Future train control systems: challenges for dependability assessment

Alessandro Fantechi[1][0000−0002−4648−4667], Stefania Gnesi[2][0000−0002−0139−0421], and Gloria Gori[1][0000−0002−8482−2612]

[1] University of Florence, Via S. Marta 3, 50139 Florence, Italy
[2] ISTI-CNR, Via G. Moruzzi 1, 56127 Pisa, Italy

Abstract. The prospected advent of advanced train control systems, such as moving block and virtual coupling, raises the issue of the effects that uncertainty on critical parameters (such as position or speed) can have on dependability. Several approaches to the evaluation of such effects have been proposed, typically based on a state-based formal modelling of the system behaviour. We present a survey of such proposals.

Keywords: Train control systems · Dependability assessment · Uncertainty.

1 Introduction

This century has seen several innovation proposals for railway transport, most of which ask for a significant advancement of train control systems. The increasing need to boost the volume of passenger and freight rail transport, while decreasing the cost, require running more trains on the existing tracks, asking for notable improvements of the operation principles of nowadays railways.

Buzzwords such as Moving Block, Virtual Coupling, Autonomous Trains, are frequently used in the visions of the railways of the future, although still quite far from the everyday life in the, rather conservative, railway domain.

The main reason for the conservativeness of the domain can be found in the safety concerns. Indeed, the advanced train control systems needed to realize the new functionalities, pose important challenges regarding safety guarantees.

One main paradigm shift that these new technologies require is to abandon the "absolute safety" that has often ruled the railway operation, in favour of a "probabilistic safety", that is anyway already foreseen in the safety guidelines issued for the development of signalling systems.

As reported in [15] one common problem of the proposed advanced train control systems is to guarantee safety in presence of some form of uncertainty on vital parameters, such as train positioning, train speed and acceleration, etc...

On the other hand, even though the same level of safety can be eventually guaranteed with respect to traditional systems, the actual adoption of the prospected systems will be possible only if they can fully exhibit their dependability, expressed in terms of availability and performability, that is, in terms of service regularity and capacity.

An emerging trend of the latest decades is to address the evaluation of dependability by means of model-based quantitative evaluation of the dependability attributes that are of interest.

The aim of this paper is actually to survey the research efforts that are available in the literature that employ formal modelling to evaluate safety and/or some dependability attributes, such as availability and performability, under some form of (quantifiable) uncertainty over vital information produced by sensors or by the system itself.

The paper is organized as follows: in Sect. 2 the context and vision for future train systems is introduced, in Sect. 3 we give a short introduction to the formalisms adopted in the literature, in Sect. 4 a survey of the most recent literature contribution is provided and Sect. 5 closes the paper illustrating final considerations and future research challenges.

2 Context

2.1 Future railway systems

The increasingly wide deployment of ERTMS-ETCS systems witnesses the possible achievement of high safety standards by means of advanced ICT technologies. ERTMS relies on the European Train Control System (ETCS), an Automatic Train Protection (ATP) system which continuously supervises the train, ensuring that the maximum safe speed and minimum safe distance are respected. ETCS is specified at four levels of operation, depending on the role of wayside equipment and on the way the information is transmitted to/from trains. Only the first two levels have been actually implemented to date.

The Level 3 of operation (ETCS-L3), currently still in development, improves upon Level 2 by removing the wayside equipment for detecting the occupancy of fixed-length tracks (fixed-block). Rather, the ETCS-L3 relies on the *moving block* principle, computing at run-time the maximum distance that a train is allowed to travel based on the knowledge of the position of the rear end of the foregoing train. In doing so, the headway between trains can be considerably reduced, improving the line capacity.

Although main line ETCS-L3 has been deployed only in experimental forms, moving block is currently implemented in automatic metros, as a feature of CBTC (Communication Based Train Control) [24]. CBTC systems for metro operations typically include Automatic Train Operation (ATO) systems, that are responsible for driving, but are still subject to a safety enforcing ATP system. ATO systems of this kind are increasingly considered for future main line implementation [1].

The availability of safe information about the position, speed, acceleration and deceleration of the preceding train, envisaged in ETCS Level 3 and in CBTC, has further inspired the idea of an innovative method of train formation, called *Virtual Coupling* [40, 17]. The concept is based on the idea of multiple trains (possibly, individual self propelling units) which run one behind the other without physical contact but at a smaller distance compared to that achievable with

moving block. The strict real-time control of the dynamic parameters of the following train with respect to those of the preceding one allows the distance between trains to be minimized, therefore with consequent increased capacity. Increased flexibility is another goal, for example in the forwarding of different segments of a train to different destinations through "on-the-fly" composition and decomposition, without stopping the train. The cross-control between coupled trains has to be negotiated locally, with a train to train communication, since it requires a precision on the relative distance between the trains that cannot be supported by ETCS-like systems.

In a parallel with the automotive domain, and inheriting autonomous cars technology, another direction of innovation is to move more and more intelligence onboard trains, to let them take autonomous decisions, with little help of ground-based infrastructure [16]. However, the physics of train motion, that requires long stretches of free track to attain high speeds, poses several challenges to the adoption of autonomy in train control.

2.2 Uncertainty

In all the innovation directions sketched above, one key element is the availability of accurate information on position, speed, acceleration of trains, as well as a strict control of the timing at which such information is related. However, the need of accurate measures of position of trains and of their speed introduces the need of coping with *uncertainty* over such measures, quantified as an error interval around the measured quantity of interest.

