specific for the VC technology. The GSM-R onboard radio system (antenna) is used for the bi-directional exchange of messages between the onboard EVC and RBC. The V2V communication onboard allows the trains to be separated by a relative braking distance. Via onboard antennas, the trains are able to exchange route and kinematic information (e.g., speed, acceleration) and to form a convoy of virtually coupled trains, also known as virtually coupled train set (VCTS).

4.1.2. Fault trees development

One of the main advantages of an FTA is that it provides a logical framework for understanding and assessing the scenarios leading to system failures. We apply the principles of the FTA in this section by looking at a high-level perspective of the cause-effect relations leading to an unsafe train movement of both MB and VC. The MB specifications have been defined by the Shift-to-Rail (S2R) X2Rail-1 (2019) and X2Rail-3 (2020) projects and they are publicly reported in the project deliverables. VC is still a visionary concept. The application conditions of VC have been investigated in S2R X2Rail-3 (2020) and further research is planned within Europe's Rail (2022), the successor of the S2R joint undertaking.

The generated combined fault tree for MB and VC is illustrated in Fig. 5. The model has been developed on the Isograph Reliability Workbench 15.0 (Isograph, 2020). The circles are basic events where no further breakdown is possible. The basic events in the fault tree can be both independent or a common cause failure. Specifically, when the same name is shown for different basic events, it means that they represent a common cause failure, which can cause multiple components to fail simultaneously. This effect can be specified in the solver tool, i.e., Isograph Reliability Workbench 15.0. All the used gates are OR gates except for EVC-WRONG which represents an AND gate. In this particular case, a wrong computation of the EVC arises from both a wrong computation of the EoA and a wrong computation of the braking curves. The transfer gate (triangular shape) represented by the GSM-R communication error (GSMR-ERR) in Fig. 5 is an extension to another location or sub-tree within the main tree. In this case, the developed elements under the referred transfer gate are RADIO-FREQ-ERR OR RADIO-BROAD-LIMIT. The elements in blue are common to both signalling systems. The orange elements are specific for the VC technology as they deal with the extra V2V component that characterizes the platooning concept. The items represented in green are modelled in SAN (Section 4.2.1). These elements relate to signalling system components and mainly belong to the third and fourth levels of the FTA starting from the Top Event as first level. We refer to these elements as those show the effects of all causes beneath them. The only element which we did not incorporate in the SAN is the 'Power supply fault' as this one does not relate to any signalling component fault that leads to an unsafe train movement but can be a potential reason to an RBC fault.

We first started by developing a fault tree for MB, then we extended it to VC by considering the potential failures that might arise from the additional V2V communication component (represented by solely the orange colour). The potential main causes for an unsafe train movement could arise from a communication fault, a trackside fault or an onboard fault. The driver error was not considered since we consider that the automatic train protection (ATP) would always interfere whatever the reason of driver error is. The potential causes that lead to a communication fault relate to a broadcasting time delay of the MA from the RBC to the train, or a broadcasting time delay of the TPR from the train to the RBC, or a V2V error which is only specific to the VC system. The reasons that lead to the latest can be a loss of the V2V, or a V2V frequency coverage error, or a V2V limited broadcasting capacity. The loss of V2V can be a consequence of a lack of coverage of the V2V technology to the entire distance between two communicating trains or an interruption of the V2V. In the case of trackside fault, the causes can be associated to an RBC fault or a TPR error. It must be noted that a TPR error can result from two different categories of failures: *(1)* a failure of the onboard system that is caused by an odometry error resulting from an inaccurate wheel diameter or a BTM error, or a train integrity error which is a consequence of a fault in the TIM sensors or an error in a satellite or a GNSS signal, *(2)* a consequence to a trackside failure due to a fault occurring on the balises, given an error in the up-link data transmission or a fault in the power supply. In addition to a TPR error, other causes could also lead to an onboard fault, namely a fault in the EVC or an anomaly in the reaction time. It must be noted that the term anomaly in the FTA is used to include either message integrity errors, wrong variable values (e.g., erroneous computation of the EoA or corresponding braking curves), as well as delayed reception/broadcasting of necessary messages/information or unexpectedly extended processing times of onboard and trackside signalling components. Given that the analysis of all possible anomalies would lead to a very complex experimental setup, we focus in this paper on a selected set of anomalies whereby preliminary observations showed to be particularly interesting to investigate with respect to safe train movement supervision. Anomalies referring to delays or extended processing times might be more relevant than wrong/erroneous value computation as redundancy of equipment will lead to a direct activation of emergency brakes if at least 2 out of 3 (2oo3) components do not find the same values (this is for instance the case of EVC redundant processors). If the anomaly would instead be a delayed computation or a delayed delivery of necessary information which is still below the threshold for fail-safe brake application, then those delays might induce violations of indicated ETCS speeds corresponding to a given ETCS braking curve. That might hence lead to non-smooth train movements with sudden deceleration or even potentially unsafe movements under certain conditions.

The failure rates of the main events related to the faults of onboard, trackside and transmission (i.e., communication) functions

Table 2
Market-specific model parameters.

Parameters		Market segment High-speed	Mainline	Regional	Urban	Freight
Train length (m)		327.6	115	96	130	670
Maximum speed (m/s)		83	44	33	22	28
Maximum acceleration (m/s^2)		0.54	0.53	0.6	0.8	0.2
Braking rates (m/s^2)	**Indication**	1	0.7	0.6	0.5	0.4
	Permitted	1	0.7	0.6	0.5	0.4
	Warning	1.25	0.875	0.75	0.625	0.5
	Emergency	1.5	1.05	0.9	0.75	0.6

were preliminary derived from a Tolerable Hazard Rate (THR) apportionment approach by UNISIG (2019). Particularly, the following apportionment was used:

- 10^{-9} / hour for ETCS onboard (installed on a train), and
- 10^{-9} / hour for ETCS trackside (installed in an area visited by a train during a reference mission).

Considering that the transmission functions are offered by the joint work of onboard and trackside equipment, UNISIG empirically apportions 1/3 of each hazard rate to the transmission functions. Hence, the THR for ETCS onboard is apportioned as 0.67×10^{-9} / hour to the onboard functions and 0.33×10^{-9} / hour to (onboard) transmission functions. Similarly, the THR for trackside functions is apportioned as 0.67×10^{-9}/ hour to the trackside functions and 0.33×10^{-9} / hour to (trackside) transmission functions. With the increasing complexity of the onboard transmission equipment, which has to support the V2V and additional functionalities, the onboard transmission functions should rely on increased quality equipment to fulfil this rate. Following a reverse engineering approach and by using the FTA principles and analysing the steady-state failure frequency, the failure rates of all the elements of the fault tree in Fig. 5 were computed. The values of the elements highlighted in green in the FTA were evaluated in the cases of the activities modelled with SAN for MB and VC by developing a sensitivity analysis on the failure rates.

