COMPUTER-AIDED CIVIL AND INFRASTRUCTURE ENGINEERING

Computer-Aided Civil and Infrastructure Engineering **31** (2016) 193–218

A Markovian–Bayesian Network for Risk Analysis of High Speed and Conventional Railway Lines Integrating Human Errors

Enrique Castillo*, Aida Calviño & Zacarías Grande

Department of Applied Mathematics and Computational Sciences, University of Cantabria, 39005 Santander, Spain

Santos Sánchez-Cambronero, Inmaculada Gallego, Ana Rivas & José María Menéndez

Department of Civil Engineering, University of Castilla-La Mancha, 13071 Ciudad Real, Spain

Abstract: *The article provides a new Markovian–Bayesian network model to evaluate the probability of accident associated with the circulation of trains along a given high speed or conventional railway line with special consideration to human error. This probability increases as trains pass throughout the different elements encountered along the line. A Bayesian network, made up of a sequence of several connected Bayesian subnetworks, is used. A subnetwork is associated with each element in the line that implies a concentrated risk of accident or produces a change in the driver's attention, such as signals, tunnel, or viaduct entries or exits, etc. Bayesian subnetworks are also used to reproduce segments without signals where some elements add continuous risks, such as rolling stock failures, falling materials, slope slides in cuttings and embankments, etc. All subnetworks are connected with the previous one and some of them are multiconnected because some consequences are dependent on previous errors. Because driver's attention plays a crucial role, its degradation with driving time and the changes due to seeing light signals or receiving acoustic signals is taken into consideration. The model updates the driver's attention level and accumulates the probability of accident associated with the different elements encountered along the line. This permits us to generate a continuously increasing risk graph that includes continuous and sudden changes indicating where the main risks appear and whether or not an action must be taken by the infrastructure manager. Sensitivity analysis allows the relevant and irrelevant parameters to be identified avoiding wastes of time and money by concentrating safety improvement actions only on the relevant ones. Finally, some examples are used to illustrate the model. In particular, the case of the Orense–Santiago de Compostela line, where a terrible accident took place in 2013.*

*To whom correspondence should be addressed. E-mail: *castie@unican.es*.

DOI: 10.1111/mice.12153

1 INTRODUCTION AND MOTIVATION

High speed trains have produced a revolution in the rail and transportation industries. Increasing speeds have led trains to successfully compete with air transportation (see Peterman et al., 2009; Todorovich and Hagler, 2011). However, accident risks and their consequences have also increased due to high speeds (see Andersson et al., 2015). This has motivated: (1) the need of probability risk assessments (PRAs) with the aim of improving safety and having a better knowledge of railway system behavior (see Lahrech, 1999; Miyashita, 2010; or Fukuyama et al., 2008), (2) the appearance of automatic train protection (ATP) systems that allow human errors to be corrected by stopping trains when necessary, and (3) the development of natural disaster early warning systems (see, e.g., Veneziano and Papadimitriou, 2001). In this problem, cooperation between industry and universities is crucial (see Sussman, 1996).

In this article, we deal with the problem of PRA of a given railway line and operating company. A guide for the preparation of risk assessments within railway safety cases is given in Beales (2002). In this guide, a huge effort is made to quantify the risks and consequences with some rigor, but in the end only a qualitative risk assessment is carried out. Similar ideas to those in this guide are applied in other countries, but unfortunately in some cases no detailed or rigorous quantification of risk is carried and only a global and poor qualitative analysis is performed (see, e.g., Ministerio de Trabajo y Asuntos Sociales, 2010; Instituto Nacional de Seguidad e Higiene en al Trabajo; Dirección de Seguridad en la Circulación, ADIF). However, a qualitative evaluation of railway risks (see, e.g., Masanori and Fumiaki, 2008) is not sufficient and some quantitative approaches should be used.

The Safety Risk Model (SRM) used by the RSSB (Railway Safety Standard Board) is based on the quantification of the risk resulting from hazardous events that have the potential to lead to fatalities, major or minor injuries. The SRM enables risk to be calculated in terms of collective, individual, or societal components. A full list of the 110 hazardous events forms the basis of the SRM. However, this type of risk analysis is global. For example, the total risk to passengers, staff, and members of the public from the 110 hazardous events modeled within the SRM, excluding suicides, was predicted to be 138 equivalent fatalities per year in 2002 with the existing current control measures (see Muttram, 2002).

The SRM provides risk information to be used in risk assessments, helping to understand the contribution of the different elements or failure modes to overall risk and to get a structured representation of causes and consequences of potential accidents arising in the railway operation and maintenance. However, line or segment risk assessments are not very common (see Lahrech (1999) for some small examples) and SRM does not provide risk profiles for specific lines of route and train operating companies but provides some bases for assessing such risk.

Nuclear power plants and air transport industries have a long tradition in using new and powerful techniques for quantitative PRAs (see, e.g., Henley and Kumamoto, 1992), such as fault and event tree analysis, Petri and Bayesian networks, discrete and continuous Markov models, etc. However, the railway industry runs slowly in this area and is at an initial stage for a systematic implementation of such methods in all countries. Nevertheless, some of the reliability and risk assessment methods used in nuclear power plants have been extrapolated to railway lines (see Bearfield and Marsh, 2005; Flammini et al., 2006), but this has been criticized because they need to be adapted to reproduce the special and particular case of railways in a better way. However, some countries, such as Japan, the United States, and the United Kingdom, use models as the SRM, where fault and event tree analysis are used and have been adapted to the railway problem. SRM is an important tool in a series of those recently developed for railway safety analysis.

Thus, though PRAs are commonly used in nuclear and aeronautical industries, they are seldom used in the rail industry. Some examples of the use of the risk assessment methodology in project management are given in Mokkapati et al. (2009) who provide a methodology for risk assessment, or Kawakami (2014) who discusses the risk analysis of high-speed rail project managements in the United States. Unfortunately, the final consequence is that in many countries PRAs are not compulsory and are not regularly used in testing the safety of railway lines.

As indicated, in this work we provide some railway-oriented methods and tools to analyze, assess, and evaluate in a probabilistic framework the risks associated with railway operations, with a special emphasis on human errors. More precisely, we adopt a different approach and concentrate on the assessment of the risk associated with a particular line reproducing the evolution of the driver's attention.

The risk associated with a railway line must include the frequency of hazardous events and their consequences (see Muttram, 2002). One way to do it is by using the number of equivalent fatalities per event, km, year, etc. Muttram (2002) points out that as society in general has an aversion to single accidents which result in multiple fatalities, it is important to be able to estimate the potential frequency of this type of accident.

When an accident occurs, investigations must not be reduced to similar hazardous events but to other potential ones. In addition, they must be analyzed looking for the actually observed and other potential causes. Unfortunately, because the location of the next accident cannot be predicted, preventing measures must be applied to all potential locations and cases, thus leading to very expensive changes that are not always socially justified. The model presented in this article allows us to analyze existing or potential lines and to identify where some actions (investments) are required.

Once we have a parametric model for PRA, we need to estimate its parameters. This is a crucial step that must be done with care if the results are to be interpreted quantitatively. In this context, the works of Kokkings and Snyder (1997), Muttram (2002), and Evans (2011), who report important railway data and a very interesting statistical analysis of the railway accidents which occurred in Europe during the period 1980–2009, become relevant.

Human error is an important factor that has to be considered in any PRA. Quantification of human error probabilities is possible with participation of miscellaneous groups of professionals including operators, conductors, PRA experts, statisticians, etc. (see, e.g., Wreathall et al., 2003; Dadashi et al., 2013; Zeilstra and Van der Weide, 2013).

This article was prompted by recent railway accidents in Spain and in the United States, where exceeding the speed limit and lack of control of this human error was the main cause. It was also motivated by the appearance of alternate double–single track lines for low-demand areas (see Castillo et al., 2011 or Castillo et al., 2014b) which allow important savings in construction and maintenance costs but contain single track segments that require a more careful risk analysis to be done.

The main original contributions of this article are:

1. For the first time, a model is presented to evaluate the risk associated with a given railway line with integration of human errors, that is, the model considers how the tiredness and the attention level of the driver evolves with traveled distance and how the latter is affected by the different signals, including acoustic ones, and other elements along the line. We note that we consider not only driver's fatigue, but the evolution of driver's attention during the driving caused by signals, sounds, etc. and their effects on train safety.
2. A Bayesian network made up by integrating different Bayesian subnetworks associated with the different elements in the line, implying a risk or a change in the driver's attention, is proposed. Contrary to fault trees (see Lahrech, 1999), Bayesian networks (see Castillo et al., 1999) allow any joint probability distribution without limitations to be reproduced with respect to dependence structures, including common causes. We want to highlight this contribution because it is new to high speed and conventional railway risk analysis in the way it is proposed.
3. A sensitivity analysis method is proposed to identify the most influential variables and to indicate those probability parameters that must be estimated with care and those that need not be estimated with precision because they have a little influence on the final risk. This reduces the complexity of the problem.
4. Some methods are given to calibrate and validate the model in real cases.
5. The model may be applied to specific lines after new types of risks are identified. Rather than systemically applying remediations, which can be very expensive, the model allows individual lines to be analyzed and the effectiveness of such remediations can be compared to their costs for site-specific application. This potentially saves resources that can be used to more effectively mitigate risk in more beneficial applications, which in turn could reduce casualties over all.
6. Some simple and some real examples are given to illustrate the power of the proposed methods.

The article is organized as follows. In Section 2, the proposed Markovian–Bayesian model is motivated. In Section 3, a detailed description of the Markovian–Bayesian model is given. In Section 4, we describe in detail the Bayesian network variables and the associated conditional probability tables. In Section 5, some simple examples of applications are used to illustrate the power of the proposed methods. In Section 6, we present a summary of the Orense–Santiago line where the accident took place. In Section 7, we provide some methods for parameter estimation and validation of the model. Finally, in Section 8, some conclusions are given.

2 JUSTIFICATION OF THE MARKOVIAN–BAYESIAN NETWORK MODEL

Safety evaluation of a railway line requires considering the whole length and all possible points or locations where safety could be jeopardized. Thus, such evaluation implies analyzing each and every one of the conflictive points and all possible chains of events leading to a danger or accident situation.

One of the most important factors to be taken into account is human error, which plays a relevant role in the accident rate level. Many authors have studied this problem in the literature. Among them, we can mention Dhillon (2007); Dhillon (1982); Dhillon (1983); Feldmann et al. (2008); Kumar and Sinha (2008); Spurgin (2009); Massaiu (2009); Kim et al. (2010); Hammerl and Vanderhaegen (2012); De Felice and Petrillo (2011); and Gibson (2012).

Among the most important consequences of human errors (e.g., a train trespassing a signal at red or passing a speed limit) are railway accidents. Thus, a valid model must include human error evaluation.

In the following sections, we build a Markovian–Bayesian model that permits us to evaluate the probability of derailments, collisions, or other types of accidents along the line being analyzed. Markovian models have been frequently used in safety analysis (see Slovak et al., 2007; Fuqua, 2007; Suyama and Kosugi, 2009; Al-Basman and Hu, 2010; Bjorkman, 2011).

The main reason for using Bayesian networks is that there is no limitation in representing any type of variable dependencies. In other words, Bayesian networks permit any set of dependencies among the variables, including common factors, to be reproduced. It is well known that event trees cannot do the same and therefore they suffer from some limitations.

We start by pointing out that the problem is very complex and implies enormous difficulties due to the large amount of factors to be taken into account and the number of parameters the model depends on. With respect to factors, it is necessary to simplify them conveniently to get a comprehensible and useful model; in this respect, it is necessary to consider the relevant variables and ignore those that play a secondary role; in this context, sensitivity analysis is very relevant. Regarding parameter estimation we face first, a problem in the lack of sufficient information to get precise parameter estimates and second, the data are very general, that is, they refer to different trains, infrastructure, drivers, etc.

Based on this idea of a parsimonious and useful model, we have decided to work with a few states and with mean values for the parameters. Therefore, one should pay less attention to the particular values of the accident probabilities and more to their relative values that allow us to determine which are the best solutions and to have an idea of the order of magnitude of improvement they lead to.

3 THE PROPOSED MODEL

In this section and with the aim of evaluating the accident risk, we present a Markovian–Bayesian model that reproduces the process of traveling along the line and facing different risk situations that the driver encounters during the trip. Each one increases the probability of accident, which is a function of the driver's attention state, the traveled length, the danger level, etc. In particular the evolution of the conductor's (driver's) attention is modeled all along the line.

In simple words, the model updates the driver's attention level and accumulates the probabilities of minor, moderate, and serious accidents after traveling a segment without signals or after passing signals or other elements where an erroneous decision can be made or an accident can occur. As it will be shown, this can be done by pre-multiplying the initial probability vector by a series of transition matrices, one per element being considered.