Uncertainty in positioning is usually managed by allowing for a longer safety margin, by assuming a maximum uncertainty threshold: in railways, positioning of a reference (say, the head) of a train is one-dimensional, because it refers to a point on the line. Uncertainty makes position to stay within an interval, so safety margins have to be computed accordingly. Speed uncertainty can be handled similarly: if an error interval is known, integrating it over time gives a position uncertainty.

One cause of uncertainty of position information is given by the positioning mechanism itself. In fixed block systems, the position of a preceding train is given by the block that it currently occupies: it is not known where the train rear end actually is inside the block, and this is conservatively considered to be at the end of the block.

In the more sophisticated positioning systems required by moving block, uncertainty is typically associated to position and speed measurement, which may be affected by random or systematic errors.

Information on trains position and speed may also be provided by satellite positioning devices. These are widely used in avionic satellite navigation, and gives, together with a position estimation, a so called *protection level*. The protection level is a statistical bound error computed to guarantee that the probability of the (unknown) real position error exceeding the protection level is smaller than or equal to a target value (called *integrity risk*). In other words, the interval (given by the protection level) around the estimated position does not contain

the real position with probability less than the integrity risk. The target integrity risk can be computed in relation to the desired THR (Tolerable Hazard Rate), a measure of the accepted level of risk of collisions or derailments.

Delays in communication and the periodic, rather than continuous, nature of communications introduce another source of uncertainty: timestamps and time-out mechanisms are used in ETCS to prevent impact on safety of a missing or out-of-time MA reception, stopping the train when given uncertainty thresholds are passed.

Last but not least, we can foresee that autonomous driving of trains will be based, as their automotive counterpart, on an increasing usage of Artificial Intelligence (AI) techniques (e.g. for artificial vision systems), that pose a significant challenge to deterministic certification of safety [16]. The widespread adoption in automotive applications will favour the acceptance of machine learning engines, or similar techniques, as "proven in use" software, especially considering that trains move in a much more predictable environment than cars, hence favouring reliability of machine learning techniques. Anyway, the estimation of the probability of incorrect classification of an AI engine may constitute another source of quantified uncertainty.

2.3 Dependability attributes

As indicated by the Shift2Rail JU [34], the primary objectives of introducing technological advances in train traffic control are not only related to an increase in the already very high safety standards of railways, but rather to preserve such standards while dramatically improving KPIs such as performability (often intended as adherence to expected timetables), availability of transport service and transport capacity, all attributes that in computer science terms could be tagged as *liveness properties*, that often conflict with safety objectives.

On the other hand, the large number of critical computing components and the complexity of distributed control algorithms increase the number of cases in which the failure of one component can bring to a fail-safe halt of a system, causing the partial or full unavailability of transport service.

This effect is worsened by the number of communication links employed in these systems: typically, the safety layers of the communication protocols adopted in these systems exploit the principle of *positive* control to allow movement of trains: a train cannot move if no explicit consensus or MA has been received. Any serious transmission error (that is, persistent over a given period of time) eventually leads to a fail-safe state. A careful evaluation of safety cannot therefore ignore an adequate analysis of availability attributes, in order to ensure an appropriate transport capacity, with the related operation cost effectiveness, through techniques of quantitative evaluation of these attributes [33].

3 Model-based evaluation of dependability

In the domain of train control systems, if we look to approaches and techniques that address uncertainty, we are confronted with two main categories, with different final aim:

- "constructive" techniques: coming from control theory, typically consider uncertainty as a disturbance input to the control algorithm, and aim at maintaining at run time the stability of some critical parameter within a certain range. The range is determined a priori as a safe one for train control. An example of critical parameter is distance between the leader and the follower trains in a virtual coupling scheme. Techniques like Model Predictive Control are adopted to keep this distance within a predetermined range also in presence of limited disturbances due to the uncertainties of read parameters, e.g. inaccuracy of the position [44] or lost train-2-train messages [39]. The lower bound of the stability distance range is determined in this case by safety consideration, while the upper bound is determined so to guarantee the least capacity gain that is promised by the introduction of virtual coupling. This research stream has been pursued in several other research efforts, especially regarding virtual coupling: a complete account is not however in the scope of this paper.
- "deductive" techniques: quantitative analysis techniques have the aim to predict, off-line, specific dependability attributes (such as safety, availability, performability) in presence of uncertainty on critical information. Typically a dependability attribute is defined as the probability $P(t)$ of the system being in a certain state at time t; thresholds or upper/lower bounds to such prediction classify the system as safe or available, or are used to plan maintenance actions, depending on the attribute of interest.
  Quantitative analysis techniques allow to evaluate the $P(t)$ dependability attribute as a function of the uncertainty quantification by means of a state-based model of the behaviour of the system.
  Consider for example a train control system that should fulfill a safety requirement expressed by requiring that a collision between two controlled trains occurs less than once in 10^9 operation hours. Suppose that the train control system critically depends on the correct localization of one of the trains: knowing the uncertainty range of the computed position, a deductive quantitative evaluation allows for computing the probability of a collision due to wrong localization, as a function of such uncertainty. The resulting probability should be lower of the above threshold, in order to guarantee safety also in case of localization uncertainty.