4.2. SAN modelling for next-generation railway systems

4.2.1. SAN modelling principles for Moving Block and Virtual Coupling

The SAN models introduced in this paper aim at analysing the system behaviour of MB and VC with the objective to estimate the frequency of braking applications (i.e., indication, permitted, warning and emergency) according to several design configurations. The SAN models take into account:

a) Some potential probabilities of failure that affect the performance of the systems;
b) Different railway market segments, specifically high-speed, mainline, regional, urban and freight railways.

The modelling approach composes reusable atomic SAN sub-models modelling the train onboard unit and railway signalling components. The VC model is obtained by extending the MB model with the V2V communication and properly modifying the model variables.

A global MB or VC model is obtained by considering a convoy of trains moving along the track. The introduction of sub-models facilitates their reuse, development and maintenance. For instance, they can be applied to different topologies with different sequences of routes and junction areas.

A braking curve is a prediction used by the ETCS onboard unit to compute in real time the braking distance. The onboard unit predicts the decrease of the train speed against a distance that must not be exceeded according to a mathematical model (ERA, 2020).

In ETCS L3 MB, the driver or the ATO must keep the speed below the permitted speed. The ETCS onboard unit continuously supervises the permitted speed and indicates when braking is required, followed by a braking intervention if the driver or the ATO does not follow up, to avoid that the train exceeds the supervised dynamic speed profile or overruns the allowed limit represented by the EoA.

The SAN model has been set up by including four different braking curves described in ERA (2020) as follows:

- Indication (I): “the I supervision limit leaves the driver enough time to act on the service brake so that the train does not overpass the permitted speed”.
- Permitted (P): “The P supervision limit in case of overspeed leaves the driver an additional time to act on the service brake so that the train will not overshoot the point beyond which ETCS will trigger the command of the brakes”.
- Warning (W): “the W supervision limit provides an additional audible warning after the permitted speed has been overpassed”.
- Emergency (EBI): “the braking curve related to the speed decrease due to the emergency brake is the Emergency Brake Intervention (EBI) curve”.

The values for the braking rates of each market segment are given in Table 2. The assumption for all market segments is that the

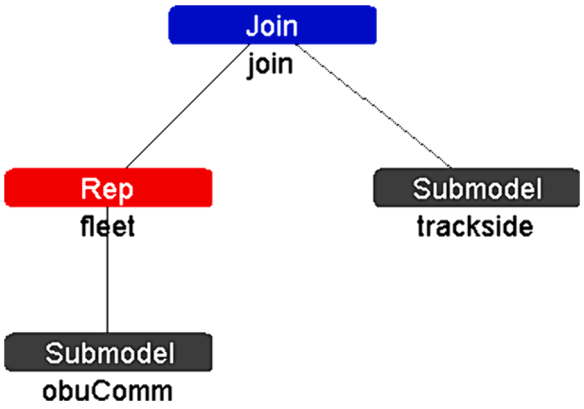

Fig. 6. SAN composed model for Moving Block signalling.

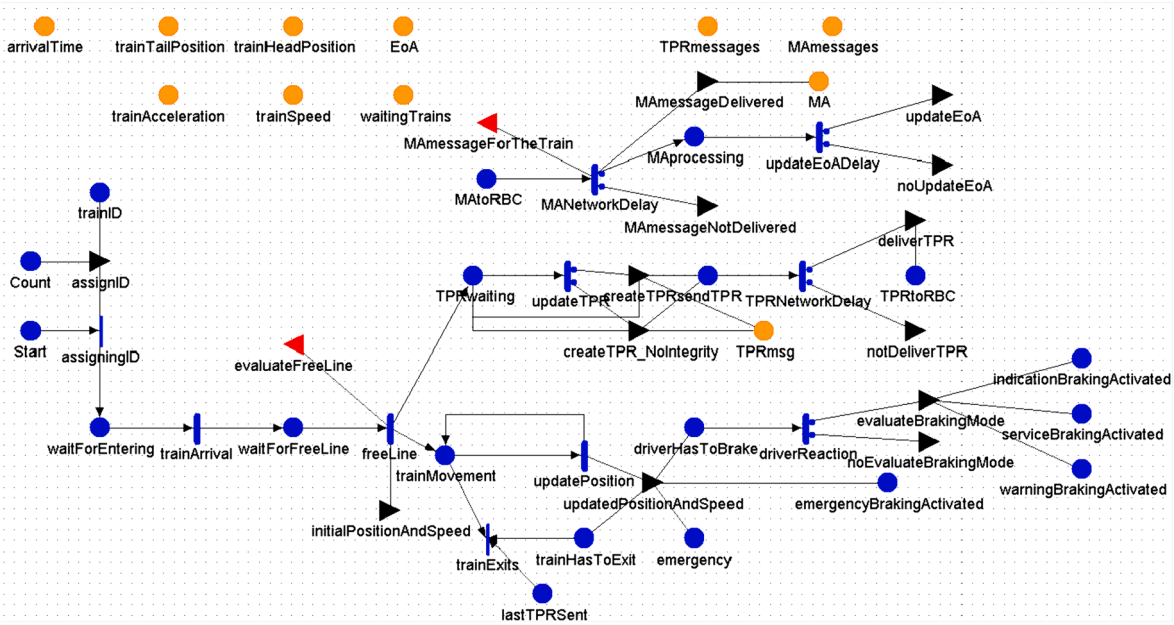

Fig. 7. SAN model for train movement in Moving Block signalling.

emergency braking rate is 25 % more than the warning braking rate and 50 % more than the service braking rate.

Research studies consider different KPIs for train safety. For instance, Scheepmaker et al. (2020) used as KPIs for train safety the time and distance available to run at the release speed between the yellow and red signal. Mlinarić et al. (2018) used as a safety KPI the number of accidents with the aim of minimizing the number of accidents on routes with Intelligent Transport Systems-ITS (including level crossings, train collisions, and derailments). Basile et al. (2022) propose several KPIs to evaluate the effectiveness of VCTS paradigm, namely time headway, time to collision, time trip, tracking error and energy consumption. To fulfil the purpose of this paper for evaluating the effective and safe behaviour of the systems, we only considered the overshooting of the Permitted (P) speed supervision limit that uses a service braking rate as a KPI. This consideration is made because for an effective supervision, the trains should not run into a Warning (W) or Emergency (EBI) operational conditions. A non-effective safe supervision of the service braking rate could lead to safety conditions, and the objective of using the proposed KPI is to have an effective supervision without running into safety–critical conditions.

Several input parameters are needed to enable the computation of the braking curves and the onboard supervision. To compute the braking curves, information is needed, such as the train instantaneous position, speed and acceleration, as well as the driver/ATO reaction time, the track profile, the MA and the braking rates referring to each of the above mentioned ETCS curves. For the onboard supervision computation, the required input parameters are the train data providing the necessary information about the vehicle's braking dynamics and track data.