By "Markovian–Bayesian network model" we understand a Bayesian network (whose diagram is shown in Figure 1) formed by adding multiple subnetworks, each one associated with a location or point of the railway line. To complete the definition of the Bayesian network (see Castillo et al., 1997b), tables of conditional probabilities (*children* conditioned to *parents*) need to be incorporated. The model is called Markovian because the probabilities of the states of the variables associated with a certain location depend on the state variables of three previous locations at most (third-order model). The model assumptions are given below.

3.1 Evolution of driver's tiredness with driving time

Because the driver is subject to an increase in time tiredness and this fact is relevant, in our model we propose a simple formula to reproduce the driver's tiredness evolution with time, as follows (see Figure 2):

$$a_t = 1 - \exp\left[-\exp\left(\frac{\lambda - t}{\delta}\right)\right] \qquad (1)$$

where a_t is the attention factor associated with a driving time t that belongs to the interval [0, 1].

For example, if we take $\delta = 2.854$ and $\lambda = 5.358$ we obtain the model shown in Figure 2.

We note that this curve provides the driver's tiredness level in a scale from 0 (minimum attention level) and 1 (maximum attention level) and t must be in driving hours. Its range of application is between 0 and a few hours (e.g., 6 hours), because due to safety reasons the driving time is limited.

We used a Gumbel formula (1) just because it is well known but without any probability justification or relation. In fact, we could use other formulas because the influence of the model being used is very small if similar data are used for the fit.

3.2 Automatic train protection

Due to its relevance, our model also considers the ATP or similar systems (ASFA, an ATP system used in Spain in conventional lines). Because the ATP (ERTMS, LZB, etc.) and other systems can act by correcting any possible driver's errors and stopping the train when necessary to calculate the probabilities of accident, we must take into account, on one hand, the probabilities of the driver's erroneous decisions (human errors), and on the other hand, the probability of failure of these systems, which even though is small is not null.

The ATP system applies brakes to prevent the train trespassing a signal at red or exceeding a speed limit, that is, it corrects the driver's error, no matter it is due to not satisfying signal orders or not reducing speed when required. Thus, this must be taken into consideration in our model.

Let C, $\bar{C}$, S, and $\bar{S}$ be the events driver's correct and incorrect decisions and correct and incorrect ATP actions, respectively. Then, we have the following combinations shown in Table 1, from which only one, which is indicated as accident, is dangerous.

The probability of accident, which occurs when both the driver and the ATP system fail simultaneously, is:

$$P(A) = P(\bar{S}, \bar{C}) = P(\bar{S}|\bar{C})P(\bar{C}) = P(\bar{S})P(\bar{C}), \quad (2)$$

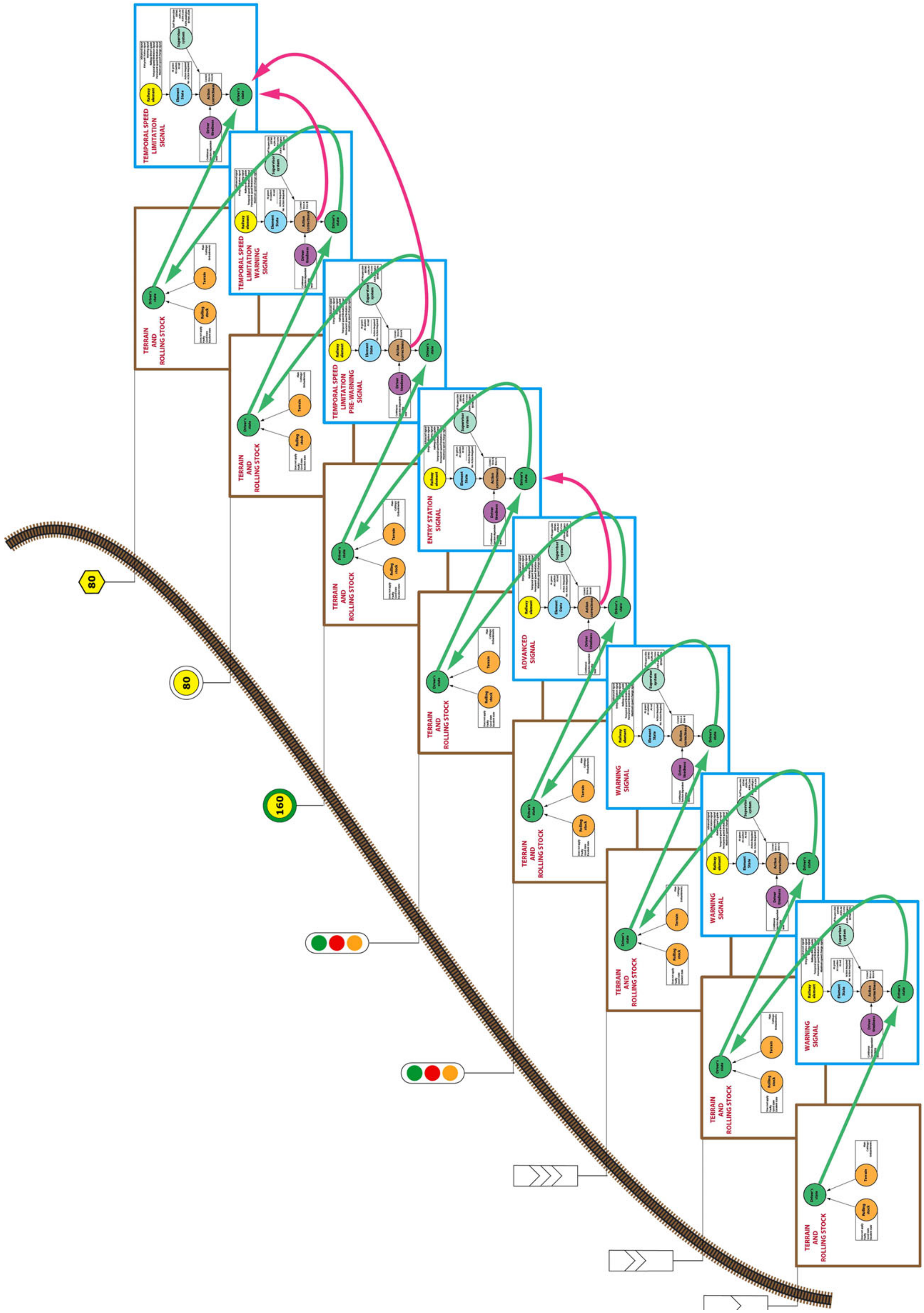

Fig. 1. Proposed Bayesian network. Illustration of the Markovian–Bayesian model showing the Bayesian subnetworks for the segments without signals (left subnetworks) and for the segments with signals or discontinuous associated risk (right subnetworks).

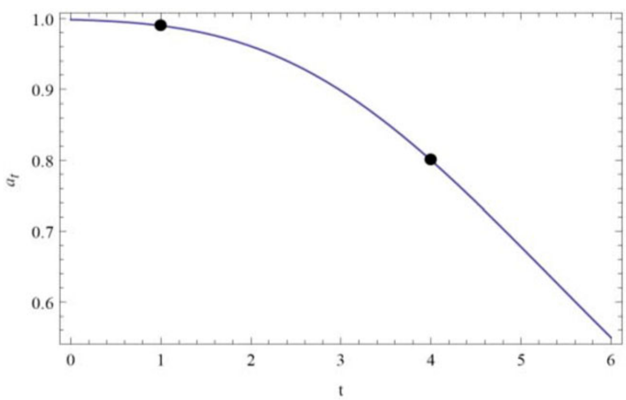

Fig. 2. Illustration of how driver's tiredness a_t evolves with driving time with the proposed model.

Table 1
Consequences from driver's decision: Illustration of the consequences derived from a driver's correct C or erroneous decision $\bar{C}$ and the failure $\bar{S}$ or the correct action S on the automatic train stopping system

	C	$\bar{C}$
S	No action	Necessary stop
$\bar{S}$	Unnecessary stop	Accident

where $p(\bar{S}, \bar{C})$ and $p(\bar{S}|\bar{C})$ are the joint probability of $\bar{S}$ and $\bar{C}$ and the probability of system failure given a driver's incorrect decision, respectively, and $P(A)$ is the probability of accident. Note that $P(\bar{S}|\bar{C}) = P(\bar{S}) = \rho$ because the system and driver's decisions are independent.

This proves that the ATP systems reduce the probabilities of failure with respect to system without supervision by a factor of $\rho = P(\bar{S})$, which has very important practical implications.

3.3 Bayesian subnetwork structure

Finally, in our model there are two types of Bayesian subnetworks:

1. One corresponding to the segments without signals, used to evaluate the risk incurred when driving, due to rolling stock failure, infrastructure state (rails, sleepers, ballast, plate, maintenance standards [see Pen and Ouyang, 2014], etc.) or problems associated with slipping or falling materials in areas of deforestation, landslides in areas of landfill, differential settlement between rails, etc. This subnetwork type considers a Markovian model in continuous time and is shown in Figure 1 to the left of each element, indicated in brown color.
2. The second subnetwork type corresponds to each of the points or locations in which signals are located, decisions subject to errors are to be taken, occasional accidents can occur due to different reasons (step turnouts, entrances and exits of tunnels, sediment accumulation on the track, etc.), viaducts entries and exits. This type of subnetwork is shown in Figure 1 to the right of each element, indicated in blue.

The Bayesian network permits us multiple possibilities, as certain variables can be assumed to be known and other variable probabilities to be determined. However, in this work we are interested only in knowing how the driver's attention and the accident probabilities evolve as the train travels along the line. Therefore, we are interested only in the marginal probabilities of the variables "driver's state-accident" corresponding to each of the points along the way.

When marginalizing, we observe that the marginal of the "driver's state-accident" variable at a given location is the product of the marginal probabilities of the same variable in a previous location, pre-multiplied by a transition matrix. Reiterating the procedure, it is concluded that these probabilities can be obtained by multiplying a series of transition matrices, one per element, by the column matrix of the probabilities of the "driver's state-accident" at the initial location.

In summary, the model includes a continuous Markov model per segment without signals, whose parameters depend on the train and segment characteristics (rolling stock state, tracks, ties, cuttings, embankments, etc.) and a Bayesian network per each point where driver's attention is improved (warning signals, acoustic indications, etc.), some concentrated risks exist or some decision subject to error occur (e.g., signals). All these elements are sorted in the line start to arrival direction and consecutive elements are always connected to exchange the required information. Some especial elements are connected to one or more previous elements because they need the associated information (about variable dependencies). Thus, the Markovian–Bayesian model implies at most four different elements, the current one and at most three previous elements.

With the aim of homogenization, we have designed a general Bayesian subnetwork whose acyclic graph is shown in Figure 3, where we can see the different variables involved in the railway problem and the dependence structure of all of them.

In this Bayesian subnetwork, we have considered the following variables:

1. *Element affecting safety.* This variable can take several values corresponding to each of the existing elements associated with the different points

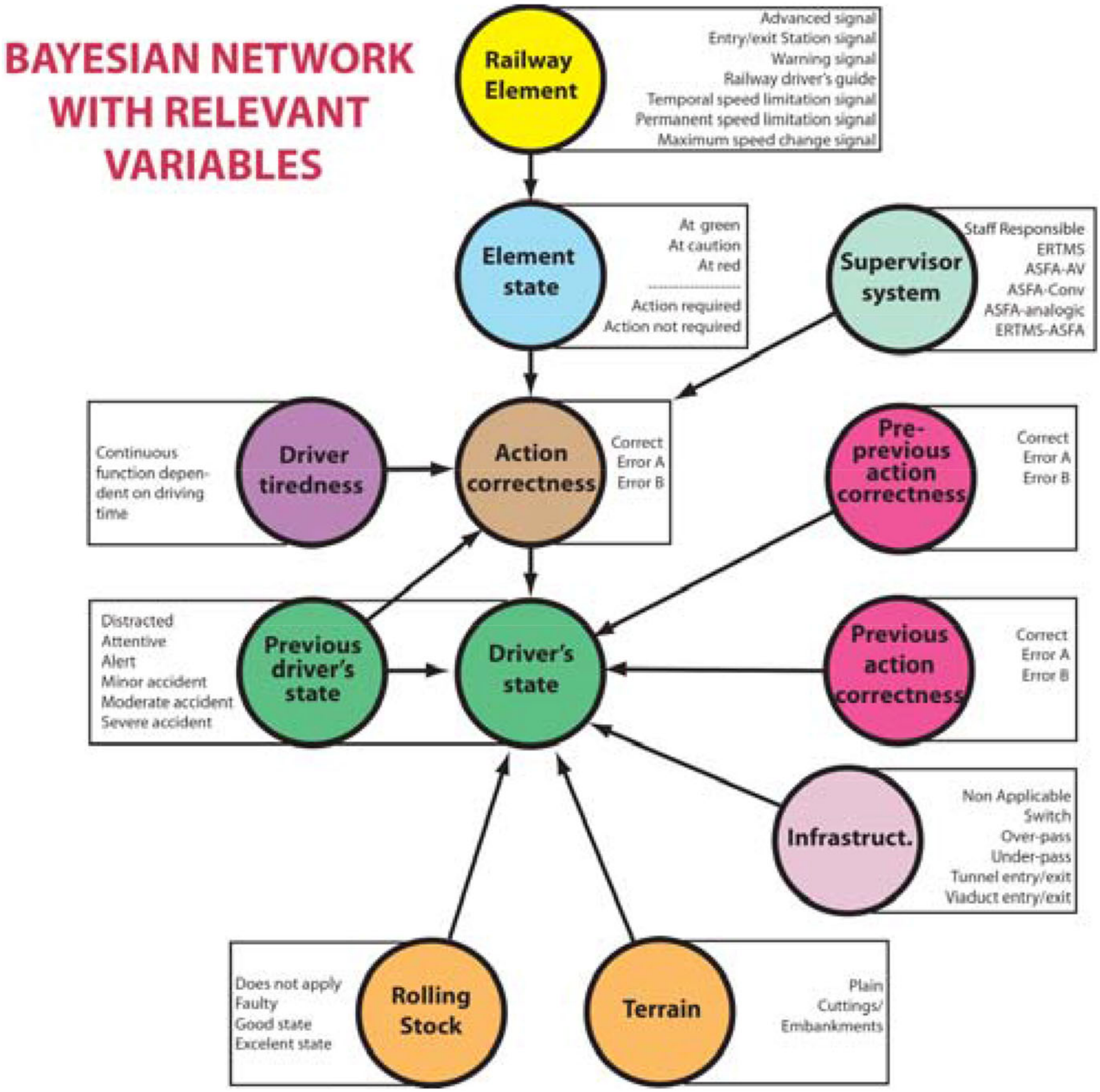

Fig. 3. Unified Bayesian network acyclic graph illustrating the dependence conditional relations of the different variables (elements) involved in the problem.