However, the probabilistic estimation of dependability needs often to take into account the distributed structure and status of the system, and the occurrence of relevant events such as reception of messages or component failures. A state-based model can describe at best these dependencies. Attaching probabilities to events and states, allows then for a fine modelling of the evolution in time of dependability attributes as time varying probability distribution.

Model-based evaluation of dependability is therefore an important enabling technique to tackle the problems that we have introduced so far: a model of the behaviour of the system is first defined, and uncertainty is taken into account, in the form of probability of inaccuracy produced by uncertainty sources. An evaluation of the model allows in the end to estimate specific dependability attributes as a function of inaccuracy. Such evaluation can provide constraints over inaccuracy that keep dependability under control.

In this paper, we survey a selection of recent works that have adopted model-based quantitative analysis techniques according to the principles enunciated above in the railway domain, classifying them in terms of techniques used, problems addressed and kind of uncertainty considered. In the next section we briefly describe the quantitative analysis frameworks that have been used in the surveyed literature.

3.1 Proposed modelling frameworks

In the literature surveyed in Section 4 several modelling frameworks have been adopted, ranging from variants of Petri nets to Stochastic Activity Networks, from Probabilistic Timed Automata to Fault Trees, and several tools supporting their quantitative evaluation have been adopted. In the following, we give a short introduction for each adopted formalisms, mentioning the related support tools.

Petri Nets A Petri net consists of places, transitions, and arcs [30]. Arcs run from a place to a transition or vice versa, but not between places nor between transitions. The places from which an arc runs to a transition are called the input places of the transition; the places to which arcs run from a transition are called the output places of the transition.

Graphically, places in a Petri net may contain a finite number of marks called tokens. Any distribution of tokens over the places will represent a configuration of the net called a marking. A transition of a Petri net may fire if it is enabled, i.e. there are sufficient tokens in all of its input places; when the transition fires, it consumes the required input tokens, and creates tokens in its output places. A firing is atomic, i.e. a single non-interruptible step.

Since firing is nondeterministic, and multiple tokens may be present anywhere in the net (even in the same place), Petri nets are well suited for modeling the concurrent behavior of distributed systems.

Stochastic Petri Nets Stochastic Petri nets are an extension of Petri nets, where the transitions fire after a probabilistic delay determined by a random variable [6].

The analysis of SPN is based upon Markov theory; with respect to other popular fameworks exploiting Markov Theory, such as queueing networks, SPN the ability to describe system behaviors like blocking, forking and synchronisation

between distributed en tities. The π-Tool[3] was developed with the aim to establish a computer-supported, clear Petri net modeling of real systems with the implementation of a complete RAMS analysis. The tool provides a streamlined interface for creating comprehensive system models based on Petri nets. It allows a visualized simulation (token game), an analysis of the model and the identification of deadlocks, which are included in the model. All common stochastic distributions can be assigned to the transitions. With the help of simulation and the determination of the switching rates of the individual transitions, all values of the RAMS aspects can read off easily. For this π-tool uses various analysis methods, state-based or stochastic ones, to consider the system sufficiently reliable.

Another tool that supports analysis of Stochastic Petri Nets, as well as Coloured Petri Nets, is TimeNET, ([45, 46]) which exploits different solution algorithms that can be used depending on the net class.

Stochastic Timed Petri Nets The need for including timing variables in the models of various types of dynamic systems is apparent since these systems are real time in nature. When a Petri net contains a time variable, it becomes a Timed Petri Net [42]. The firing rules are defined differently depending on the way the Petri net is labeled with time variables. Stochastic timed Petri nets (STPN) are Petri nets in which stochastic firing times are associated with transitions. An STPN is essentially a high-level model that generates a stochastic process. STPN-based performance evaluation basically comprises modeling the given system by an STPN and automatically generating the stochastic process that governs the system behavior. This stochastic process is then analyzed using known techniques. STPN's are a graphical model and offer great convenience to a modeler in arriving at a credible, high-level model of a system.
The analysis of STPN is supported by the ORIS Tool [8, 29], which efficiently implements the method of stochastic state classes, including regenerative transient, regenerative steady-state, and non-deterministic analyses.

Stochastic Colored Petri Nets In a standard Petri net, tokens are indistinguishable. Because of this, Petri nets have the distinct disadvantage of producing very large and unstructured specifications for the systems being modeled. To tackle this issue, high-level Petri nets were developed to allow compact system representation. Colored Petri nets [25] and Predicate/Transition (Pr/T) nets [20] are among the most popular high-level Petri nets. A Colored Petri Net (CPN) has each token attached with a color, indicating the identity of the token. Moreover, each place and each transition has attached a set of colors. A transition can fire with respect to each of its colors. By firing a transition, tokens are removed from the input places and added to the output places in the same way as that in original Petri nets, except that a functional dependency is specified between the color of the transition firing and the colors of the involved tokens.

[3] https://www.iqst.de/en-pitool/

The color attached to a token may be changed by a transition firing and it often represents a complex data-value. CPNs lead to compact net models by using of the concept of colors. CPN Tools [26] support analysis of CPNs, by simulation and state space exploration.

Stochastic Colored Petri Nets (SCPN) [19] combine the strength of GSPN (Generalised Stochastic Petri Nets) with a high-level programming language, making SCPN very powerful in modelling large, complex and dynamic systems in a compact way. Generalized Stochastic Petri Nets (GSPN) are an extension of Petri Nets incorporating two types of transitions: immediate transitions and timed transition. Immediate transitions correspond to transitions in classic Petri Nets and fire immediately if enabled. Timed transitions, by contrast, fire after an exponentially distributed time $t - \exp(\lambda)$.