The model analysis aims at quantitatively evaluating the impacts of a selected set of variables (see Table 1) on the service offered by

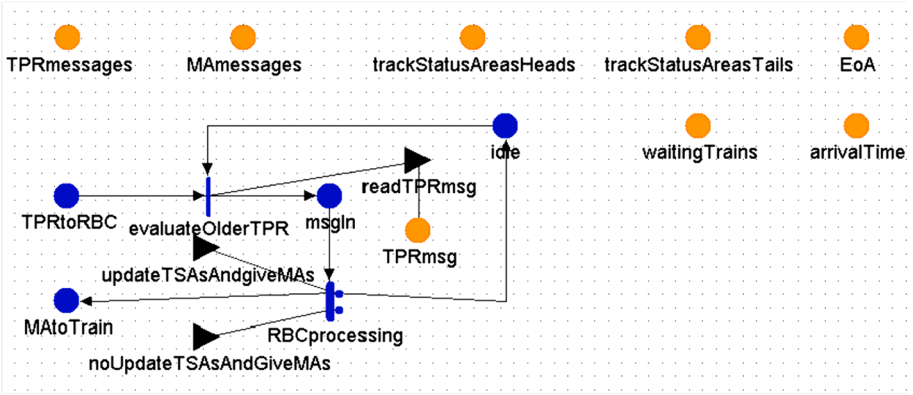

Fig. 8. SAN model of RBC in Moving Block signalling.

the system. The developed models also allow to evaluate the effect of possible failures on the behaviour of the system.

We apply a sensitivity analysis to provide indications about the impact of the MB and VC signalling system functionalities on a safe train movement. We mean by "safe" situations where failures can occur but do not lead to collisions or derailment. Moreover, we look at the capability of signalling systems to safely supervise trains without leading to emergency braking, which could consequently lead to injuries or even fatalities. Therefore, an effective supervision refers to train operations without running into safety–critical conditions. Therefore, we study the impact of fluctuations in signalling design variables on the behaviour of trains based on the number of triggered braking applications during operation. These variables are used as input to our analysis and include the RBC processing time, the RBC to train (MA) communication time, the MA update time, the EVC processing time of the MA, the TPR and integrity update time, the train to RBC (TPR) communication time, the period between subsequent TPRs, and the additional V2V communication (frequency coverage and broadcasting capacity) only in the case of VC. An additional design variable is the driver or ATO reaction time. For a fairer comparison between the outcomes of the MB and VC systems, we consider the ATO reaction when modelling the behaviour of both MB and VC. In the following sections 4.2.2 and 4.2.3, a detailed description of the SAN models for MB and VC is provided, respectively.

4.2.2. SAN model for Moving Block

The SAN introduced in this section provides a high-level representation of the behaviour of the MB system. *Two sub-models* have been developed; the first models the *trackside* sub-system (namely, the *trackside* SAN atomic model which represents the RBC), the second models *the onboard sub-system and the communication* between the trackside and the onboard (namely, the *obuComm* SAN atomic model). They are composed to build the complete SAN model, by instantiating more replicas of the *obuComm* model (one per each train in the fleet) and just one trackside model, which are integrated by the join operation as depicted in Fig. 6.

Fig. 7 illustrates the obuComm SAN atomic model, it represents the movement of a train on a railway track in MB signalling. The extended places (orange circles in Fig. 7) represent all the information needed by a single train such as the arrival time, the train rear position, the train head position, the train speed and acceleration, as well as the EoA, and the TPR and MA messages. Some of them are superposed in the replica and join operations. The management of these places is given to the code written in input and output gates (red and black triangles in the figure, respectively). For the sake of clarity, they are not explicitly connected to the gates which update their values. In fact, gates are part of the transition logic that determines how and when state changes occur. Moreover, by keeping extended places separated from the gates, the model remains clear and each element has a distinct role.

The description of the transition logic of this model, which is the set of ordinary places, activities and gates that govern when a transition can fire, can be separated in different parts. In the left part of the model, a unique ID is assigned to the train (from 0 to N-1): the initial marking of the place *Start* is 1, therefore the instantaneous activity *assigningID* is enabled; when it fires the ID is assigned to the train through the output function of its output gate *assignID* and a token is generated in the place *waitforEntering* to enable in turn the timed transition *trainArrival* whose rate is given by the time distribution function which is deterministic and returns the train arrival time. When the activity *trainArrival* completes, the marking of the place *waitForFreeLine* is incremented and the timed activity *freeLine* is enabled if the associated predicate of the input gate *evaluateFreeLine* evaluates true. The predicate function of the input gate checks the value of the EoA. In case the train is authorized to move, two paths go in parallel; the first on the lower part of Fig. 7 models the movement of the train on the line. When *freeLine* fires, the output gate *initialPositionAndSpeed* is executed, which in turn updates the marking of the place *trainMovement*. Then the train computes its distance to the EoA and the speed at the next step by means of the timed activity *updatePosition* which is enabled by tokens in the place *trainMovement*. This activity executes the output gate *updatedPositionAndSpeed*, which aims at updating the position and speed of the train. More specifically, the train has to brake if its speed distance coordinates hit one of the braking curves computed backward from the EoA. If for a certain amount of time, the current train position hits the permitted speed, then the train would start braking according to a permitted braking curve. In case of emergency braking, tokens are added in the place *emergency* and *emergencyBrakingActivated*. Finally, when the train reaches the end of the line, it has to exit it and a new token is added in the place *trainHasToExit*. It is worth noting that in the proposed model, a fine-grained