considered along the railway line and where the safety can be jeopardized. In particular, they correspond to advanced signals, entry/exit signals, warning signals, temporal or permanent speed limitation signals, maximum speed change signals, etc. The railway driver's guide is also considered at the points where an action subject to possible error must be taken.

2. *Element state.* This variable corresponds to the different states allowed for the considered element. For example, an advanced signal can be "at green," "at green-yellow" (stop-ahead announcement) or "at red" (stop), a speed limitation signal can require an immediate action (reduce speed) and a warning signal does not require any action.

3. *Action correctness.* When the element implies an action we need to consider the cases of correct action and all possible erroneous alternatives (speed reduction error, stop error, etc.). Because the action correctness depends on the element state, the tiredness of the driver, the driver's attention level, and the existence of a supervising system, this node is connected to all of them.
4. *ATP system.* This variable refers to the supervising or driving assistance system operating at the element. It takes the values: staff responsible, ERTMS, ASFA-AV, ASFA-conv, analogic-ASFA, ERTMS-ASFA, etc.
5. *Previous and pre-previous action correctness.* Because some elements are related, as, for example, the speed limitation signals, which are normally installed in groups of three signals (pre-announce, announce, and speed limitation), we need to know the chain of possible errors made at all the three signals to determine the associated risks. Thus, we must know what they are. Consequently, we need to include graph links in the Bayesian subnetwork to the corresponding variables in previous Bayesian subnetworks. Obviously, the values taken by these variables are the same as they were in their previous versions.
6. *Driver's state.* This variable takes the six following values: distracted, attentive, alert, minor accident, moderate accident, and severe accident (see Figure 4 where the possible transitions among different states are shown by arrows). In fact, this variable tries to reflect the fact that the driver can be in two situations: normal driving or accident, but we have divided each of them into three possible alternatives. We also consider that once the accident situation is reached, the driver remains there (the three accident states are considered absorbing barriers), that is, that as soon as one of these states is reached they are never abandoned. In other words, an accident implies the end of the trip. Because the state of this variable depends on the state of this variable in the previous subnetwork, there will be a link joining them. In addition, because this variable depends on the ATP system, on the correctnesses of previous decisions, on the infrastructure, the terrain and the rolling stock state, this node is connected to all of them.

By *distracted* we understand a situation in which the driver lacks the necessary attention to correctly react when an action is required. By *attentive* we refer to the case in which the driver is able to react adequately to the required actions with a small probability of error. Finally, *alert* refers to the case where the driver is ready to take an action and knows that he/she has to act immediately (e.g., after seeing a warning signal or consulting the railway driver's guide, etc.). The practical difference between attentive and alert is that the probabilities of a correct decision or action in the case of alert are greater than those for the case of attentive.

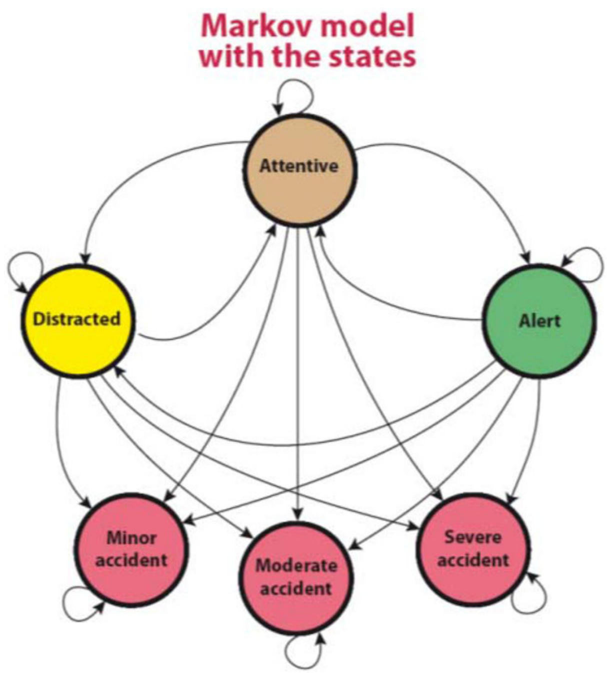

Fig. 4. Illustration of the Markov model with its six states: distracted, attentive, alert, minor accident, moderate accident, and severe accident and their connections.

In summary, our model, which is time continuous but discrete in other variables, considers that the driver is in one of the following six states: circulating under the attention levels: distracted, attentive, and alert; and in a minor, moderate, or severe accident situation.

7. *Driver's tiredness.* This variable is assumed deterministic and takes a fixed value at each location depending on the driving time, and is calculated by using the model already described.
8. *Rolling stock.* This variable takes the values: faulty, good state, and excellent. They indicate the assumed three levels of rolling stock condition.
9. *Terrain.* This variable takes values: plain, cutting, or embankment. They are used to consider the risk associated with falling stones on the infrastructure or slope slidings.
10. *Infrastructure.* With this variable we consider the infrastructure state (rails, sleepers, ballast, plate, maintenance standards, etc.) and the risks associated with passing throughout switches, over and under-passes, and entries and exits to tunnels

or viaducts, where some sudden changes in the infrastructure stiffness or accumulation of deposits can occur.

This acyclic graph defines the dependence structure of the variables involved in the Bayesian network and permits conclusions to be drawn on conditional independencies of the variables. In particular, we can know whether or not a set of certain variables contributes new information on another set of variables when the information on a third set of given variables is known or they simply report redundant information.

For example, the driver's attention is determined by his/her previous state and the level of tiredness. Similarly, the probabilities of the different types of accidents (minor, moderate, and severe) are determined by the driver's attention, his/her tiredness level, the correctness of previous actions, the supervising system (ERTMS, ASFA, etc.), the infrastructure state, and the rolling stock condition.

We note that the Bayesian network includes all dependencies among the variables. In particular the common causes are considered. We also consider that an improvement or deterioration of the driver's attention is common to all decisions.

As indicated, this Bayesian network permits to model all studied elements, but needs to be particularized for each of them. In Figure 5, as some examples, we show from left to right and top to bottom the cases of warning, advanced, entry station, speed limitation signals, railway driver's guide, maximum speed change, infrastructure, and terrain signals. Note that the circles representing the variables having no sense in each case have been faded.

To complete the Bayesian network it is necessary to add the conditional probability tables of the nodes conditioned by their parents (see Arnold et al., 1999 or Arnold et al., 2001). Later we explain how these tables can be given and what are the corresponding selected parameters and their physical meaning.

4 DETAILED DESCRIPTION OF SOME BAYESIAN SUBNETWORKS

In this section, we describe the different Bayesian subnetworks and the conditional probability tables associated with them.

The "driver's state-accident" is the main variable we are interested in. Thus, this variable appears in all subnetworks. On the one hand, we assume that signals, external agents, etc. produce a random attention improvement on the driver, which can be reproduced by our Markov model (see Kijima, 1997; Doob, 1953; or Benjamin and Cornell, 1970), that is to say, we assume that the driver's attention level at a given moment depends only on the driver's attention level at a previous moment and the received information (from signals, acoustic warnings, lighted icons, etc.) though corrected by the tiredness factor a_t, explained before. Note that the factor a_t being smaller than one must be used as a multiplying factor and cannot be used as a denominator to increase a failure probability because it can lead to values larger than one, that is, to an inconsistent model (see Castillo et al., 2014a). On the other hand, some signals, depending on their state, require a given action from the driver, which, in case of being ignored, lead to a hazard or risk situation and possibly to an accident.

4.1 Segment without signals

In this section, a model analyzing how the driver's attention and the probabilities of minor, moderate, and severe accidents evolve with time when the train circulates in segments without signals is analyzed. In this case, the driver does not make any decisions subject to error, but derailments or accidents can occur due to failures in the rolling stock, the tracks, slope slidings in cuttings or embankments, or other events jeopardizing safety. Given the special character of these events, we can assume a given failure rate per unit length or per unit time (they are related by a speed factor). This rate must include all the above-mentioned risk factors and will depend on the characteristics of the particular segment being analyzed and on maintenance quality.

We must note that any change in the probabilities of the different types of accidents, minor, moderate, or severe, will produce a change in the probabilities of the different attention states of the driver, distracted, attentive, and alert, because if the driver is in one of the three attention states, this implies that no accident has occurred. More precisely, the sum of the probabilities of all six states must be one, or, in other words, the sum of the probabilities of the attention states is the probability of no accident up to the position being considered.

To reproduce driver and train behavior in a segment without signals, we can use a discrete or continuous Markov process (see Kijima, 1997; Doob, 1953; or Benjamin and Cornell, 1970). In the following section, we consider only the continuous case, because it seems to be more appropriate.

In this case, we have the differential equation associated with a standard Markov mode:

$$\begin{pmatrix} p_0^{'}(a_{t^*}, t - t_0) \\ p_1^{'}(a_{t^*}, t - t_0) \\ p_2^{'}(a_{t^*}, t - t_0) \\ p_{A_1}^{'}(a_{t^*}, t - t_0) \\ p_{A_2}^{'}(a_{t^*}, t - t_0) \\ p'_{A_3}(a_{t^*}, t - t_0) \end{pmatrix} = T(a_{t^*}) \begin{pmatrix} p_0(a_{t^*}, t - t_0) \\ p_1(a_{t^*}, t - t_0) \\ p_2(a_{t^*}, t - t_0) \\ p_{A_1}(a_{t^*}, t - t_0) \\ \mathrm{p}_{A_2}(a_{t^*}, t - t_0) \\ p_{A_3}(a_{t^*}, t - t_0) \end{pmatrix} \quad (3)$$