Immediate transitions have priority over timed transitions. In case multiple immediate transitions are enabled, firing order is according to a specific firing policy.

Stochastic Activity Networks Stochastic Activity Networks (SANs) are a convenient, graphical, high-level language for describing systems behavior. SANs are a stochastic generalization of Petri nets, defined for the modeling and analysis of distributed real-time systems. A SAN is composed of places, activities, input gates, and output gates. Places and activities have the same interpretation as places and transitions in Petri nets. Input gates control the enabling conditions of an activity and define the change of marking when an activity starts. Output gates define the change of marking upon completion of the activity. Activities can be of two types: instantaneous or timed. Instantaneous activities complete once the enabling conditions are satisfied. Timed activities take an amount of time to complete, following a temporal stochastic distribution function which can be, e.g., exponential or deterministic. Cases are associated to activities, and are used to represent probabilistic uncertainty about the action taken upon completion of the activity. Primitives of the SAN models are defined using C++ code.
The mostly used stochastic analysis tool for SANs are Moebius [11] that can be traced back much further, to its predecessors UltraSAN [12, 31] and MetaSAN [32]. Moebius [11] offers a distributed discrete-event simulator, and, for Markovian models, explicit state-space generators and numerical solution algorithms.

Timed Automata and Statistical Model checking Timed automata are finite-state automata enhanced with real-time modelling through clock variables; their stochastic extension replaces non-determinism with probabilistic choice and time delays with probability distributions (uniform for bounded time and exponential for unbounded time). These automata may communicate via (broadcast) channels and shared variables. The resulting stochastic hybrid automata (SHA) form the input models of the statistical model checker UPPAAL SMC [13] on which it is possible to check (quantitative) properties over simulation runs. Statistical Model Checking (SMC) concerns running a sufficient number of

(probabilistically distributed) simulations of a system model to obtain statistical evidence (with a predefined level of statistical confidence) of the quantitative properties to be checked. UPPAAL SMC is an extension of UPPAAL [21], a toolbox for the verification of real-time systems modelled by (extended) timed automata. The properties must be expressed in Weighted Metric Temporal Logic (WMTL) [9]. Statistical Model Checking may be traced back to hypothesis testing in the context of probabilistic bisimulation. Tools that support SMC are more recent: the first version of UPPAAL SMC was released in 2014.

Dynamic Fault Trees Fault Tree Analysis (FTA) is one of the well-established and widely used methods for safety and reliability engineering of systems. Fault trees (FTs), in their classical static form, are directed acyclic graphs (DAG) with nodes defining a boolean relation (AND, OR, etc.) over the successor nodes. Nodes without successors are called basic (failure) events. Occurrences of basic events are governed by probability distributions. Similarly, a node fails if the failure condition over the children holds. The probability of failure of the top-level event can be computed by properly combining those of the basic events. FTs are however inadequate for modelling dynamic interactions between components and are unable to include temporal and statistical dependencies in the model. Dynamic Fault Trees (DFT) were introduced to enhance the modelling power of its static counterpart [10]. In DFT, the expressiveness of fault tree has been improved by introducing new dynamic gates. While the introduction of the dynamic gates helps to overcome many limitations of FTs and allows to analyse a wide-range of complex systems, it adds some overhead, e.g. the straightforward combinatorial approaches used for qualitative and quantitative analysis are no longer applicable to DFTs.

Several tools have been developed to model and analyse DFT [2], among which here we mention STORM [27], which performs probabilistic model checking by generating from the DFT a continuous-time Markov chain (CTMC) which captures its behavior of the DFT. The CTMC is analyzed with respect to reliability metrics.

4 Survey of railway case studies

In the following survey of applications of model-based dependability techniques in the railway domain we start by the innovations that can be considered not far from deployment, by shifting gradually to the more visionary ones.

4.1 Performability evaluation of the ERTMS/ETCS – Level 3

The pioneer paper [45] is considered the first to develop Stochastic Petri net models of communication behaviour of the ERTMS/ETCS L3 moving block system. Stochastic Petri nets are used to model and evaluate in a hierarchical way the failure and recovery behavior of the train-to-RBC communication link, and to model the exchange of location information and movement authority

between train and RBC. The models evaluation, obtained through customized SPN resolution algorithms, supported by the TimeNET Tool ([45, 46]) shows the significant influence of reliability of the underlying communication system on efficient train operation.

In [7], the authors develop the results of [45] by presenting a communication model with multiple concurrent non-exponential timers, computing an upper bound on the first-passage probability that a train is stopped due to a communication failure. The authors combine analytic evaluation of failures due to burst noise and connection losses with numerical solution of a non-Markovian model representing also failures due to handovers between radio stations. The analysis, supported by the ORIS tool, show that the periodic trains transit at handovers makes the behavior of the overall communication system recurrent over the period of message exchanges and the periodic arrivals at cell borders.

4.2 Safety evaluation of moving block systems by statistical model checking

In [3] the full moving block specification for ETCS-L3 is formally described by Probabilistic Timed Automata. UPPAAL SMC is used to verify safety properties in presence of communication delays, and to verify whether the performability gain (1 minute minimum headway) promised by moving block can be obtained in such setting.