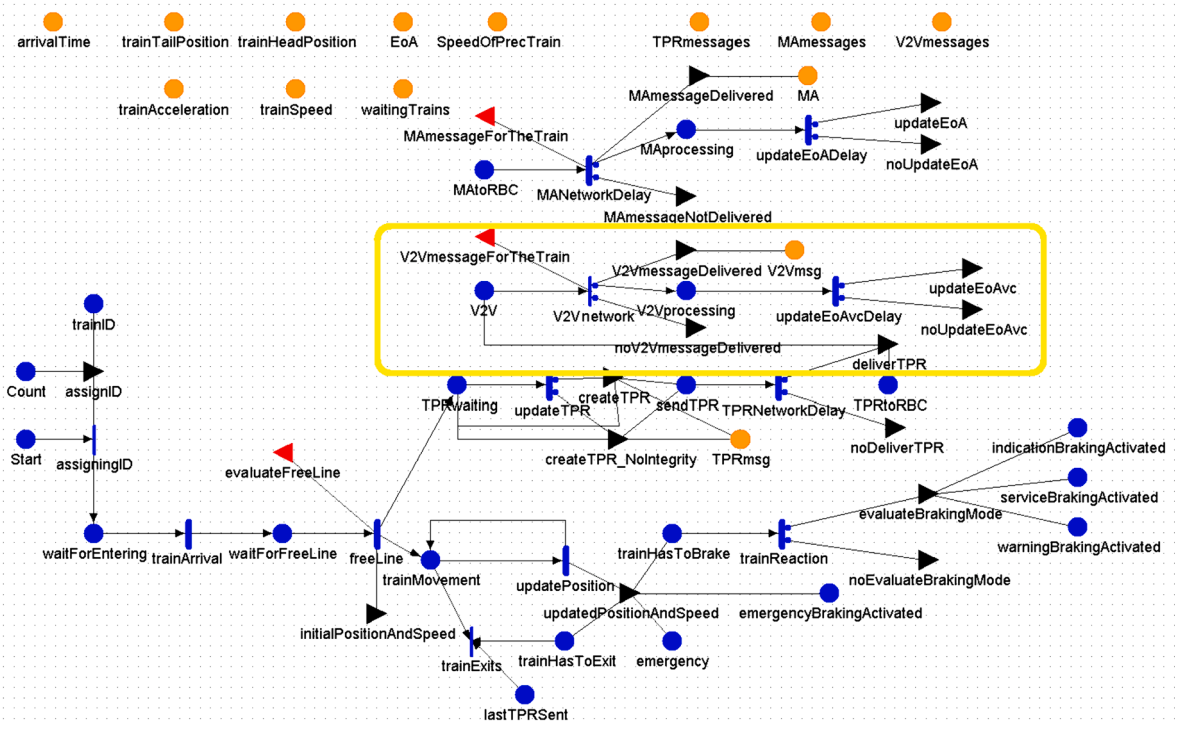

Fig. 9. SAN model for train movement in Virtual Coupling signalling.

discretization of the railway track is used that allows to represent the MB concept by a step-by-step movement of the trains.

Along the second path, on top of the timed activity *freeLine* in Fig. 7, the train continuously computes and sends its TPR to the RBC (the trackside) via the communication network. The elements of the FTA that are displayed in green in Fig. 5 are modelled in the cases of the activities in the SAN models. For instance, the TPR is generated by means of the timed activity *updateTPR*. When the activity *updateTPR* fires, two cases are possible. The first case is when the train confirms its integrity. This enables the execution of the output gate *createTPR,* which in turn updates the marking of the place *sendTPR* and the extended place *TPRmsg* according to the output function associated with the activity. However, the problem is that this function could fail, i.e., cannot know whether the train confirmed its integrity. In that case (i.e., case 2 that enables the output gate *createTPR_NoIntegrity*), the train would need to resend another TPR to the RBC via the communication network. If the train does not deliver a new TPR, the message is lost, and the RBC processes the next received message. Similarly, when the activity *TPRNetworkDelay* fires, two cases are possible. The first enables the execution of the output gate *deliverTPR* which in turn updates the marking of the place *TPRtoRBC.* The second enables the execution of the output gate *notDeliverTPR* which returns zero markings.

At the top part of the figure, an MA is generated by the RBC and sent to the train. Here, a failure could also potentially arise. Therefore, two cases are defined where in the degraded condition, if the MA message is not delivered, the train does not update its EoA and the message is cancelled. The input gate *MAmessageForTheTrain* is to show that there is an MA message ready to be sent from the RBC to the train. The RBC model is developed in a trackside atomic model in Fig. 8.

The trackside atomic model mainly models the exchange of messages between a train and the RBC. In particular, it aims at evaluating the TPR messages received by the train, processing them, updating the track status areas (TSAs) and sending back MA messages to the train (see Fig. 8).

The extended places *TPRmessages* and *MAmessages* are shared with the replicas of the *obuComm* models, and represent the messages on the communication network. The extended places *trackStatusAreasHeads* and *trackStatusAreasTails* model the track status variables of the trackside. Each extended place contains an array of short values, which represents the front and the back position of a track status area, respectively. The values in the i^{th} position of the arrays represent the track status area associated with the train whose ID is *i*. As for the previous figure, also in this model the extended places are not graphically connected to the transition logic, but they are updated from the code executed in the gates.

A token in the place *TPRtoRBC* means that a TPR message is ready to be analysed. The activity *RBCprocessing* models the processing time of the RBC. The output gate *updateTSAsAndgiveMAs* is executed when the activity *RBCprocessing* fires, its output function updates the track status areas (and stores the values in the proper extended places) and generates the MA for the train on the basis of the "known" position of the preceding train.

The trackside has been modelled as a shared resource able to process a single TPR message at a time, this is modelled through the place *idle* which is an input place of the activity *evaluateOlderTPR* and whose initial marking is 1: the token in the place idle is consumed when the TPR message is processed and regenerated after the activity *RBCprocessing* completes.

4.2.3. SAN model for Virtual Coupling

Similar to what is described in the SAN model for MB, the VC model developed in this section (Fig. 9) models the movement of successive trains on railway track. The model analysis aims at quantitatively evaluating the impact of a selected set of variables on the service offered by the system. Those variables apply also to the MB system except for the additional V2V-related variables that are only specific to VC. Note that the V2V additional functionalities were also updated in the RBC atomic model.

Hence, the VC SAN model is based on the MB model but adds a subnet modelling the V2V between trains and some parameters to define the number of convoys moving on the track and the number of trains in the convoys. With respect to the previous model described in Fig. 7, the main part that has been updated is made of elements that are surrounded with the yellow box in Fig. 9. The first train in the convoy sends the TPR message not only to the trackside but also to its following train, through the activity *V2Vnetwork* and the *V2V* place, and each train in the convoy propagates the message back to its follower. The output function of the *deliverTPR* gate and the extended place *V2Vmsg* are used to model this behaviour and the message exchange. Hence, we consider that only the first train in the convoy sends the TPR to the trackside, the following trains just communicate with their immediate neighbours. The V2V network can possibly fail as modelled by the cases of the *V2Vnetwork* activity. Therefore, the developed model also allows to evaluate the effect of possible failures on the behaviour of the trains under VC operation.

5. Results

The methodological framework in Section 3 is applied by starting with the identification of the different system components of MB and VC and the evaluation of their functionalities and dependencies. More details can be found in Aoun et al. (2022) where a breakdown structure of interacting signalling components in both MB and VC is provided.

That breakdown is extended in this work by introducing a cascading sequence of system failures and cause-effect relationships to capture the effect of a component's failure across other components. For instance, a delayed or not received MA from the RBC can lead to a fault in the EVC. As a KPI to measure the safe train supervision effectiveness of MB and VC, we consider the number of times that a train brakes according to the permitted braking curve which uses a service braking rate. As we refer to the ETCS signalling standard, the KPI will hence report the number of overshooting the speed relative to one of the supervised braking curves, namely Indication, Permitted, Warning, and Emergency (ERA, 2020).