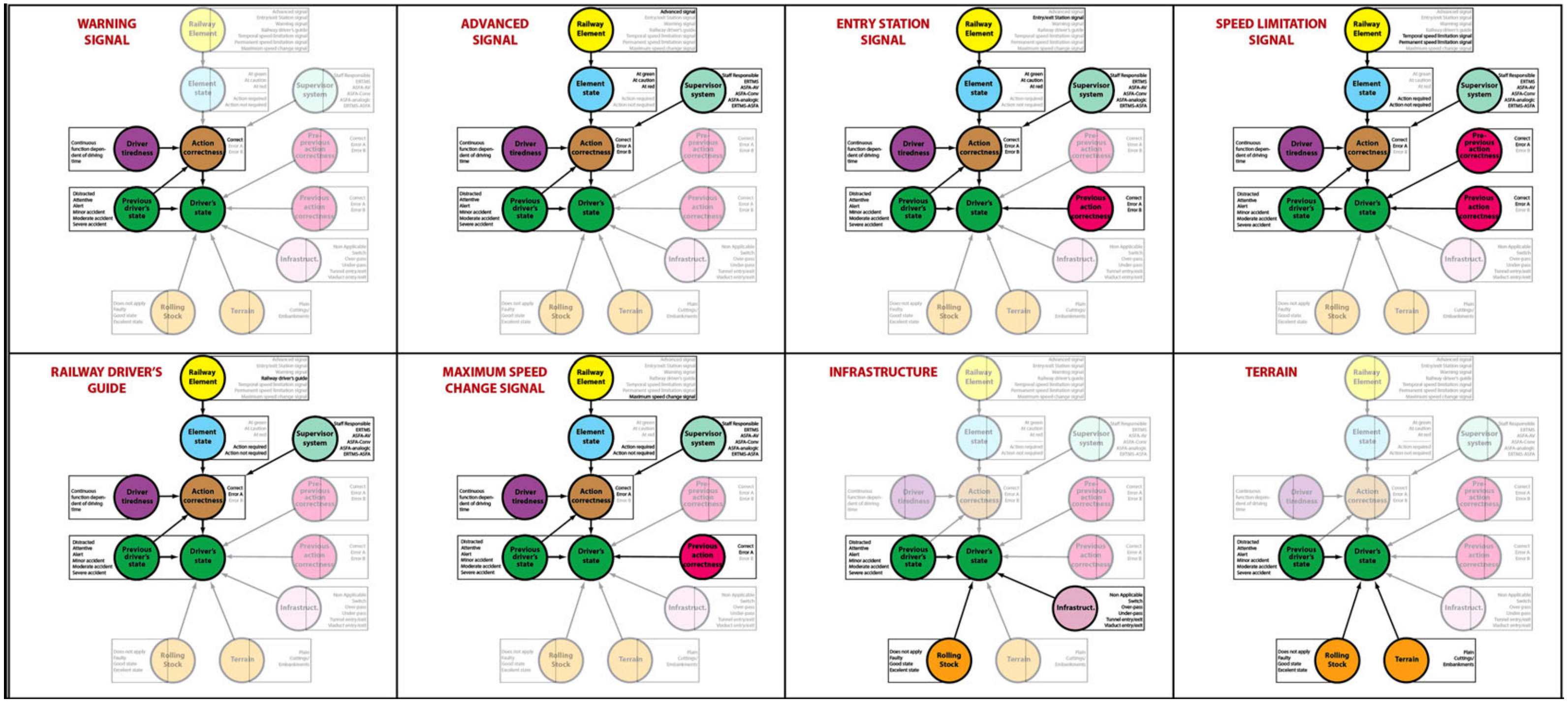

Fig. 5. From left to right and top to bottom the Bayesian subnetwork graphs corresponding to: warning signal, advanced signal, entry station signal, speed limitation signal, railway driver's guide, maximum speed change signal, infrastructure, and terrain. The circles representing the variables having no sense in each case have been faded.

$$T(a_{t^*}) = \begin{pmatrix} -\eta a_{t^*} - \psi & \frac{\gamma_1}{a_{t^*}} & \frac{\gamma_2}{a_{t^*}} & 0 & 0 & 0 \\ \eta a_{t^*} & -\frac{\gamma_1}{a_{t^*}} - \psi & \gamma_3 a_{t^*} & 0 & 0 & 0 \\ 0 & 0 & -\frac{\gamma_2+\gamma_3 a_{t^*}^2}{a_{t^*}} - \psi & 0 & 0 & 0 \\ \psi_1 & \psi_1 & \psi_1 & 0 & 0 & 0 \\ \psi_2 & \psi_2 & \psi_2 & 0 & 0 & 0 \\ \psi_3 & \psi_3 & \psi_3 & 0 & 0 & 0 \end{pmatrix}$$

where t, t_0, and t^* are a given time, the segment starting time, and the mean segment time, respectively, and ηa_{t^*} is the time rate of recovering attention when the driver is distracted after a time t^* from the beginning of the trip, $\psi = \psi_1 + \psi_2 + \psi_3$ is the accident time rate due to technical failure, infrastructure, or terrain in segments without signals, ψ_1, ψ_2, and ψ_3 are the minor, moderate, and severe accident associated time rates, respectively, $\gamma_i/a_{t^*}; i = 1, 2$ are the time rates of becoming distracted when being attentive and alert, respectively, and $\gamma_3 a_{t^*}$ is the time rate of becoming attentive when the driver is alert, which leads to the model

$$\begin{pmatrix} p_0(a_{t^*}, t - t_0) \\ p_1(a_{t^*}, t - t_0) \\ p_2(a_{t^*}, t - t_0) \\ p_{A_1}(a_{t^*}, t - t_0) \\ \mathrm{p}_{A_2}(a_{t^*}, t - t_0) \\ p_{A_3}(a_{t^*}, t - t_0) \end{pmatrix} = M_\ell(a_{t^*}, t - t_0; \eta, \gamma, \psi) \begin{pmatrix} p_0^0 \\ p_1^0 \\ p_2^0 \\ p_{A_1}^0 \\ p_{A_2}^0 \\ p_{A_3}^0 \end{pmatrix} \quad (4)$$

Formula (4) permits us to calculate how the probabilities of each of the six states evolve with time $t - t_0$ and, in particular, how the probabilities of the different accident types increase with travel length or time.

4.2 Warning signals

In this section, we analyze how seeing warning signals modify the driver's attention. We assume that a warning signal produces an improvement of the driver attention, which can be modeled by our Markov model and that it does not modify the probabilities of minor, moderate, or severe accidents (see the top-left Figure 5). Consequently, these warning signals produce a re-adjustment of the probabilities of the driver's attention states in the sense of improving them probabilistically (a probability transfer is made to better attention states), but they do not modify the probabilities of the different accident types.

If p_0, p_1, p_2, p_{A_1}, p_{A_2}, and p_{A_3} are the probabilities associated with the six states (distracted, attentive and alert and the three accident types) before seeing the signal, and p_0^*, p_1^*, p_2^*, $p_{A_1}^*$, $p_{A_2}^*$, and $p_{A_3}^*$ are the same probabilities after seeing and trespassing it, the last probabilities can be calculated by means of the following transition matrix equation (see Figure 4):

$$\begin{pmatrix} p_0^* \\ p_1^* \\ p_2^* \\ p_{A_1}^* \\ p_{A_2}^* \\ p_{A_3}^* \end{pmatrix} = \begin{pmatrix} 1 - \lambda a_t & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 - (1-\varepsilon)a_t & 0 & 0 & 0 & 0 \\ \lambda a_t & (1-\varepsilon)a_t & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \\ p_2 \\ p_{A_1} \\ \mathrm{p}_{A_2} \\ p_{A_3} \end{pmatrix} \quad (5)$$

where $0 \le \lambda \le 1$ is the probability of recovering attention when seeing the signal if the driver is distracted and $0 \le \varepsilon \le 1$ is the probability of the driver being unaware of the signal presence when he/she circulates under an attentive attention level. Note that seeing these signals never produces an accident and that the reaction probabilities have been reduced using an attention factor a_t.

The probability ε is assumed very small. However, the value of λ is much higher than ε, that is, $\lambda >> \varepsilon$.

Equation (5) permits updating the probabilities of being in each of the six states when passing a warning signal. Given the transition matrix structure, it is clear that this always produces a statistical improvement of the driver's attention and never an accident.

4.3 Advanced signal

The case of an advanced signal is illustrated in the second place of the upper row of Figure 5, where the circles representing the variables having no sense have been faded.

We assume that when seeing an advanced signal an improvement of the driver's attention takes place. If the signal is "at green," the driver does not have to take any action, if it is at "green-yellow" condition, the driver must reduce speed to be ready to stop at the next signal (otherwise he/she will make a speed reduction error), and if it is "at red" the driver must stop before the signal (otherwise he/she will make a stop error). Consequently, the driver must adequately obey the signal orders, that is, he/she is subject to the possibility of making an error. However, in case of making a speed reduction error, no accident will occur in the following segment because the signal guarantees that the segment is free. Contrary, in the case of a stop error, an accident can occur in the next segment. Consequently, we need to calculate the probabilities of the different errors and store them to evaluate the risks when the entry signal is surpassed and to evaluate the accident probabilities in the following segment.

The conditional probabilities defining the Bayesian subnetwork probability tables in the case of an advanced signal are:

1. The nodes "element state," "supervision system," and "driver's tiredness" the variables have no parents, so that the conditional probabilities become

marginal probabilities and due to the fact that they take a unique value these probabilities become unity.

2. For the node "driver's state-accident," the marginal probabilities are those in the previous Bayesian network, that is, p_0, p_1, p_2, p_{A_1}, p_{A_2}, p_{A_3}.
3. For the node "element state" the conditional probabilities to the unique state are q_g, q_{ap} and $q_p = 1 - q_g - q_{ap}$, where q_g, q_{ap}, and q_p represent the probabilities of a signal to be "at green," "at green-yellow," or "at red," respectively.
4. The probabilities of node "action correctness" conditioned to the previous driver's state, to the element state, the driver tiredness and the ATP system are those given in Table 2. Note that after the accident has occurred we have assumed that we are in an absorbing barrier.
5. The conditional probabilities of the node "driver's state-accident" conditioned to the "previous driver's state-accident," "action correctness," and "ATP system" (it takes a unique value) are those in Table 3, where α_1 is the probability of no accident when a red signal has been improperly surpassed and α_2, α_3, and $\alpha_4 = 1 - \alpha_1 - \alpha_2 - \alpha_3$ are the probabilities of a minor, moderate, and severe accident, when the train trespasses a signal "at red," respectively. We note that the values of this table depend on the ATP system through the factor ρ.

After considering the above conditional probabilities and marginalizing with respect to the driver's state node, we obtain the transition matrix $N_{av}(a_t, \alpha_1, \alpha_2, \alpha_3, q_g, q_{ap}, \theta_s, \tau_s, \rho)$ for this case of advanced signal (see Equation (6)), and the transition matrix in Equation (7) to obtain the marginal of the node "action correctness" where $q_p = 1 - q_g - q_{ap}$ and $p_{E_2} = 1 - p_C - p_{E_1}$ and P_C, P_{E_1}, p_{E_2} are the marginal probabilities of the node "action correctness," that is, the probabilities of making a correct decision and errors A and B, respectively.

4.4 Entry signal

At the entry signals, in addition to improving the driver's attention when seeing the signal, the driver must stop the train if the signal is at red or reduce the speed in case of a "stop-ahead" warning situation. Thus, the driver is subject to making an erroneous decision on the one hand and to being unable to obey the signal order, on the other hand, because of the non-fulfillment of the order of a previous advanced signal. This implies that the probabilities of the driver's attention and of the different types of accidents must be changed with consideration of what happened at this and at the previous one.

The conditional probabilities that define this Bayesian network, which is shown in the upper row of Figure 5, are the following:

$$\begin{pmatrix} p_C \\ p_{E_1} \\ p_{E_2} \end{pmatrix} = \begin{pmatrix} 1-(1-\alpha_1)\rho(a_t(\tau-1)+1)(1-q_{ap}-q_g) & 0 & 0 & 0 & 0 & 0 \\ 0 & 1+\dfrac{(\alpha_1-1)\rho\theta(1-q_{ap}-q_g)}{a_t} & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ \alpha_2\rho(a_t(\tau-1)+1)(1-q_{ap}-q_g) & \dfrac{\alpha_2\rho\theta(1-q_{ap}-q_g)}{a_t} & 0 & 1 & 0 & 0 \\ \alpha_3\rho(a_t(\tau-1)+1)(1-q_{ap}-q_g) & \dfrac{\alpha_3\rho\theta(1-q_{ap}-q_g)}{a_t} & 0 & 0 & 1 & 0 \\ \rho(a_t(\tau-1)+1)(1-q_{ap}-q_g)(1-\alpha_1-\alpha_2-\alpha_3) & \dfrac{\rho\theta(1-q_{ap}-q_g)(1-\alpha_1-\alpha_2-\alpha_3)}{a_t} & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} p_0^* \\ p_1^* \\ p_2^* \\ p_{A_1}^* \\ p_{A_2}^* \\ p_{A_3}^* \end{pmatrix} \tag{6}$$

$$\begin{pmatrix} p_C \\ p_{E_1} \\ p_{E_2} \end{pmatrix} = \begin{pmatrix} (q_g-1)\rho(a_t(\tau-1)+1)+1 & \dfrac{a_t+(q_g-1)\rho\theta}{a_t} & 1 & 1 & 1 & 1 \\ q_{ap}\rho(a_t(\tau-1)+1) & \dfrac{q_{ap}\rho\theta}{a_t} & 0 & 0 & 0 & 0 \\ \rho(a_t(\tau-1)+1)(1-q_{ap}-q_g) & \dfrac{\rho\theta(1-q_{ap}-q_g)}{a_t} & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} p_0^* \\ p_1^* \\ p_2^* \\ p_{A_1}^* \\ p_{A_2}^* \\ p_{A_3}^* \end{pmatrix} \tag{7}$$

Table 2
Conditional probabilities associated with advanced, entry, and exit signals: conditional probabilities $\Pr(A|B, C, D, E)$ where A = action correctness, B = previous driver's state, C = element state, D = driver's tiredness, and E = ATP system, where the last two take a single value, speed reduction error means failing to reduce speed when the signal is "at green-yellow," and stop error means failing to stop when the signal is "at red"