Statistical Model checking is also used in [28] inside a more complex framework aimed at hazard and risk prediction in Communication Based Train Control based on train-to-train communication, also based on deep recurrent neural networks. An ad hoc algorithm based on SMC is used for estimating the probability of wrong Movement Authority calculation.

Finally, in in [23], authors carry out an analysis of a Zone Controller (ZC) handover scenario, a typical operation function in Communication Based Train Control (CBTC) system. However, due to the nondeterministic communication between the onboard equipment and the ZC, the behavior of delay and timeout determine the complexity of probability evaluation. The authors propose a novel method based on Statistical Model Checking (SMC), which introduces a sequential operator to evaluate the probabilities of all scenarios in a CBTC system. In a CBTC system, different scenarios have different behaviors and probabilities. Therefore, in the ZC handover process, the trigger handover, crossing the demarcation point and logout switching scenarios are modeled by Network Priced Timed Automata (NPTA); the whole probability of successful ZC handover is evaluated as 0.99985, a high value that guarantees that the safety requirements of the CBTC system are satisfied.

4.3 Train-to-train communication modeling

Due to high installation and maintenance costs of wayside equipment, moving more and more intelligence on board is considered as a promising direction, and

this requires to develop adequate train-to-train communication means. Starting from his PhD Thesis [36], Haifeng Song has addressed, with colleagues in Braunschweig, modeling and analysis dependability attributes of innovative systems of this kind [37, 38]. In particular, an enhanced movement authority system is proposed, which combines advantages of the *train-centric communication* with current movement authority mechanisms. To obtain the necessary train distance interval data, the onboard equipment and a new train-to-train distance measurement system (TTDMS) are applied as normal and backup strategies, respectively. To assist the system development, Colored Petri nets are used to formalize and evaluate the system structure and its behavior. The system performance is assessed in detection range and accuracy by means of both mathematical simulation and practical measurements validation. The results indicate that the system is feasible to carry out distance measurements both in metropolitan and main railway lines.

In [39] availability and performance of a direct train-to-train communication system is studied, considering different parameters that can affect the performance of the communication system, such as bit error and transmission rates. The system availability and performance are evaluated by means of Stochastic Petri nets.

Train-to-train communication is also studied in [41] in the context of Virtual Coupling, as reported later in the section on this topic.

4.4 Modelling uncertainty in satellite localisation

Satellite positioning has been recently considered as an enabling technique for moving block, since it potentially allows a train to know its position and speed at any time. A characteristic of this technology is that the position information given by a GNSS receiver comes already associated with an uncertainty measure, that shows the probability with which the real position is in an envelope centered on the computed position. Providing safety evidence for a system based on this technology necessarily requires hence to adopt quantitative safety evaluation.

In [22] the authors present a model-based approach, adapted for the evaluation of GNSS-based localisation systems in railway. Models are defined using probabilistic timed automata, to achieve a modular representation of trains dynamics in the context of GNSS-based localization. In particular, the representation of the position related errors, the mechanisms of balises detection and the dynamics of the trains movements are addressed. The safety and performance properties to be checked are formulated by means of temporal logics. The evaluation phase by UPPAAL-SMC yields both qualitative and quantitative results and allows for assessing the impact of various parameters and functional choices on both safety and performance.

4.5 Safety and availability of virtual balises: the SISTER project

Traditional solutions for tramway interlocking systems are based on physical sensors (balises) distributed along the infrastructure which detect passing of the

trams and trigger different actions, like the communications with the ground infrastructure and the interlocking system. This approach is not easily scalable and maintainable, and it is costly. One of the aims of the SISTER project was the study of a possible substitution of track circuits by virtual track circuits supported by satellite positioning. The key idea is to trigger actions when the local position computed on board a tram corresponds to a virtual tag. However, the estimated position, even in absence of faults, is affected by errors, compared to the real one. Therefore, it is important to understand the impact of these new solutions on the traffic that can be supported by the tramway network.

In [5], the authors investigate this issue with the definition of a model of the envisaged solution, and its analysis using UPPAAL Statistical Model Checker. The analysis emphasises how the virtualisation of legacy track circuits and on-board satellite positioning equipment may give rise to new hazards, not present in the traditional system.

In [35] the same issue is faced with a stochastic modeling approach aiming to identify the parts of the tramway network that are more critical and sensible to the variation of the traffic conditions and to the setting of the key architectural parameters. The presented model is built using Stochastic Activity Networks and sensitivity analyses are run on the accuracy of the positioning, on the different SISTER parameters, and considering possible outages temporarily blocking the journey of a tram. This analysis allows to properly set and fine-tune the key architectural parameters, to understand the impact of the accuracy on the positioning, to understand the impact of the outages.

4.6 Virtual Coupling: performability evaluation

Virtual Coupling has raised the interest of several research groups active in model-based quantitative analysis.

In [14] the authors provide a proof of concept of Virtual coupling by introducing a specific operating mode within the ERTMS/ETCS standard specification, and by defining a coupling control algorithm accounting for time-varying delays affecting the communication links. To support the proof of concept with quantitative results in a case-study simulation scenario, the authors provide a numerical analysis exploiting a methodology used to study platooning in the automotive field.