This section provides the simulation results and discussion for five case studies (Section 5.1) based on the developed models and outcomes in Section 4. We first set up the simulations. Then we perform the two simulation analyses as explained in Sections 5.3 and 5.4. The execution of simulations has been facilitated by the Möbius tool (Courtney et al., 2009). Möbius is a software tool used for modelling and analysing stochastic systems, which includes support for SANs. In our paper, it specifically supported the Model Specification step, in which we defined the SAN model and the relevant parameters, as described in Section 4. It also supported the Experimental Setup, by enabling the possibility to setup the initial conditions (reported in the following for each experiment), specifying which performance measures to collect, and determining the simulation parameters such as the length of the simulation run and the number of runs for statistical accuracy. Additionally, Möbius supported the Model Solution, by executing the simulations based on the Experiment Setup, showing the results in a graphical interface and storing them in a textual format.

5.1. Case studies

Five case studies are defined in this paper corresponding to a specific corridor of each market segment, namely:

1. For high-speed: Rome–Bologna (Italy).
2. For mainline: London Waterloo–Southampton (United Kingdom).
3. For regional: Leicester–Peterborough (United Kingdom).
4. For urban: London Lancaster–London Liverpool (United Kingdom).
5. For freight: Rotterdam–Hamburg (between the Netherlands and Germany).

The baseline signalling system for mainline, regional, urban and freight railways is three-aspect signalling, whereas for high-speed railways, the baseline is ETCS Level 2.

Since SAN is a parametric model, it was possible to adjust values of train movement parameters to emulate specific operational conditions of a given market segment. In the brake build-up time typical for freight trains, we used in the SAN model a larger value of the reaction time or the control delay of the trains, which resulted in a delayed application of the service brakes, producing the same effect of the brake build-up time.

For all the analysed market segments, the SAN-based effectiveness analysis of MB and VC signalling will be performed on a route stretch of 24 km and a total number of 4 trains for the sake of computational efficiency. A time-step of 0.15 s is used to update kinematic variables of simulated trains such as speed, position and acceleration. For each rail market segment, specific values are considered for train length, maximum speed, maximum acceleration and various braking rates as provided in Table 2. The model was analysed by Möbius running on a notebook equipped with an Intel i7 processor and 16 GB of RAM. The simulation-based solution of such models ensures that longer stretches of line and additional trains could be analysed by executing the solver on more powerful machines (e.g., running it on the cloud), without falling into the typical state space explosion of formal models.

Table 3
Market-specific minimum headway and max TPR for Moving Block and Virtual Coupling.

	Market segment	MB	VC
Minimum Headway (s)	**High-speed**	53	12
	Mainline	43	12
	Regional	40	13
	Urban	39	17
	Freight	69	34
Max TPR net delay (s)	**High-speed**	3.9	1.2
	Mainline	3.8	1.5
	Regional	3.3	1.4
	Urban	2.7	0.9
	Freight	3.9	0.8

5.2. Setting up the simulations

The SAN models introduced so far provide a practical means to analyse the MB and VC systems' behaviour at a high level of abstraction with respect to different variables and parameters. Here information is provided about the simulation in the Möbius tool to introduce the experimental trials. The composed model defines a stochastic process allowing for the evaluation of performance/performability measures of interest. Performance variables relate the stochastic process to such measures, in particular they are reward variables.

A reward variable relates to state markings or activity throughputs, and it is defined through a reward function. Two types of rewards are possible: impulse reward, associated with state changes (at activity completion), and rate reward assigned to markings. A difference is given between Interval-of-Time or Instant-of-Time measures. In particular, for rate reward variables, the former measures accumulate over the interval of time that the model spends in those markings, whereas the Instant-of-Time measure gives the rate reward associated with the markings at time t. Based on the reward model, discrete event simulation is performed. Confidence intervals are generated for the performance variables defined in the reward model using the replication method for terminating simulation. The simulator will run several batches to generate data for the confidence interval. It will continue to run more batches until all the reward variables have converged to their specified confidence interval or the maximum number of batches is reached. A minimum number of batches is specified to cope with rare events. For the MB and VC SAN models, both impulse and rate reward variables are defined:

- The performance variables related to *braking events* are rate rewards on the markings of the onboard sub-model. The rate reward is defined to be an Instant-of-Time measure *evaluating the marking of the places modelling the activation of braking* (e.g., the place *emergencyBrakingActivated* in Fig. 7) at time t for each instance of the *obuComm* atomic model.
- The performance variables measuring *the number of trains exiting the line* in the time interval are instead Interval-of-time rate reward. They provide *the throughput of the activities modelling the trains that exit the line* (e.g., the activity *trainExits* in Fig. 7) in the given interval of time, over all the instances of the the *obuComm* atomic model.

5.3. Analysis of the minimum headway and maximum TPR net delay in Moving Block and Virtual Coupling

The first analysis aims to estimate the minimum headway in free-flow nominal traffic operational conditions, yielding conflict-free train movements. It is worth mentioning that 'conflict-free' does not refer to collisions but rather to smooth operation where there are no unnecessary braking applications that can lead to passengers' discomfort or to the risk of injuries. For this analysis, we consider a minimum processing time of the RBC and onboard as well as minimum communication delays, as reported in Table 1. It is assumed that under VC signalling, trains can form convoys/platoons of up to four trains. More are deemed to be unlikely to operate because of incompatibility with infrastructure characteristics of existing rail networks (e.g., platform lengths, length of interlocking areas).

The results are displayed in Table 3. It is evident from the obtained outcomes for MB that the most critical market segment is high-speed, where the highest maximum speed of the trains requires a high minimum headway and consequently train separation (of around 53 s and 4 km, respectively). On the contrary, trains in the urban segment could run significantly closer one to another (with a minimum separation of 728 m). Regional and mainline railways offer intermediate performance, with a minimum headway of 40 – 43 s and consequently a train separation between 1 and 2 km, respectively. The freight segment also requires high separation of around 1.3 km and 69 s, where the highest length is combined with the lowest braking rate of the trains.

In VC, the minimum separation between two convoys is equal to the one without VC, i.e., under MB operations, but great benefits are evident in the separation among trains in a convoy (see VC in Table 3). In fact, in high-speed, the minimum headway could be reduced by around 77 % (to 12 s). Analogously, the minimum headway in the urban market segment could be reduced by 56 % (to 17 s), which is equivalent to a reduction of 66 % in terms of train separation (244 m). For mainline and regional, the minimum headway could be reduced by respectively 72 % and 68 %. Furthermore, the freight segment could benefit also from the introduction of VC; in fact, the minimum headway could be reduced by 51 % (to 34 s). Hence, with the considered variables, we could say that the advantages are higher for high-speed and mainline railways since VC offers a significant minimum headway reduction.