		A		
B	*C*	*Correct*	*Speed reduction error* $\Pr(A\|B, C, D, E)$	*Stop error*
Distracted	*g*	1	0	0
	ap	$1-\rho\,(1-(1-\tau)\,a_t)$	$\rho\,(1-(1-\tau)\,a_t)$	0
	p	$1-\rho\,(1-(1-\tau)\,a_t)$	0	$\rho\,(1-(1-\tau)\,a_t)$
Attentive	*g*	1	0	0
	ap	$1-\theta\rho/a_t$	$\theta\rho/a_t$	0
	p	$1-\theta\rho/a_t$	0	$\theta\rho/a_t$
Alert	*g*	1	0	0
	ap	1	0	0
	p	1	0	0
Minor	*g*	1	0	0
	ap	1	0	0
	p	1	0	0
Moderate	*g*	1	0	0
	ap	1	0	0
	p	1	0	0
Severe	*g*	1	0	0
	ap	1	0	0
	p	1	0	0

Table 3
Conditional probabilities associated with an advanced signal: conditional probabilities $\Pr(A|B, C, D)$ where A = driver's state, B = previous driver's state, C = action correctness, and D = ATP system (takes a single value)

		A					
		Distracted	*Attentive*	*Alert*	*Minor*	*Moderate*	*Severe*
B	*C*	$\Pr(A\|B, C, D)$					
Distracted	Correct	1	0	0	0	0	0
	Speed reduction error	1	0	0	0	0	0
	Stop error	α_1	0	0	α_2	α_3	α_4
Attentive	Correct	0	1	0	0	0	0
	Speed reduction error	0	1	0	0	0	0
	Stop error	0	α_1	0	α_2	α_3	α_4
Alert	Correct	0	0	1	0	0	0
	Speed reduction error	0	0	1	0	0	0
	Stop error	0	0	α_1	α_2	α_3	α_4
Minor	Correct	0	0	0	1	0	0
	Speed reduction error	0	0	0	1	0	0
	Stop error	0	0	0	1	0	0
Moderate	Correct	0	0	0	0	1	0
	Speed reduction error	0	0	0	0	1	0
	Stop error	0	0	0	0	1	0
Severe	Correct	0	0	0	0	0	1
	Speed reduction error	0	0	0	0	0	1
	Stop error	0	0	0	0	0	1

1. For the nodes "element state," "ATP system," and "driver's tiredness" because the variables have no parents, they take a unique value and then the conditional probability becomes its marginal probability, that is, unity.
2. For the node "driver's state-accident," the marginal probabilities are those in the previous Bayesian network, that is, p_0, p_1, p_2, p_{A_1}, p_{A_2}, and p_{A_3}.
3. For the node "element state": q_g, q_{ap}, and $q_p = 1 - q_g - q_{ap}$, where q_g, q_{ap}, and q_p are the probabilities of the signal being in states "at green," "at green-yellow," and "at red," respectively.
4. The probabilities of node "action correctness" conditioned to the nodes "driver's state-accident," "element state," "driver's tiredness," and "ATP system" are those in Table 2.
5. The probabilities of the node "driver's state-accident" conditioned to the nodes "driver's state-accident," "action correctness," "previous action correctness" and "ATP system," that takes a unique value, are given in Table 4, that is, the conditional probabilities $\Pr(A|B, C, D)$ where A = driver's state, B = previous driver's state, C = previous action correctness, D = action correctness, and E = ATP system. Variables C and D take values 0, 1, and 2, that correspond to "Correct," "Speed reduction error" (Error A), and "stop error" (Error B), respectively.

The subindices 1, 2, 3, and 4 of parameters $\alpha, \beta, \sigma, \delta, \mu$, and ν refer to the probabilities of no accident and minor, moderate, and severe accident, respectively, and correspond to the cases of ST error-ST error or SP error-ST error, correct-ST error, ST error-SP error or SP error-SP error, correct-SP error, ST error-correct and SP error-correct, respectively, where SP and ST are used for speed reduction and stop errors, respectively.

The seriousness of the different combinations is reflected in the following sorting of the probability values:

$$\alpha_1 < \mu_1 < \beta_1 < \sigma_1 < \nu_1 < \delta_1 \tag{8}$$

Marginalizing the Bayesian network for the node "driver's state-accident," we obtain the corresponding transition matrix, which is too complex to be detailed here:

$$N_e(a_t, q_g, q_{ap}, \theta_s, \tau_s, \alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3, \sigma_1, \sigma_2, \sigma_3, \delta_1,$$
$$\delta_2, \mu_1, \mu_2, \mu_3, \nu_1, \nu_2, \nu_3, p_C, p_{E_1}, \rho).$$

4.5 Speed limit signal

The speed limit signals are generally located in Spain in groups or three signals: pre-announcement, with a value of 160 km/h, announcement, whose limit value corresponds to the final limit, and the forced limitation signal where the train must satisfy the limitation. There are permanent and temporal speed limitation signals that receive different treatment by the ATP systems, that is, some ATP systems do not cover permanent speed limitation signals.

The pre-announcement speed limitation signal improves the driver attention when it is seen and requires a speed reduction to the indicated value before reaching the following signal. Consequently, if the actual speed is higher than the speed limit the driver is subject to a possible error (not reducing the speed). However, in this case no accident will occur between the two signals, because we assume that the driving is safe at this speed before the final signal. This means that we need to modify the probabilities of the driver's attention, calculate the error probabilities, and store them to be used later. Thus, the accident probabilities do not suffer change at this stage.

Similarly, the speed limit announcement signal improves the driver attention too and requires a speed reduction to the indicated value before reaching the final speed limit signal. If there is no maximum speed change, the probabilities of accident remain the same because no accident occurs here. Consequently, the same driver's attention probability updating with no change in the accident probabilities applies.

Finally, the final speed limit signal also improves the driver attention and requires satisfying the speed limit condition after trespassing it. Failing to do this can lead to an accident. This implies modifying not only the driver's attention but the accident probabilities too, but taking into consideration the previous error probabilities already stored.

The "action correctness" associated with the pre-announcement and announcement speed limit respond to the following relation that can be obtained by marginalizing the probabilities of the Bayesian network for the node "action correctness" corresponding to the speed limit pre-announce and announce signals:

$$\begin{pmatrix} p_C \\ p_E \end{pmatrix} = \begin{pmatrix} \rho\,(a_t\,(-\tau) + a_t - 1) + 1 & 1 - \frac{\rho\theta}{a_t} & 1 & 1 & 1 & 1 \\ \rho\,(a_t\,(\tau - 1) + 1) & \frac{\rho\theta}{a_t} & 0 & 0 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} p_0 \\ p_1 \\ p_2 \\ p_{A_1} \\ p_{A_2} \\ p_{A_3} \end{pmatrix} \tag{9}$$

Table 4
Conditional probabilities associated with an entry signal: conditional probabilities $\Pr(A|B, C, D)$ where A = driver's state, B = previous driver's state, C = previous action correctness, D = action correctness, and E = ATP system. Variables C and D take values 0, 1, and 2 that correspond to "Correct," "Error A," and "Error B," respectively

		C, D								
		00	*10*	*20*	*01*	*11*	*21*	*02*	*12*	*22*
A	B	$\Pr(A\|B, C, D, E)$								
Distracted	Distracted	1	ν_1	μ_1	δ_1	σ_1	σ_1	β_1	α_1	α_1
	Attentive	0	0	0	0	0	0	0	0	0
	Alert	0	0	0	0	0	0	0	0	0
	Minor	0	0	0	0	0	0	0	0	0
	Moderate	0	0	0	0	0	0	0	0	0
	Severe	0	0	0	0	0	0	0	0	0
Attentive	Distracted	0	0	0	0	0	0	0	0	0
	Attentive	1	ν_1	μ_1	δ_1	σ_1	σ_1	β_1	α_1	α_1
	Alert	0	0	0	0	0	0	0	0	0
	Minor	0	0	0	0	0	0	0	0	0
	Moderate	0	0	0	0	0	0	0	0	0
	Severe	0	0	0	0	0	0	0	0	0
Alert	Distracted	0	0	0	0	0	0	0	0	0
	Attentive	0	0	0	0	0	0	0	0	0
	Alert	1	ν_1	μ_1	δ_1	σ_1	σ_1	β_1	α_1	α_1
	Minor	0	0	0	0	0	0	0	0	0
	Moderate	0	0	0	0	0	0	0	0	0
	Severe	0	0	0	0	0	0	0	0	0
Minor	Distracted	0	ν_2	μ_2	δ_2	σ_2	σ_2	β_2	α_2	α_2
	Attentive	0	ν_2	μ_2	δ_2	σ_2	σ_2	β_2	α_2	α_2
	Alert	0	ν_2	μ_2	δ_2	σ_2	σ_2	β_2	α_2	α_2
	Minor	1	1	1	1	1	1	1	1	1
	Moderate	0	0	0	0	0	0	0	0	0
	Severe	0	0	0	0	0	0	0	0	0
Moderate	Distracted	0	ν_3	μ_3	$1-\delta_1-\delta_2$	σ_3	σ_3	β_3	α_3	α_3
	Attentive	0	ν_3	μ_3	$1-\delta_1-\delta_2$	σ_3	σ_3	β_3	α_3	α_3
	Alert	0	ν_3	μ_3	$1-\delta_1-\delta_2$	σ_3	σ_3	β_3	α_3	α_3
	Minor	0	0	0	0	0	0	0	0	0
	Moderate	1	1	1	1	1	1	1	1	1
	Severe	0	0	0	0	0	0	0	0	0
Severe	Distracted	0	$1-\nu_1-\nu_2-\nu_3$	$1-\mu_1-\mu_2-\mu_3$	0	$1-\sigma_1-\sigma_2-\sigma_3$	$1-\sigma_1-\sigma_2-\sigma_3$	$1-\beta_1-\beta_2-\beta_3$	$1-\alpha_1-\alpha_2-\alpha_3$	$1-\alpha_1-\alpha_2-\alpha_3$
	Attentive	0	$1-\nu_1-\nu_2-\nu_3$	$1-\mu_1-\mu_2-\mu_3$	0	$1-\sigma_1-\sigma_2-\sigma_3$	$1-\sigma_1-\sigma_2-\sigma_3$	$1-\beta_1-\beta_2-\beta_3$	$1-\alpha_1-\alpha_2-\alpha_3$	$1-\alpha_1-\alpha_2-\alpha_3$
	Alert	0	$1-\nu_1-\nu_2-\nu_3$	$1-\mu_1-\mu_2-\mu_3$	0	$1-\sigma_1-\sigma_2-\sigma_3$	$1-\sigma_1-\sigma_2-\sigma_3$	$1-\beta_1-\beta_2-\beta_3$	$1-\alpha_1-\alpha_2-\alpha_3$	$1-\alpha_1-\alpha_2-\alpha_3$
	Minor	0	0	0	0	0	0	0	0	0
	Moderate	0	0	0	0	0	0	0	0	0
	Severe	1	1	1	1	1	1	1	1	1

Table 5
Conditional probabilities of the pre-announcement, railway driver's guide or speed limit signals: conditional probabilities $\Pr(A|B, C)$ where A = action correctness, B = previous driver's state, C = ATP system, where the last takes only one value. The error consists of failing to reduce speed to 160 km/h or to the indicated value

	A	
B	*Correct* $\Pr(A\|B, C)$	*Error*
Distracted	$1 - \rho\,(1 - (1 - \tau)\,a_t)$	$\rho\,(1 - (1 - \tau)\,a_t)$
Attentive	$1 - \theta\rho/a_t$	$\theta\rho/a_t$
Alert	1	0
Minor	1	0
Moderate	1	0
Severe	1	0

The conditional probabilities of the Bayesian network shown in the right of upper row of Figure 5 are the following:

1. For the nodes "element state," "ATP system" and "driver's tiredness" the variables have no parents and take a unique value, that is, the conditional are their marginals and take value one.
2. For the node "driver's state," $p_0, p_1, p_2, p_{A_1}, p_{A_2}$, and p_{A_3}.
3. The probabilities of node "action correctness" conditioned to the "driver's state," "element state," "driver's tiredness," and "ATP system" are those in Table 5.
4. The probabilities of node "driver's state-accident" conditioned to the "driver's state-accident," "pre-previous action correctness," "previous action correctness," and "action correctness" are those in Table 6, that is, the conditional probabilities $\Pr(A|B, C, D, E)$ where A = driver's state, B = previous driver's state, C = Pre-previous action correctness, D = previous action correctness, E = action correctness. Variables C, D, and E take the values 0 and 1 that correspond to "Correct" and "Error," respectively.

Marginalizing we obtain the following transition matrix $N_{lv}\,(a_t, \theta_v, \tau_v, \pi_1, \pi_2, \pi_3, \pi_4, \pi_5, p_{C_1}, p_{C_2}, \rho)$ which is too complex to be included here. We note that in this matrix we automatically get the contribution of all possible combinations of hazardous events to the probability of accident.