[18] aims at providing an approach to investigate the potential of Virtual Coupling in railways by composing Stochastic Activity Networks model templates. to provide an approach to perform quantitative evaluation of capacity increase in reference to Virtual Coupling scenarios. The approach can be used to estimate system capacity over a modelled track portion, accounting for the scheduled service as well as possible failures. Due to its modularity, the approach can be extended towards the inclusion of safety model components. The contribution of this paper is a preliminary result of the PERFORMINGRAIL (PERformance-based Formal modelling and Optimal tRaffic Management for movING-block RAILway signalling) project funded by the European Shift2Rail Joint Undertaking.

The paper [41] presents a model-based approach for the evaluation of the communication system under virtual coupling operation. Namely, Stochastic Colored Petri Net (SCPN) models are developed to depict the exchanges of the various information needed under virtual coupling operation. The analysis scope is limited to function Supervising Train Separation Distance. Dependability evaluation is then performed by means of simulation; the impact of various communication parameters is examined while taking into account different operational scenarios. The obtained results allow the identification of the most impacting aspects on dependability analysis and provide valuable inputs to support the technological choices in terms of communication to implement virtual coupling.

In [44], the authors analyse the virtual coupling operation mode under train control system based on train-to-train communication, and compare it with a traditional train operation mode. A typical scenario of train virtual coupling is described by SysML, and the key properties of the function, such as boundedness and reachability, are validated by modeling with Colored Petri nets. In this paper, formal modeling and verification of typical scenarios in the train virtual coupling mode are carried out to ensure that the system meets safety, functionality and performance requirements.

4.7 Reliability and maintenance plans

Reliability engineering of railway infrastructure aims at understanding failure processes and improving the efficiency and effectiveness of investments and maintenance planning, so that a high quality of service is achieved. In particular, quantitative methods to analyze the service reliability associated with specific system designs are emerging as a promising research activity.

In [43] formal fault-tree modeling is proposed for providing a quantitative assessment of the railway infrastructure's service reliability in the design phase. While, individually, most subsystems required for route-setting and train control are well understood, the system's reliability to globally provide its designated service capacity is less studied. To this end, a framework based on dynamic fault trees is proposed to analyze the possibilities of routing trains on paths provided by the interlocking system. The work focuses on the dependency of train paths on track-based assets such as switches and crossings, which are particularly prone to failures. By using probabilistic model checking to analyze and verify the reliability of feasible route sets for scheduled train lines, performance metrics for reliability analysis of the system as a whole as well as criticality analysis of individual (sub-)components become available. The fault trees obtained in the analysis of major stations contain up to 6 million states and are among the largest described in the literature. By allowing to pinpoint critical infrastructure components, the approach is suited to provide assistance in asset management to improve the effectiveness and efficiency of infrastructure investments, maintenance and monitoring systems.

4.8 Summary

Table 1 summarizes the findings in the cited literature. The *Goal* column shows the evaluation goal, where Av stands for Availability, R for Reliability, S for Safety, C for Capacity, P for some specific kind of Performability.

Table 1. Summary of the reviewed literature

Ref.	Y.	APPLICATION	FORM.	TOOL	UNCERTAINTY	Goal
[45]	2005	Comm. in ETCS L3	SPN, GSPN	TimeNET	Handover loss, packet loss	R
[7]	2017	ERTMS/ETCS-L3	STPN	ORIS	Burst noise, comm. losses	P
[3]	2022	ETMS/ETCS L3	PTA	UPPAAL SMC	Communication delays	S,P
[28]	2020	T2T comm. in CBTC	own tool	SMC	Wrong MA computation	S
[23]	2020	Zone controller	SMC	UPPAAL SMC	Communication delays	S
[37]	2017	T2T Dist. Meas. Sys.	CPN	CPNTools	Connection failures	S
[39]	2019	T2T communication	SPN	Pi-Tool	communication latency	Av,P
[22]	2021	satellite positioning	PTA	UPPAAL SMC	Positioning error	S, P
[5]	2021	sat. posit., tram	PTA	UPPAAL SMC	Positioning error	S
[35]	2021	sat. posit., tram	SAN	Moebius	Positioning error	Av
[14]	2020	Virtual Coupling	PN	Simulation	Communication delays	P
[18]	2021	Virtual Coupling	SAN	Moebius	Communication delays	C
[41]	2021	T2T communication	SCPN	TimeNET	Communication delays	Av
[44]	2020	Virtual Coupling	CPN	CPNTools	Communication delays	Av
[43]	2022	Infrastruct. Mainten.	DFT	STORM	Switch failures	R

Looking at the table, we can note a certain prevalence of Petri net based models and tools: the used tools are typically of academic origin, and although they may differ in the offered features and the evaluation algorithms employed, they are actually competing in the "market" of model-based dependability analysis.

We refer to [4] for a comparison of the modelling and analysis capabilities of two formalisms from the two classes and their associated support based tools, namely UPPAAL SMC and Moebius.

The existence of diverse, competing tools may serve the purpose of defining multiple modelling processes able to compare results obtained with different tools and formalisms, strengthening the results in case of concordance, and helping to detect modelling errors or biases otherwise. Due to the need of guaranteeing specific dependability targets in the domain of advanced railway signalling, multiple modelling can be an important element in the process.

5 Conclusions

The surveyed literature, far from being complete, is nevertheless representative of the main research activities in this area, and shows already that quantitative modeling of dependability of future train control systems is spreading more and more in the recent years in academic research, and is a promising enabling

technique in support of the development of innovative and more performing train control systems. Support tools are still at a low Technical Readyness Level (TRL), although a few of them, such as UPPAAL and Moebius have a quite large adoption base. Industrial application of these techniques and tools is still limited, but will be in our opinion necessary for the successful adoption of the prospected future train control systems.