The impact of the TPR delay is measured in terms of the minimum headway which can be allowed between two consecutive trains

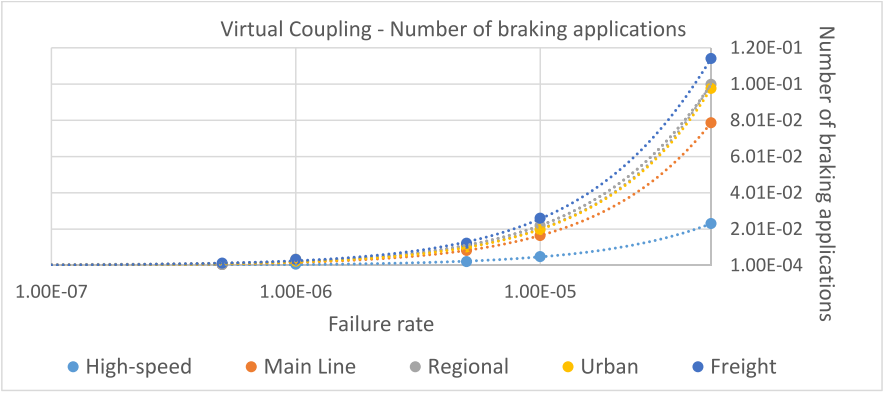

Fig. 10. Number of braking applications vs. TPR error failure rate for Virtual Coupling.

without the trigger of any warning or emergency braking interventions. This means that for a given headway, the max TPR delay is identified as the threshold beyond which trains start activating service braking to avoid overshooting the granted movement authority. The Max TPR delay results show that for all the market segments, the threshold allowed for MB is higher than for VC. This means that to ensure a safe train movement, VC cannot absorb a TPR delay of longer than 1.5 s, which corresponds to the mainline market segment. For MB instead, the results show that the maximum TPR delay can reach 3.9 s for high-speed and freight railways, followed by 3.8 s for mainline railways.

In the case of MB, the max TPR delay follows the minimum headway, which means that the higher the minimum headway, the higher the max TPR delay is. For VC instead, the TPR delay is not dependent on the minimum headway but on the braking rate of the trains assumed per market. This means that on a general trend, a higher braking rate (better braking performance) can tolerate a higher TPR delay. For instance, for high-speed and mainline, the TPR delay can be larger than in the case of urban and freight railways.

The main reason why VC shows larger advantages for those market segments is related to the dynamic safety margin that we have considered (as defined in Quaglietta et al., 2022) to mitigate train collision even in case of sudden emergency braking applications of the leader train. This margin includes among its most relevant terms a function of the service braking rate of the follower minus the emergency braking rate of the leader. This term allows a train to have a full service braking distance to safely stop even if the leader suddenly arrest for an emergency. This term becomes prevalent for markets having trains with lower service braking rate (such as the regional and the freight segment), resulting in longer safe train separations, hence lower headway reductions versus MB.

5.4. *Impact of a TPR error in Moving Block and Virtual Coupling*

In this analysis, the goal is to assess the impact of a TPR error on the overall service offered by the system. We remind that the "TPR error", according to the FTA, can be the effect of two different failures: *(1)* a failure of the onboard system that is either unable to evaluate the train integrity or an error of the odometry subsystem, *(2)* a consequence to a trackside failure due to a fault occurring on the balises. The combination with the FTA helps in the identification of the possible rates of this event, which are then used as an input to the SAN to evaluate the effects on the systems, specifically on the activation of braking.

From the FTA, we estimated that this event shall occur with a maximum rate of 5.58×10^{-10}. We used this value in the SAN and performed a sensitivity analysis by varying it in the range $[10^{-10}, 5 \times 10^{-5}]$ (with a logarithmic step). In fact, for all market segments, we identified the presence of braking with values of failure rates higher than 10^{-7}. This means that the system well tolerates the occurrence of this possible failure, without tangible effects on the service. The analysis is conducted by considering the system at its highest capacity (i.e., trains running at the minimum headway) for the different market segments, to understand the mutual relationships between the considered values of the model variables.

The graph in Fig. 10 shows the relationship between the failure rate of a TPR error (x-axis) and the corresponding number of braking applications (y-axis) which would be triggered under VC train operations. The analysis is performed for each of the five market segments depicted with specific colours as indicated in the legend. The number of braking applications obtained by the SAN-based simulations are represented by the coloured large dots, which are connected by a polynomial regression of the braking curve trend versus the TPR error failure rate.

Based on the experiments that we performed for VC which considered trains moving synchronously at the same speed, we observed that the number of braking applications has a trend that depends on the braking rates of the trains. Specifically, market segments with a higher braking performance result in having on average a lower number of braking applications. Therefore, the influence of a TPR error in VC becomes higher for market segments with lower braking performances, specifically regional and freight railways. In the case of VC, the highest effect is from the braking rate due to the dynamic safety margin term which allows trains to have a full service braking distance to safely arrest even in case of sudden emergency braking applications of the leader. Lower braking performances hence signifies longer train separation between trains under VC. This means that for a given planned headway, the same value of TPR error will affect more markets with lower braking performances as they will need to brake more frequently to maintain the longer

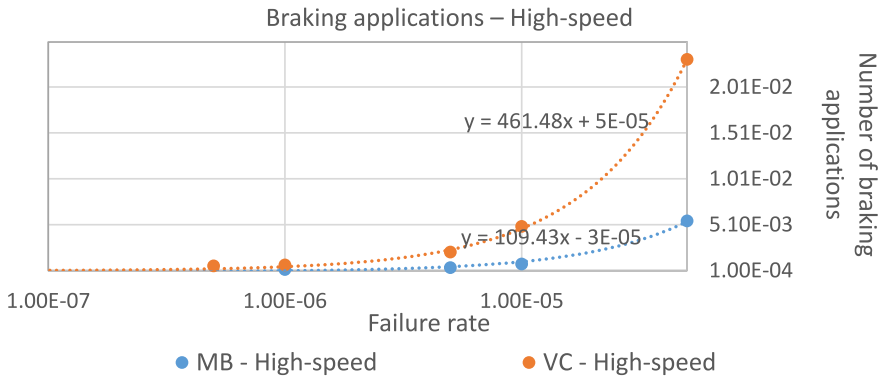

Fig. 11. Braking applications for high-speed in the case of MB and VC.

safety distances. Therefore, as in regional and freight railways the braking rates are relatively low, an error in the TPR would have a higher impact on these market segments than on other segments with higher braking capabilities like high-speed or mainline railways.

Fig. 11 illustrates a comparison of the number of braking applications for MB and VC. For the sake of brevity, we report in this paper the comparison for the high-speed case as similar trends were observed for the other market segments. The results provided by the FTA-SAN experiments match our expectations as VC shows a higher number of braking applications with respect to MB for the same TPR error failure rate. This means that for VC to effectively supervise the train separation at the same safety level as MB, we would need to have a much higher reliability of the TPR. For instance, we have observed that to obtain a number of braking applications of 2×10^{-4} which is obtained for MB for a failure rate of 10^{-6}, we would need a TPR failure rate of VC equal to 3.25×10^{-7}. With reference to Aoun et al. (2021), in order for VC to outperform MB, there is a need to find a KPI that provides the same value of safety to both signalling alternatives. This goal can therefore be achieved by considering the number of braking applications as the KPI for safety that takes into account the corresponding failure rates for each market segment.