4.6 Switch passes and entries and exits to tunnels and viaducts

The Bayesian network associated with these cases requires the conditional probabilities of $\Pr(A|B, C)$ where A = driver's state, B = previous driver's state, and C = infrastructure, and leads to the transition matrix $N_{inf}\,(\chi, \phi_1, \phi_2, \phi_3)$ that becomes:

$$\begin{pmatrix} 1-\chi\phi & 0 & 0 & 0 & 0 & 0 \\ 0 & 1-\chi\phi & 0 & 0 & 0 & 0 \\ 0 & 0 & 1-\chi\phi & 0 & 0 & 0 \\ \chi\phi_1 & \chi\phi_1 & \chi\phi_1 & 1 & 0 & 0 \\ \chi\phi_2 & \chi\phi_2 & \chi\phi_2 & 0 & 1 & 0 \\ \chi\phi_3 & \chi\phi_3 & \chi\phi_3 & 0 & 0 & 1 \end{pmatrix} \tag{10}$$

where $\phi = \phi_1 + \phi_2 + \phi_3$ and ϕ_1, ϕ_2, and ϕ_3 are the probabilities of having a minor, moderate, or severe accident when passing switches or entering or exiting tunnels or viaducts, and χ is the probability of having a problem at these elements.

5 EXAMPLES OF APPLICATIONS

With the aim of illustrating how the model performs in this section, we include some examples. We discuss four cases in which the ATP systems are different:

1. *ERTMS supervision.* The ERTMS supervises all actions related to light and speed limit signals.
2. *ERTMS/ASFA supervision.* This case assumes that two supervising systems act simultaneously.
3. *ASFA supervision.* In this case, the system supervises errors due to light signals and temporal speed limitations but not permanent speed limitations.
4. *Staff responsible.* In this case, there is no ATP system, that is, the train circulates only under the driver's responsibility.

Because we have considered minor, moderate, and severe accidents, even though we have the probabilities of all types of accidents, to simplify the analysis we work with the expected number of equivalent severe accidents (ENESA) considering that 25 minor and 5 moderate accidents are equivalent to 1 severe accident. The results shown in the following section provide this expected number.

It is interesting to see that reliability can be associated with two different sources: line and signals. If human errors in signals are protected by ATP systems, then the probabilities of an accident are very much reduced and then other sources of accident become apparent. On the

Table 6
Conditional probability tables associated with the driver's state: conditional probabilities $\Pr(A|B, C, D, E)$ where A = driver's state, B = previous driver's state, C = Pre-previous action correctness, D = previous action correctness, E = action correctness. Variables C, D, and E take the values 0 and 1 that correspond to "Correct" and "Error," respectively.

		C, D, E								
		111	*110*	*101*	*100*	*011*	*010*	*001*	*000*	*N. T. S.*
A	B	$\Pr(A\|B, C, D, E)$								
Distracted	Distracted	$1-(\pi_1+\pi_2)$	1	$1-(\varepsilon_1+\varepsilon_2)$	1	$1-(\pi_1+\pi_2)$	1	1	1	p_0
	Attentive	0	0	0	0	0	0	0	0	p_0
	Alert	0	0	0	0	0	0	0	0	p_0
	Minor	0	0	0	0	0	0	0	0	p_0
	Moderate	0	0	0	0	0	0	0	0	p_0
	Severe	0	0	0	0	0	0	0	0	p_0
Attentive	Distracted	0	0	0	0	0	0	0	0	p_1
	Attentive	$1-(\pi_1+\pi_2)$	1	$1-(\varepsilon_1+\varepsilon_2)$	1	$1-(\pi_1+\pi_2)$	1	$1-\varepsilon_1$	1	p_1
	Alert	0	0	0	0	0	0	0	0	p_1
	Minor	0	0	0	0	0	0	0	0	p_1
	Moderate	0	0	0	0	0	0	0	0	p_1
	Severe	0	0	0	0	0	0	0	0	p_1
Alert	Distracted	0	0	0	0	0	0	0	0	p_2
	Attentive	0	0	0	0	0	0	0	0	p_2
	Alert	$1-(\pi_1+\pi_2)$	1	$1-(\varepsilon_1+\varepsilon_2)$	1	$1-(\pi_1+\pi_2)$	1	$1-\varepsilon_2$	1	p_2
	Minor	0	0	0	0	0	0	0	0	p_2
	Moderate	0	0	0	0	0	0	0	0	p_2
	Severe	0	0	0	0	0	0	0	0	p_2
Minor	Distracted	π_1	0	0	0	π_1	0	0	0	p_{A_2}
	Attentive	π_1	0	ε_1	0	π_1	0	ε_1	0	p_{A_2}
	Alert	π_1	0	ε_1	0	π_1	0	ε_1	0	p_{A_2}
	Minor	0	0	0	0	0	0	0	0	p_{A_2}
	Moderate	1	1	1	1	1	1	1	1	p_{A_2}
	Severe	0	0	0	0	0	0	0	0	p_{A_2}
Moderate	Distracted	π_2	0	0	0	π_2	0	0	0	p_{A_3}
	Attentive	π_2	0	ε_2	0	π_2	0	ε_2	0	p_{A_3}
	Alert	π_2	0	ε_2	0	π_2	0	ε_2	0	p_{A_3}
	Minor	0	0	0	0	0	0	0	0	p_{A_3}
	Moderate	0	0	0	0	0	0	0	0	p_{A_3}
	Severe	1	1	1	1	1	1	1	1	p_{A_3}
Severe	Distracted	0	0	0	0	0	0	0	0	p_{A_1}
	Attentive	0	0	0	0	0	0	0	0	p_{A_1}
	Alert	0	0	0	0	0	0	0	0	p_{A_1}
	Minor	1	1	1	1	1	1	1	1	p_{A_1}
	Moderate	0	0	0	0	0	0	0	0	p_{A_1}
	Severe	0	0	0	0	0	0	0	0	p_{A_1}

contrary, when no protection exists, then the errors in light signals become the relevant ones.

5.1 ERTMS supervision example

In this case, we assume that the train circulates under supervision of the ERTMS system.

Figure 6 shows a virtual segment of 150 kilometers in which we have included some signals, such as warning, advanced, entry and the three speed limit types, for permanent and temporal cases, and maximum speed change signals together with the driver's guide (LH). Close to each element, we have indicated the corresponding kilometer. The bottom band refers to the ATP system, which in this case is ERTMS (green). Tunnels and viaducts are also being represented in blue and pink, respectively, in the upper band. We note that the different elements in the figure are shown equidistant; however, the real distances corresponding to the space between elements are not the same.

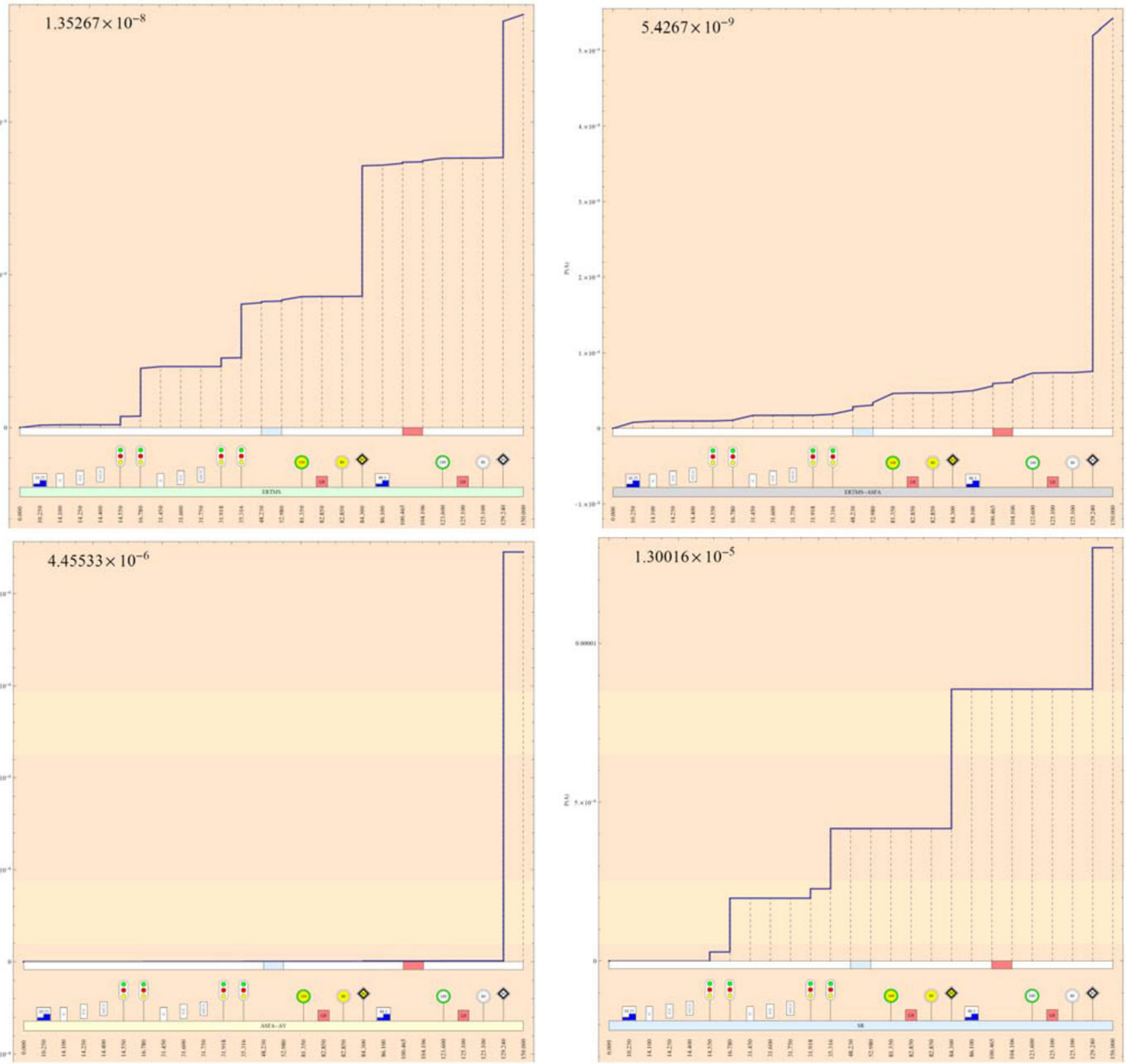

Fig. 6. Examples under ERTMS, ERTMS and ASFA, ASFA and Staff Responsible supervisions.

The ordinates of the graph represent the accumulated ENESA and the abscissa is the traveled distance.

An analysis of the graph shows the following facts: (1) relevant discontinuous changes appear at light and speed limit signals, where the speed limit jumps are higher than the light ones; (2) a small jump appears at advanced signals, due to the possibility of a red light and the associated error; (3) a continuous increase can be observed in long segments, due to rolling stock, infrastructure, cutting, and embankments type failures; (4) small changes at entries and exits of tunnels and viaducts are also present.

The proposed method has been applied to this case, where the accumulated ENESA at the end of the trip is $p_A = 1.35 \times 10^{-8}$, as we can see in the left upper part of Figure 6.

Table 7 shows two sets of parameters values assumed v_w and v_b that represent two extremes: the worst and the best assumptions, respectively. Column k_v represents the percentage of improvement obtained (with respect to the value $p_A = 1.35 \times 10^{-8}$) when the worst value of the parameter v is replaced by the best one, but keeping the worst values for the remaining parameters. These values allow the ENESA to be recalculated when

Table 7
Parameter ranges used and sensitivity analysis: illustrative example with ERTMS as ATP system. Improvements of the accumulated ENESA with respect to the worst expected number $p_A = 1.35 \times 10^{-8}$, due to individual improvements of each of the factors v and associated improvement percentages k_v

Parameter (v)	v_w	v_b	k_v	*Parameter* (v)	v_w	v_b	k_v
η	1.8×10^2	2.4×10^2	17.	σ_2	$1. \times 10^{-1}$	1.67×10^{-1}	0.
γ_1	$4. \times 10^{-2}$	0.	40.8	σ_3	$1. \times 10^{-1}$	1.67×10^{-1}	0.
γ_2	$1. \times 10^{-2}$	0.	37.5	δ_1	$9. \times 10^{-1}$	1.	0.
γ_3	$3. \times 10^1$	$1. \times 10^1$	20.9	δ_2	$1. \times 10^{-1}$	0.	0.
ψ_1	$7. \times 10^{-10}$	$7. \times 10^{-11}$	0.2	μ_1	$1. \times 10^{-1}$	$3. \times 10^{-1}$	0.
ψ_2	$7. \times 10^{-10}$	$7. \times 10^{-11}$	0.9	μ_2	$3. \times 10^{-1}$	$2. \times 10^{-1}$	0.
ψ_3	$7. \times 10^{-10}$	$7. \times 10^{-11}$	4.3	μ_3	$3. \times 10^{-1}$	$2. \times 10^{-1}$	0.
λ	$7. \times 10^{-1}$	$9. \times 10^{-1}$	65.2	ν_1	$6. \times 10^{-1}$	$7. \times 10^{-1}$	0.
ε	$1. \times 10^{-4}$	0.	0.	ν_2	1.5×10^{-1}	$2. \times 10^{-1}$	0.
q_g	$9. \times 10^{-1}$	9.5×10^{-1}	17.1	ν_3	$1. \times 10^{-1}$	$1. \times 10^{-1}$	0.
q_{ap}	2.5×10^{-2}	$5. \times 10^{-2}$	5.7	π_1	0.	$2. \times 10^{-1}$	0.
θ_s	1.42×10^{-3}	$1. \times 10^{-6}$	14.7	π_2	0.	$2. \times 10^{-1}$	0.
θ_v	1.74×10^{-4}	$1. \times 10^{-6}$	0.	π_3	$1. \times 10^{-1}$	0.	0.
α_1	0.	$1. \times 10^{-1}$	0.	π_4	$3. \times 10^{-1}$	$1. \times 10^{-1}$	0.
α_2	0.	$1. \times 10^{-1}$	0.	π_5	$5. \times 10^{-1}$	$2. \times 10^{-1}$	0.
α_3	$1. \times 10^{-1}$	0.	0.	τ_s	9.99×10^{-1}	$9. \times 10^{-1}$	0.
β_1	3.33×10^{-1}	$4. \times 10^{-1}$	0.	τ_v	9.99×10^{-1}	$9. \times 10^{-1}$	0.
β_2	$4. \times 10^{-1}$	3.33×10^{-1}	0.	q_{gs}	$1. \times 10^{-1}$	$2. \times 10^{-1}$	0.
β_3	$2. \times 10^{-1}$	3.33×10^{-1}	0.	q_{aps}	$5. \times 10^{-2}$	$1. \times 10^{-1}$	0.
σ_1	$5. \times 10^{-1}$	$7. \times 10^{-1}$	0.				

the parameters values are changed close to the worst values.