References

1. Amendola, A., Barruffo, L., Bozzano, M., Cimatti, A., Simone, S.D., Fedeli, E., Gabbasov, A., Garrubba, D.E., Girardi, M., Serra, D., Tiella, R., Zampedri, G.: Formal design and validation of an automatic train operation control system. In: Dutilleul, S.C., Haxthausen, A.E., Lecomte, T. (eds.) Proc. RSSRail 2022. LNCS, vol. 13294, pp. 169–178 (2022), https://doi.org/10.1007/978-3-031-05814-1_12
2. Aslansefat, K., Kabir, S., Gheraibia, Y., Papadopoulos, Y.: Dynamic Fault Tree Analysis: State-of-the-Art in Modelling, Analysis and Tools, pp. 73–112 (06 2020)
3. Basile, D., ter Beek, M.H., Ferrari, A., Legay, A.: Exploring the ERTMS/ETCS full moving block specification: an experience with formal methods. Int J Softw Tools Technol Transfer (Apr 2022)
4. Basile, D., ter Beek, M.H., Giandomenico, F.D., Fantechi, A., Gnesi, S., Spagnolo, G.O.: 30 Years of Simulation-Based Quantitative Analysis Tools: A Comparison Experiment Between Möbius and Uppaal SMC. In: Margaria, T., Steffen, B. (eds.) Proc. ISoLA 2020 Part I. LNCS, vol. 12476, pp. 368–384 (2020)
5. Basile, D., Fantechi, A., Rucher, L., Mandò, G.: Analysing an autonomous tramway positioning system with the Uppaal Statistical Model Checker. Form Asp Comp **33**(6), 957–987 (Dec 2021)
6. Bause, F., Kritzinger, P.S.: Stochastic Petri nets - an introduction to the theory (2. ed.) (2002)
7. Biagi, M., Carnevali, L., Paolieri, M., Vicario, E.: Performability evaluation of the ERTMS/ETCS – Level 3. Transp Res Part C **82**, 314–336 (Sep 2017)
8. Bucci, G., Carnevali, L., Ridi, L., Vicario, E.: Oris: a tool for modeling, verification and evaluation of real-time systems. Int J Softw Tools Technol Transfer **12**(5), 391–403 (2010)
9. Bulychev, P., David, A., Larsen, K.G., Legay, A., Li, G., Poulsen, D.B.: Rewrite-based statistical model checking of WMTL. In: Qadeer, S., Tasiran, S. (eds.) Runtime Verification. pp. 260–275 (2013)
10. Cepin, M., Mavko, B.: A dynamic fault tree. Reliab. Eng. Syst. Saf. **75**(1), 83–91 (2002), https://doi.org/10.1016/S0951-8320(01)00121-1
11. Clark, G., Courtney, T., Daly, D., Deavours, D., Derisavi, S., Doyle, J., Sanders, W., Webster, P.: The mobius modeling tool. In: Proc. 9th Int. Workshop on Petri Nets and Perf. Models. pp. 241–250 (2001)
12. Couvillion, J., Freire, R., Johnson, R., Obal, W., Qureshi, M., Rai, M., Sanders, W., Tvedt, J.: Performability modeling with UltraSAN. IEEE Softw **8**(5), 69–80 (1991)
13. David, A., Larsen, K.G., Legay, A., Mikuăionis, M., Poulsen, D.B.: Uppaal SMC tutorial. Int J Softw Tools Technol Transf **17**(4), 397–415 (aug 2015)
14. Di Meo, C., Di Vaio, M., Flammini, F., Nardone, R., Santini, S., Vittorini, V.: ERTMS/ETCS Virtual Coupling: Proof of Concept and Numerical Analysis. IEEE Trans on ITS **21**(6), 2545–2556 (Jun 2020)