6. Conclusions

This paper proposed a novel approach combining FTA and SAN to quantitatively analyse the effectiveness of next-generation signalling in safely supervising train movements under nominal and/or degraded conditions involving signalling equipment failures. An FTA model has been built for both MB and VC which describes the functional relationship among trackside, onboard and radio communication signalling components and mutual cause-effect dependencies which might lead to unsafe train movements. An apportionment of failure rates has been made possible among the different signalling components considering a Safety Integrity Level 4. The component failure rates were then used as input to the SAN model to assess the effectiveness of MB and VC signalling in supervising safe train movements under nominal conflict-free conditions as well as in the scenario that a TPR error occurs. Experiments have been conducted over five different rail market segments by analysing the impact that different failure rates of the TPR can have on the number of braking applications. Specifically, the KPI used for safety and effectiveness relates to the number of braking applications that would be triggered in case a TPR error occurs under MB and VC operations, respectively.

Results indicated that the FTA-SAN method can capture the stochastic behaviour of a system in normal and degraded operational conditions, and could be used for representing concurrent systems such as the V2V communication in VC. In addition, FTA-SAN evaluates the complexities and challenges imposed by new technologies in real-world conditions. The proposed approach can also deal with the aspects of the RAMS analysis, namely reliability, availability, maintenance and safety. The study investigated the effectiveness of MB and VC in safely supervising train movements for several market segments in scenarios involving different types of degraded conditions and failure rates of signalling components and design variables. The results show that the overall approach can support infrastructure managers, railway undertakings, maintenance service providers and data analysts to assess a given configuration of MB and VC signalling components in terms of the effectiveness in supervising and guaranteeing safe train movements. Therefore, the methodology and the models developed so far are promising and have high potential.

In future research, we will continue the model development, by increasing the level of detail of all the modelling artifacts, and this way investigating the application of the FTA-SAN to more specific and more detailed use cases for the safety-performance evaluation of train-centric signalling systems. This would be developed by taking into account the characteristics of the track layouts considered for each case study with switches (merging and diverging junctions), or level crossings, or other exogeneous factors. In addition, as the application of emergency braking could trigger injuries (and fatalities), there is a need to conduct a risk analysis where safety is assessed in terms of both probability and severity.

The impact of a collision or derailment in physically coupled trains is usually very high as all cars in the train move as one whole entity. In VC operations instead, given the fact that a follower train continuously receives updates about the position, speed and acceleration of its predecessor and since the trains are virtually connected, the magnitude of a derailment event might be reduced. This is particularly true when an adequate dynamic safety margin is modelled and designed to ensure a sufficient distance in case of emergency braking of the leader train. Therefore, a recommendation for future research would be to do a Risk Assessment according to

the Common Safety Method (CSM-RA) to evaluate the potential types of accidents that might occur in the case of VC and better understand whether and how the collision propagation can be restrained to the following trains within the same convoy.

CRediT authorship contribution statement

Joelle Aoun: Conceptualization, Formal analysis, Investigation, Methodology, Visualization, Writing – original draft. **Rob M.P. Goverde:** Validation, Writing – review & editing. **Roberto Nardone:** Formal analysis, Visualization. **Egidio Quaglietta:** Funding acquisition, Project administration, Supervision, Writing – review & editing. **Valeria Vittorini:** Formal analysis, Visualization.

Acknowledgements

This research has received partial funding from the Shift2Rail Joint Undertaking (JU) under the European Union's Horizon 2020 research and innovation programme under Grant Agreement N. 101015416 PERFORMINGRAIL. The JU receives support from the European Union's Horizon 2020 research and innovation program and the Shift2Rail JU members other than the Union. The content of this document reflects only the authors' view — the Joint Undertaking is not responsible for any use that may be made of the information it contains.

References

Aoun, J., Goverde, M.P., Nardone, R., Quaglietta, E., Vittorini, V., 2022. "Towards a fault tree analysis of moving block and virtual coupling railway signalling systems", In: *Proceedings of the 6th International Conference on System Reliability and Safety (ICSRS)*, Venice, Italy.

Aoun, J., Quaglietta, E., Goverde, R.M.P., 2020. Investigating market potentials and operational scenarios of virtual coupling railway signaling. Transp. Res. Rec. 2674 (8), 799–812. https://doi.org/10.1177/0361198120925074.

Aoun, J., Quaglietta, E., Goverde, R.M.P., Scheidt, M., Blumenfeld, M., Jack, A., Redfern, B., 2021. A hybrid Delphi-AHP multi-criteria analysis of moving block and virtual coupling railway signalling. Transp. Res. Part C: Emerging Technol. 129, 103250.

Aoun, J., Quaglietta, E., Goverde, R.M.P., 2023. Roadmap development for the deployment of virtual coupling in railway signalling. Technol. Forecast. Soc. Chang. 189, 122263.

ASTRail Consortium, 2019. "Deliverable 2.2 Moving Block signalling system Hazard Analysis".

Basile, G., Napoletano, E., Petrillo, A., Santini, S., 2022. Roadmap and challenges for reinforcement learning control in railway virtual coupling. Discover Artif. Intell. 2, 2022, 27.

Bertolino, A., Calabró, A., Di Giandomenico, F., Nostro, N., 2011. "Dependability and Performance Assessment of Dynamic CONNECTed Systems", In: Bernardo, M., Issarny, V. (eds), *Formal Methods for Eternal Networked Software Systems. SFM 2011. Lecture Notes in Computer Science*, pp. 350-392, Springer, Berlin, Heidelberg.

Biagi, M., Carnevali, L., Paolieri, M., Vicario, E., 2017. Performability evaluation of the ERTMS/ETCS – level 3. Transp. Res. C 82, 314–336.

Clark, G., Courtney, T., Daly, D., Deavours, D., Derisavi, S., Doyle, J.M., Sanders, W.H., Webster, P., 2001. "The Möbius Modeling Tool", In: *Proceedings of The 9th IEEE International Workshop on Petri Nets and Performance Models*, Aachen, Germany.

Courtney, T., Gaonkar, S., Keefe, K., Rozier, E.W., Sanders, W.H., 2009. Möbius 2.3: an extensible tool for dependability, security, and performance evaluation of large and complex system models. In: In: 2009 IEEE/IFIP International Conference on Dependable Systems & Networks. IEEE, pp. 353–358.

Da Silva, L.D., Lollini, P., Mongelli, D., Bondavalli, A., Mandò, G., 2021. A stochastic modeling approach for traffic analysis of a tramway system with virtual tags and local positioning. J. Braz. Comput. Soc. vol. 27, article number 2.