This table shows as most relevant parameters $\lambda, \gamma_1, \gamma_2, \gamma_3, q_g$, and η.

Figure 7 shows how the accumulated ENESA changes when the indicated parameters change and all other parameters remain equal to their worst values. The red and green points correspond to the worst and best cases, respectively. Only the graphs associated with the parameters whose effect (k_v) is larger than 20% are shown. Note that not all curves are linear.

A simple look to the left upper part of Figure 6 indicates that any safety improvement effort should be addressed to improve the safety in light and speed limit signals, because the most important part of the accumulated ENESA is due to them. This suggests the use of two simultaneous ATP systems, for example, adding the ASFA system, as it is shown in the simultaneous ERTMS and ASFA supervision example.

5.2 Simultaneous ERTMS and ASFA supervision example

In this case, we assume that the train circulates under the simultaneous supervision of the ERTMS and the ASFA systems.

As we can see in the right upper part of Figure 6, the accumulated ENESA at the end of the trip is $p_A = 5.43 \times 10^{-9}$.

Similar tables and sensitivity plots as those in the previous example have been obtained. However, lack of space prevents us from including them here.

Note the fact that most of the ENESA can be associated with the permanent speed limit signal because unfortunately the ASFA system does not cover human errors at this type of signals. In spite of that, we have reduced the ENESA to approximately one half. However, with a correction of this ASFA limitation, which is the obvious suggested improvement after visualization of the graph, we would get a much higher safety improvement.

It is worth mentioning that, in this case, the effect of the light and temporal speed limit signals is significantly smaller than the one associated with tunnels and viaducts, rolling stock, cuttings and embankments, etc.

5.3 ASFA supervision example

In this case, we assume that the train circulates under supervision of the ASFA system.

As we can see in the left lower part of Figure 6, the accumulated ENESA at the end of the trip is $p_A = 4.46 \times 10^{-6}$, significantly greater than the value $p_A = 1.35 \times 10^{-8}$ obtained for the ERTMS case.

A simple look at the graph reveals the main cause (permanent speed limit signals not covered by ASFA) of a larger value for the ENESA and how to proceed to improve safety.

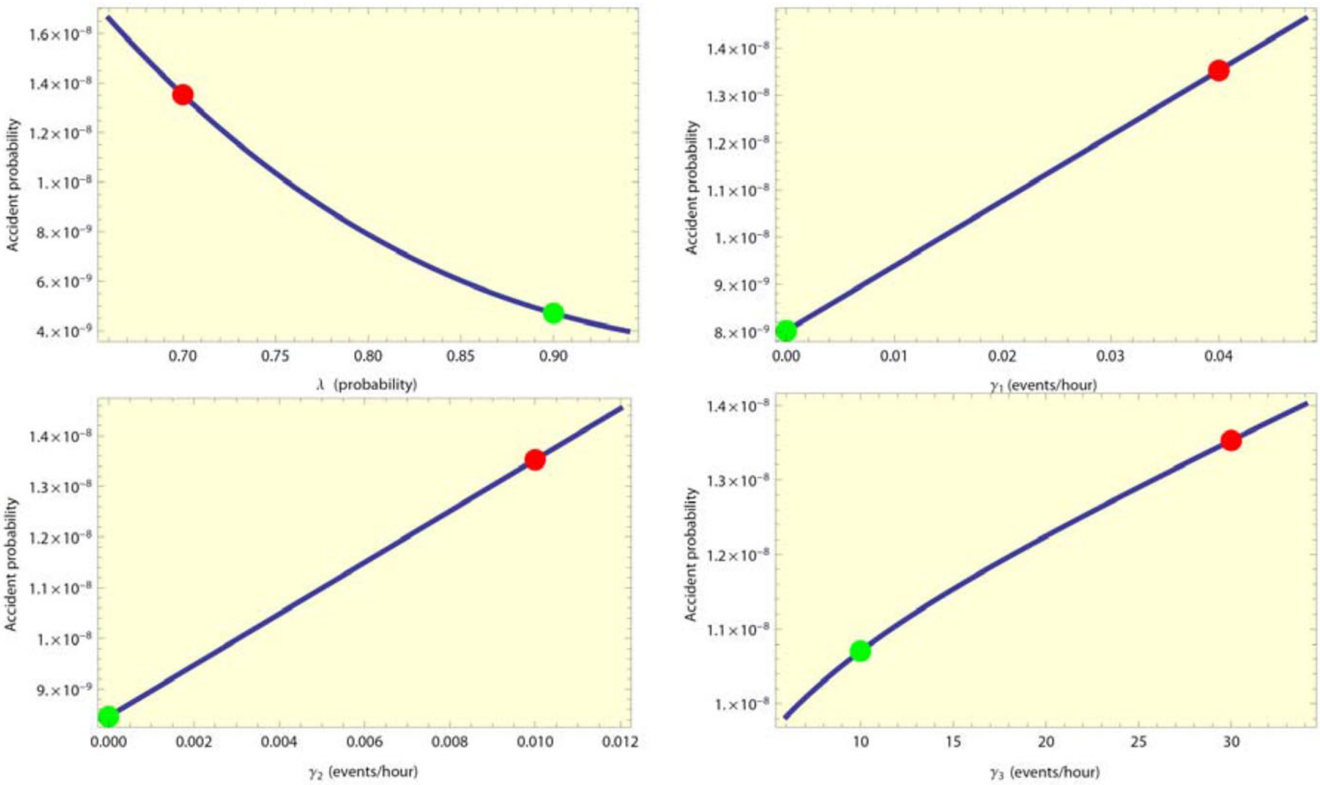

Fig. 7. Illustrative example with ERTMS as ATP system. Changes on the accumulated ENESA due to changes in the most influential ($k_v > 20\%$) individual parameters.

5.4 Staff responsible example

In this case, we assume that there is no ATP system and then the responsibility is passed onto the train driver.

As we can see in the right lower part of Figure 6, the accumulated ENESA at the end of the trip is $p_A = 1.30 \times 10^{-5}$, as expected much higher than the previous values, as no ATP system exists.

The graph suggests a safety improvement based on supervising the light and speed limit signals. It can be seen that, in the absence of an ATP system, the positive effect of the warning signals reduces the ENESA to one half (compare the jumps at the light and speed limit signals in the graph).

6 THE ORENSE–SANTIAGO LINE EXAMPLE

In this section, we show some results of the application of the proposed model to the Orense–Santiago line, where an accident involving 80 casualties took place in July 2013. This line contains 14 light signals, 18 warning signals, 4 maximum speed changes, 31 tunnels, 35 viaducts, and 68 intervals where some events, such as slope stability, falling stones, broken tracks, or other problems can arise. This example is large enough to give an idea of the complexity of the model because it contains more than 1,700 variables.

This example corresponds to a report that evaluates the probability of the 2013 accident and is to be used in Court. To this end, we tried it to be based on data previous to the accident, so we intentionally tried to avoid overfitting. In other words, we did not calibrate any parameters using the data related to the accident to present a knowledge situation previous to the accident occurrence.

We estimated the model parameters based on previous experience on accidents and data from international databases and technical recommendations of reliable institutions in the field (mainly RSSB) together with common sense. The calibration of parameters was done by statistical hypotheses testing. In other words, we tested that the accident and other event observations did not contradict the results we obtained with the model.

To simplify, we analyze four cases that can be of interest for the case to take place in court:

Case 1. The line state in July 24, 2013, which is the day of the accident (with digital ASFA as ATP system from Orense to Santiago).

Case 2. It corresponds to a modified project, which was proposed as an alternative to the actual one. It was operated under staff responsible (SR) from PK 1.845 to 14.953, ERTMS to PK 80.119 and analogic ASFA to Santiago.

Case 3. The existing line after incorporating speed temporal limitation signals after the accident. Since a decision of incorporating temporal limitation signals after the accident was made, it is interesting to evaluate how the probability of accident is improved by adopting this solution.

Case 4. The line in the hypothetical case of using two ATP systems (ASFA and ERTMS) and without using temporal speed limit signals. It is analyzed to demonstrate the beneficial effect of duplicating ATP systems. Actually, even though two ATP systems are implemented, only one is operated at each time.

In Figure 8 we show the accumulated probability of equivalent severe accidents with traveled distance for the Orense–Santiago line for the four different analyzed cases.

A simple look at the figures reveals the following:

1. In Case 1 we obtain 8.22×10^{-6} expected accidents (for each line travel) and it is clear that the maximum speed reduction signal at PK 84.273, indicated only on the drivers booklet but not by side signals and not covered by the ATP system (the conventional ASFA system) is the most critical point on the line. It was the place where the accident took place because of a driver's distraction, who did not respect the 80 km/h speed limit traveling at 170 km/h, more than twice the maximum allowed speed. It is also clear that a detailed risk analysis would have almost definitely pointed out the possibility of this critical possible human error, almost definitely avoiding the accident.
2. The graph associated with Case 2 shows that in addition to the maximum speed change location, there is an advanced light signal located at PK 12.000, which is not covered by ATP because there the train would have circulated under the sole responsibility of the driver. This implies an increase in the probability of accident, proving that the actual project was safer than the modified one.
3. In Case 3, the use of temporal speed limit signals produce the action of the ATP system (the conventional ASFA system) in the case of a speed violation, which implies an important reduction in the probability of accident (1.22×10^{-7}). These small numbers permit us to graphically observe the small contribution to the probability of accident associated with the entries and exits to tunnels and viaducts (see the small stairs in the graphs) and the relevance of the exit signal station at PK 1.845 relative to other signals.
4. Finally, Case 4 shows that a double ATP system acting in parallel produces a reduction in the probability of accident to 5.15×10^{-8}, only limited by the maximum speed change, not covered by one of the ATP systems (the conventional ASFA system).

Finally, to validate the result, we have tested the probability of accident 8.22×10^{-6} associated with Case 1 using the number of circulating trains during the period of more than one and a half years of the Orense–Santiago line and the resulting accident probability 8.22×10^{-6} could not be rejected by a statistical test of significance for the usual significance level of 0.05.

These examples show the power and interest of the proposed methods in reducing risks and optimizing the cost of safety systems by analyzing whether or not the risk due to different elements is equilibrated.

7 PARAMETER ESTIMATION AND VALIDATION OF THE MODEL

One of the shortcomings and at the same time one of the advantages of the proposed model is the high number of parameters involved. On the one side, this permits very different variables that play a role in railway safety to be reproduced, but on the other side, this implies a large number of parameters to be estimated.

First, we must say that any serious probability risk analysis must include all the relevant factors and elements playing a role in safety and that this implies many assumptions about probabilities. For example, in the case of nuclear power plants, where there is a long tradition in using these methods, the analysis is far more complicated than that of railways and the number of probabilities involved are much more. In addition, the consequences of failure can be much worse.

It must be recognized that all PRA procedures in any field are subject to the problem of dealing with rare events, that is, events that occur with a very small probability and this means events with a small probability of occurrence, which is difficult to estimate (see Haan and Sinha, 1999). Therefore, this is a common problem that cannot be avoided and as it is well known, requires some subjective knowledge mixed with some objective information. However, a successful quantification of uncertain parameters is possible with participation of miscellaneous groups of professionals (see, e.g., Wreathall et al., 2003).