15. Fantechi, A.: Connected or autonomous trains? In: Dutilleul, S.C., Lecomte, T., Romanovsky, A.B. (eds.) Proc. RSSRail 2019. LNCS, vol. 11495, pp. 3–19 (2019)
16. Flammini, F., Donato, L.D., Fantechi, A., Vittorini, V.: A vision of intelligent train control. In: Dutilleul, S.C., Haxthausen, A.E., Lecomte, T. (eds.) Proc. RSSRail 2022. LNCS, vol. 13294, pp. 192–208 (2022)
17. Flammini, F., Marrone, S., Nardone, R., Petrillo, A., Santini, S., Vittorini, V.: Towards railway virtual coupling. In: Int Transp Electrif Conf (ITEC) (2018)
18. Flammini, F., Marrone, S., Nardone, R., Vittorini, V.: Compositional modeling of railway Virtual Coupling with Stochastic Activity Networks. Form Asp of Comp **33**(6), 989–1007 (Sep 2021)
19. Gehlot, V., Nigro, C.: Colored petri net model of the session initiation protocol (sip). IECON 2010 - 36th Annual Conference on IEEE Industrial Electronics Society pp. 2150–2155 (2010)
20. Genrich, H.J.: Predicate/transition nets. In: Brauer, W., Reisig, W., Rozenberg, G. (eds.) Petri Nets: Central Models and Their Properties. pp. 207–247 (1987)
21. Hendriks, M., Yi, W., Petterson, P., Hakansson, J., Larsen, K., David, A., Behrmann, G., Hendriks, M., Yi, W., Petterson, P., Hakansson, J., Larsen, K., David, A., Behrmann, G.: UPPAAL 4.0. In: QEST'06. pp. 125–126 (2006)
22. Himrane, O., Beugin, J., Ghazel, M.: Toward Formal Safety and Performance Evaluation of GNSS-based Railway Localisation Function. IFAC-PapersOnLine **54**(2), 159–166 (Jan 2021)
23. Huang, J., Lv, J., Feng, Y., Luo, Z., Liu, H., Chai, M.: A novel method on probability evaluation of ZC handover scenario based on SMC. In: Qian, J., Liu, H., Cao, J., Zhou, D. (eds.) Robotics and Rehabilitation Intelligence. pp. 319–333 (2020)
24. IEEE: Vehicular technology society, 1474.1 - standard for communications - based train control (CBTC) - performance and functional requirements. (2004)
25. Jensen, K.: Coloured petri nets. In: Brauer, W., Reisig, W., Rozenberg, G. (eds.) Petri Nets: Central Models and Their Properties. pp. 248–299 (1987)
26. Jensen, K., Kristensen, L.M., Wells, L.: Coloured Petri Nets and CPN Tools for modelling and validation of concurrent systems. International Journal on Software Tools for Technology Transfer **9**(3), 213–254 (2007)
27. Katoen, J.: The probabilistic model checking landscape. In: Grohe, M., Koskinen, E., Shankar, N. (eds.) Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science, LICS '16, New York, NY, USA, July 5-8, 2016. pp. 31–45 (2016), https://doi.org/10.1145/2933575.2934574
28. Liu, J., Zhang, Y., Han, J., He, J., Sun, J., Zhou, T.: Intelligent hazard-risk prediction model for train control systems. IEEE Trans on ITS **21**(11), 4693–4704 (2020)
29. Paolieri, M., Biagi, M., Carnevali, L., Vicario, E.: The ORIS Tool: Quantitative Evaluation of Non-Markovian Systems. IEEE Trans on Softw Eng **47**(6), 1211–1225 (2021)
30. Reisig, W.: Petri nets and algebraic specifications. Theor. Comput. Sci. **80**(1), 1–34 (1991), https://doi.org/10.1016/0304-3975(91)90203-E
31. Sanders, W., Obal, W., Qureshi, M., Widjanarko, F.: The UltraSAN modeling environment. Perf Eval **24**(1), 89–115 (1995), performance Modeling Tools
32. Sanders, W., Meyer, J.: METASAN: A performability evaluation tool based on Stochastic Activity Networks. pp. 807–816 (Dec 1986)
33. Schulz, O., Peleska, J.: Reliability analysis of safety-related communication architectures. In: Proc. SAFECOMP 2010. pp. 1–14 (2010)

34. Shift2Rail Joint Undertaking: Multi-annual action plan (November 2015), http://ec.europa.eu/research/participants/data/ref/h2020/other/wp/jtis/h2020-maap-shift2rail_en.pdf
35. da Silva, L.D., Lollini, P., Mongelli, D., Bondavalli, A., Mandò, G.: A stochastic modeling approach for traffic analysis of a tramway system with virtual tags and local positioning. J of the Brazilian Comp Soc **27**(1), 2 (Feb 2021)
36. Song, H.: Development and analysis of a Train-centric Distance Measurement System by means of Colored Petri Nets. Ph.D. thesis (2018)
37. Song, H., Liu, J., Schnieder, E.: Validation, verification and evaluation of a train to train distance measurement system by means of Colored Petri Nets. Rel Eng & Sys Safety **164**, 10–23 (2017)
38. Song, H., Schnieder, E.: Modeling of railway system maintenance and availability by means of colored Petri nets. EiN **20**(2), 236–243 (Mar 2018)
39. Song, H., Schnieder, E.: Availability and Performance Analysis of Train-to-Train Data Communication System. IEEE Trans on ITS **20**(7), 2786–2795 (Jul 2019), conference Name: IEEE Trans on ITS
40. UIC: Virtually coupled trains, http://www.railway-energy.org/static/Virtually_coupled_trains_86.php. Accessed 24 Feb. 2019.
41. Verma, S., Ghazel, M., Berbineau, M.: Model-based dependability evaluation of a Wireless Communication System in a Virtually Coupled Train Set. IFAC-PapersOnLine **54**(2), 179–186 (Jan 2021)
42. Wang, J.: Stochastic Timed Petri Nets and Stochastic Petri Nets, pp. 125–153 (1998)
43. Weik, N., Volk, M., Katoen, J.P., Nießen, N.: DFT modeling approach for operational risk assessment of railway infrastructure. Int J Softw Tools Technol Transfer (Apr 2022)
44. Yong, Z., Sirui, Z.: Typical Train Virtual Coupling Scenario Modeling and Analysis of Train Control System Based on Vehicle-Vehicle Communication. In: 2020 IEEE 6th ICCSSE. pp. 143–148 (Jul 2020)
45. Zimmermann, A., Hommel, G.: Towards modeling and evaluation of ETCS real-time communication and operation. J Syst Softw **77**(1), 47–54 (Jul 2005)
46. Zimmermann, A., Knoke, M., Huck, A., Hommel, G.: Towards version 4.0 of TimeNET. pp. 1 – 4 (04 2006)