Di Meo, C., Di Vaio, M., Flammini, F., Nardone, R., Santini, S., Vittorini, V., 2019. ERTMS/ETCS virtual coupling: proof of concept and numerical analysis. IEEE Trans. Intell. Transp. Syst. 21 (6), 2545–2556.

Europe's Rail, Work Programme 2022-2024 adopted by the EU-Rail Governing Board on 1 March 2022, 2022.

European Commission, 2023. ETCS Levels and Modes, Mobility and Transport. Available at: https://transport.ec.europa.eu/transport-modes/rail/ertms/what-ertms-and-how-does-it-work/etcs-levels-and-modes_en.

European Railway Agency (ERA), 2020. *Introduction to ETCS Braking Curves – ERTMS*.

European Union Agency for Railways (EUAR), 2023. Control command and signalling TSI. Available at: https://www.era.europa.eu/domains/technical-specifications-interoperability/control-command-and-signalling-tsi_en.

Fantechi, A., Gnesi, S., Gori, G., 2022. "Future Train Control Systems: Challenges for Dependability Assessment", In: *Proceedings of the 11th International Symposium Part IV – Leveraging Applications of Formal Methods, Verification and Validation (ISoLA 2022)*, Rhodes, Greece.

Felez, J., Kim, Y., Borrelli, F., 2019. A model predictive control approach for virtual coupling in railways. Transactions on Intelligent Transportation Systems 20, 2728–2739.

Fenner, D., 2016. UK Railway Safety & Standards Board research into 'Closer Running'. *Institution of Railway Signal Engineers (IRSE) NEWS*, vol. 225, pp. 11-15.

Flammini, F., Marrone, S., Nardone, R., Petrillo, A., Santini, S., Vittorini, V., 2019. Towards Railway Virtual Coupling. In: *Proceedings of The 2018 IEEE International Conference on Electrical Systems for Aircraft, Railway, Ship Propulsion and Road Vehicles and International Transportation Electrification Conference*, Nottingham, UK.

Flammini, F., Marrone, S., Nardone, R., Vittorini, V., 2021. Compositional modeling of railway virtual coupling with stochastic activity networks. Form. Asp. Comput. 33 (6), 989–1007.

Isograph, 2020. Reliability Workbench. Available at: https://www.isograph.com/software/reliability-workbench/.

Khakzad, N., Khan, F., Amyotte, P., 2011. Safety analysis in process facilities: comparison of fault tree and bayesian network approaches. Reliab. Eng. Syst. Saf. 96, 925–932.

Limnios, N., 2007. Fault trees. ISTE Ltd, London.

Mahboob, Q., Straub, D., 2011. "Comparison of Fault Tree and Bayesian Networks for Modeling Safety Critical Components in Railway Systems", In: *Proceedings of Advances in Safety, Reliability and Risk Management, European Safety and Reliability Conference (ESREL)*.

Meyer, J.F., Movaghar, A., Sanders, W.H., 1985. Stochastic activity networks: structure, behavior, and application. IEEE Computer Society, Washington, DC, International workshop on timed Petri Nets, pp. 106–111.

Mlinarić, T.J., Đorđević, B., Krmac, E., 2018. Evaluation framework for key performance indicators of railway ITS. Scientific Journal on Traffic and Transportation Research 30 (4), 491.

MOVINGRAIL (MOving block and VIrtual coupling New Generations of RAIL signalling, 2018, EU Horizon.

MOVINGRAIL, 2020. *Business Analysis of Virtual Coupling*, Deliverable D4.3, Shift2Rail.

National Aeronautics and Space Administration (NASA), 2002. *Fault Tree Handbook with Aerospace Applications*, Office of Safety and Mission Assurance, Washington, DC.

PERFORMINGRAIL, 2020. Deliverable D4.1 Real-Time Traffic Rescheduling Algorithms for Perturbation Management and Hazard Prevention in Moving-Block Operations.

Quaglietta, E., Wang, M., Goverde, R.M.P., 2020. A multi-state train-following model for the analysis of virtual coupling railway operations. J. Rail Transp. Plann. Manage. 15, 100195.

Quaglietta, E., Spartalis, P., Wang, M., Goverde, R.M.P., van Koningsbruggen, P., 2022. Modelling and analysis of virtual coupling with dynamic safety margin considering risk factors in railway operations. J. Rail Transp. Plann. Manage. 22, 100313.

RailEngineer, 2023. Migrating from GSM-R to FRMCS, Paul Darlington. Available at: https://www.railengineer.co.uk/migrating-from-gsm-r-to-frmcs/.

RailTech, 2022. FRMCS to replace GSM-R by 2030. Available at: https://www.railtech.com/infrastructure/2022/05/24/frmcs-to-replace-gsm-r-by-2030/?gdpr=deny.

Sanders, W.H., Malhis, L.M., 1992. Dependability evaluation using composed SAN-based reward models. J. Parallel Distrib. Comput. 15, 238–254. https://doi.org/10.1016/0743-7315(92)90006-9.

Sanders, W.H., Meyer, J.F., 2001. Stochastic activity networks: formal definitions and concepts. Lectures on Formal Methods and Performance Analysis 2090, 315–343.

Sanders, W.H., 1999. "Integrated frameworks for multi-level and multi-formalism modeling," In: *Proceedings of PNP M'99: 8th International Workshop on Petri Nets and Performance Models*, Zaragoza, Spain.

Scheepmaker, G.M., Willeboordse, H.Y., Hoogenraad, J.H., Luijt, R.S., Goverde, R.M.P., 2020. Comparing train driving strategies on multiple key performance indicators. J. Rail Transp. Plann. Manage. 13, 100163.

Shubinsky, I.B., Rozenberg, E.N., Baranov, L.A., 2023. "Safety-critical railway systems", In: M. Ram, L. Xing (eds.), *Reliability Modeling in Industry 4.0*, Elsevier, pp. 83-122.

Theeg, G., Vlasenko, S., 2009. Railway Signalling & Interlocking: international compendium. Eurailpress, Hamburg.

UIC, 2023. FRMCS Future Railway Mobile Communication System. Available at: https://uic.org/rail-system/telecoms-signalling/frmcs.

UNISIG, 2019. "SUBSET-088-2 Part 1 - ETCS Application Level 2 - Safety Analysis, Part 1 - Functional Fault Tree", issue 3.7.0.

X2Rail-1, 2019. Start-up activities for Advanced Signalling and Automation Systems. Moving Block Preliminary Safety Analysis, Deliverable 5.3, Shift2Rail.

X2Rail-3, 2018. "Advanced Signalling, Automation and Communication System (IP2 and IP5) – Prototyping the future by means of capacity increase, autonomy and flexible communication", Shift2Rail.

X2Rail-3, 2020. Virtual Train Coupling System Concept and Application Conditions. Deliverable 6.1, Shift2Rail.

Zafar, N.A., Khan, S.A., Araki, K., 2012. Towards the safety properties of moving block railway interlocking system. Int. J. Innovative Comput., Information and Control 8, 5677–5690.