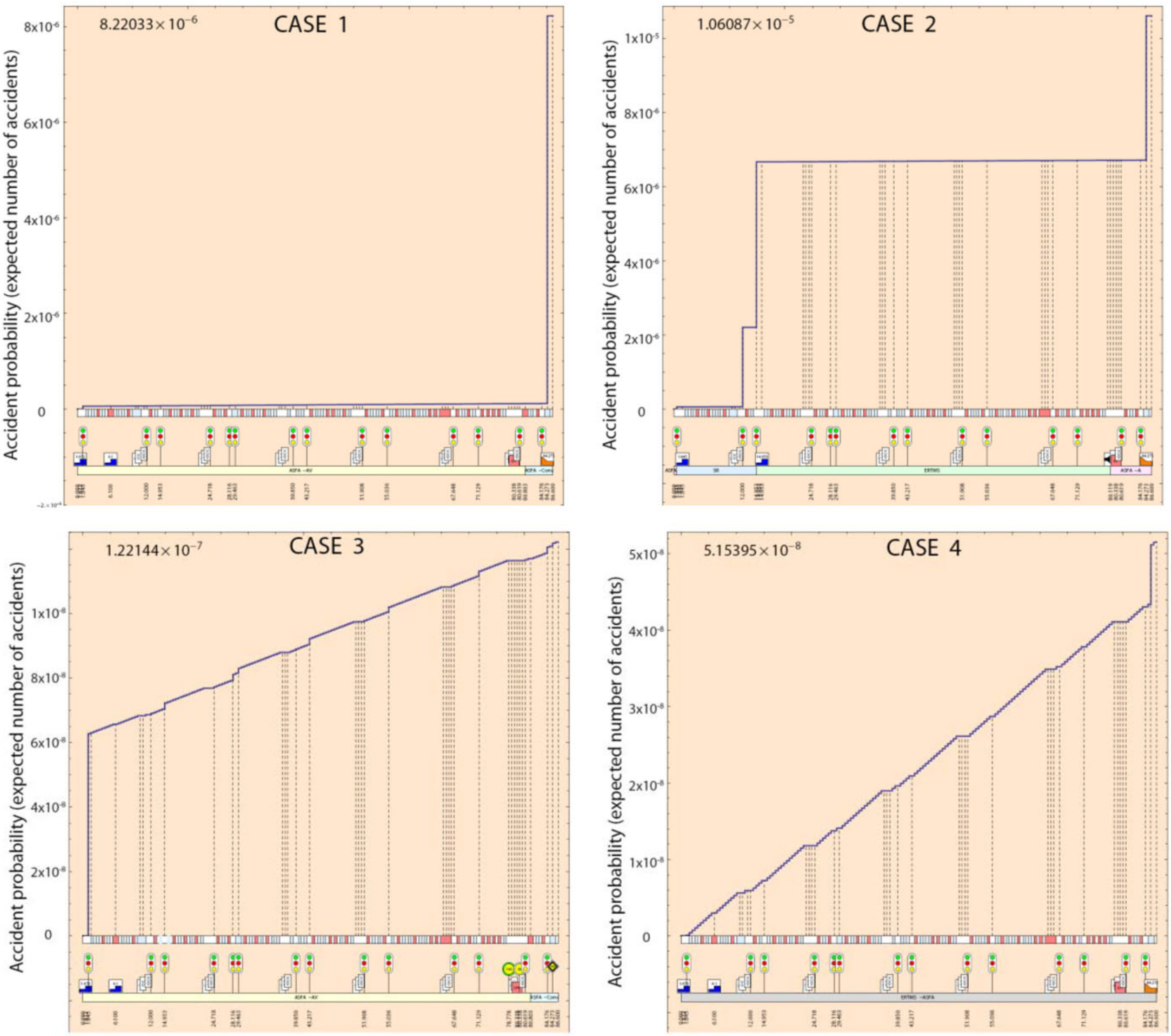

Fig. 8. Accumulated probability of equivalent severe accidents with traveled distance for the Orense–Santiago line for the four different analyzed cases.

Because we cannot be very precise when assigning values to our parameters, we can initially work with ranges (confidence intervals when available or simply upper and lower bounds for the parameters). Fortunately, the model allows a sensitivity analysis (see Castillo et al., 1997a) to be easily done by considering upper and lower bounds of all probabilities associated with the variable ranges provided. Then, we can measure and sort the relative influence of the different parameters in the final failure probabilities we are interested in. In this way we can exclude a long list of parameters that have no important influence and identify and analyze in more detail those which play an important role (an example is given in Table 7 and Figure 7). This procedure avoids a lot of work and doubts because we can concentrate only on the main factors and ignore the unimportant ones. We want to point out here that this task is not trivial and we frequently discover that some parameters, which are expected to be relevant, are not and also that other parameters considered irrelevant are really important.

In the case of railways, when data for a given line are not available, we can use data from similar lines or even from data from other countries with the corresponding corrections mixed with common sense. In this context, official data on railways, and statistical data of railway societies and other institutions or authors are very useful as a starting point for selecting point or interval parameter estimates (see, e.g., Muttram, 2002; Wreathall et al., 2003; Mokkapati et al., 2009; or Evans 2011).

In addition, once we have calculated the probabilities of all events (not only accidents), we can validate them with real observations. If the parameter values selected lead to contradictions between calculated and observed values, we can redo the calculations by modifying the corresponding parameters until a consistent result is obtained.

In summary, the results obtained by these methods should be regarded as relative ones in the sense that they permit comparing safety associated with different scenarios. If more precise probabilities are required, extreme care must be taken in the parameter estimation process.

This technique has been used in an evaluation of the risks associated with the Orense–Santiago de Compostela line, where the terrible accident killing 80 people took place in July 2013. The technique proved to be satisfactory for detecting some deficiencies in safety, mainly related to ATP systems and to maximum speed changes not directly indicated by side signals on the line but in a time book given to the driver. These deficiencies were immediately detected from graphs as those in Figure 8.

Summarizing, we think that it is not difficult for rail safety experts to provide some general ranges for the different parameters involved in the proposed model to be particularized for each case studied. We also think that our model could be very valuable to practitioners because even if the parameter estimation is not very precise, one can obtain very interesting relative values of the risks associated with different sources with the possibility of identifying those who deserve immediate action. Consequently, the model can be useful to evaluate different rail lines and prevent accidents. In fact, we think that if this methodology were used for this line at the design stage, the accident could have been avoided.

8 CONCLUSIONS

The following conclusions can be drawn from the previous discussion:

1. Due to their particular characteristics, railway risk probability assessments (PRA) require specific tools to quantify probabilities and their dependencies of railway lines, which lead to the fact that extrapolating other tools coming from nuclear power plants or other areas to this field becomes difficult and problematic.
2. In particular, human error must be carefully considered in an integrated form, that is, considering how it depends on tiredness and attention levels, as being one of the most important factors in the safety of railway networks and lines. In this direction, the driver's tiredness caused by a long driving time and the evolution of the driver's attention with the sequence of events faced when driving must be taken into account.
3. A Markovian–Bayesian network model has been proposed to analyze how the probability of accident accumulates and how the driver's attention evolves when the train travels along a given line and faces different elements that have associated potential hazards. This can be done by simply multiplying the corresponding transition matrices by the actual vector of probabilities and by other standard evidence propagation methods used in Bayesian networks. The model allows for a very general probability distribution dependence structure, which permits reproducing all relations among the different variables involved including common causes. Bayesian networks permit all generalities, but other models do not.
4. The proposed model permits reproducing railway lines in a natural way, so that all different elements, such as all types of signals, cuttings, embankments, rolling stock, tracks, infrastructure, switches, supervising systems, etc. can be included. The proposed model makes an important effort to quantify the influence of all these elements at risk.
5. The proposed model must consider all the possible sequences of events leading to accidents to guarantee that all possible combinations are taken into account. Bayesian networks have a special facility to do this because they reproduce dependence among all the variables involved.
6. Application of the model to some illustrative examples permits observing the important role of ATP systems that substantially reduce accident probabilities and export the main risks from light and speed signals, initially the main causes of accident, to other elements such as the infrastructure or the rolling stock. This means that when a good ATP system has been installed, extra efforts to improve safety must be addressed to the infrastructure or the rolling stock, because then an extra effort on signals safety will not produce a significant safety improvement.
7. Application of the proposed model permits not only determining the relative contribution of each

element to the general safety but determining where an action must be taken.

8. Since the model is very rich in parameters, because it includes many sources of accident, these parameters need to be estimated and validated. This means that a great effort must be made to fix ranges of reasonable values for the parameters and how they can be determined in practical situations. Official railway data and data coming from railway societies become very relevant for initial point or interval estimators.
9. Some methods have been given to identify the relevant and the irrelevant parameters so that efforts can be concentrated on the relevant ones avoiding wasting time and money expenses with the irrelevant ones. Sensitivity analysis has been proved as a very powerful tool to proceed to such an identification.

9 NOTATION

A accident.
C driver's correct decision.
$M_\ell()$ transition matrix associated with a segment without signals.
$M_a()$ transition matrix associated with a warning signal.
$N_s^0()$ transition matrix associated with the visualization of a signal.
$N_s^v()$ transition matrix associated with the start of a speed limit signal
S ATP system correctness.
$T\,(a_{t^*})$ Continuous Markov process transition matrix.
a_t attention level at time t.
k_v percentage of contribution of parameter v to the driver's error probability.
p_{A_1} probability of minor accident.
p_{A_2} probability of moderate accident.
p_{A_3} probability of severe accident.
p_A expected value measured in equivalent severe accidents.
p_A^v probability of accident when parameter v attains its most favorable value.
p_C probability of driver's correct decision.
p_{E_1} probability of driver's speed reduction error.
p_{E_2} probability of driver's stop error.
p_0 probability of the driver's being distracted.
p_1 probability of the driver's being attentive.
p_2 probability of the driver's being alert.
p_0^0 probability of the driver's being distracted at the beginning of the trip.
p_1^0 probability of the driver's being attentive at the beginning of the trip.
p_2^0 probability of the driver's being alert at the beginning of the trip.
p_0^* probability of the driver's being distracted after an event.
p_1^* probability of the driver's being attentive after an event.
p_2^* probability of the driver's being alert after an event.
q_{ap} probability of the signal's being on stop-ahead.
q_g probability of the signal's being on green.
q_p probability of the signal's being on stop.
q_s probability of the signal's being on state s.
t time corresponding to the considered instant attention level.
t_0 segment starting time.
v parameter.
α_1 probability of no accident when the trains go beyond a signal at red.
α_2 probability of minor accident when a red signal has been improperly surpassed.
α_3 probability of moderate accident when a red signal has been improperly surpassed.
α_4 probability of severe accident when a red signal has been improperly surpassed.
$\beta_1, \sigma_1, \delta_1, \mu_1, \nu_1$ probabilities of no accident corresponding to the cases of correct-ST error, ST error-SP error or SP error-SP error, correct-SP error, ST error-correct and SP error-correct.
$\beta_2, \sigma_2, \delta_2, \mu_2, \nu_2$ probabilities of minor accident corresponding to the cases of correct-ST error, ST error-SP error or SP error-SP error, correct-SP error, ST error-correct and SP error-correct.
$\beta_3, \sigma_3, \delta_3, \mu_3, \nu_3$ probabilities of moderate accident corresponding to the cases of correct-ST error, ST error-SP error or SP error-SP error, correct-SP error, ST error-correct and SP error-correct.
$\beta_4, \sigma_4, \delta_4, \mu_4, \nu_4$ probabilities of severe accident corresponding to the cases of correct-ST error, ST error-SP error or SP error-SP error, correct-SP error, ST error-correct and SP error-correct.
$\gamma_i/a_{t^*}; i = 1, 2$ time rates of getting distracted when the driver is attentive and alert, respectively.
$\gamma_3/a_{t^*}; i = 1, 2$ time rates of recovering attention when the driver is alert.

δ parameter of the proposed formula to reproduce driver's tiredness evolution.
Δt time increment.
ε probability of being unaware of the signal presence when the driver circulates under an attentive level.
ηa_{t^*} time rate of recovering attention when driver is distracted after a time t^* from the beginning of the trip.
λ probability of recovering attention when visualizing the signal when being distracted.
θ conditional probability of error when the driver is attentive and the signal is not in free state.
θ_s conditional probability of error when the driver is attentive and the light signal is not in free state.
θ_v conditional probability of error at a speed limit signal when the driver is attentive.
μ mean.
π_1 probability of moderate accident if the driver ignores all three signals.
π_2 probability of moderate accident if the driver ignores the first two signals.
ρ the ATP system error probability.
σ standard deviation.
τ conditional probability of error when the driver is distracted and the signal is not in free state.
τ_s conditional probability of error when the driver is distracted and the light signal is not in free state.
τ_v conditional probability of error at a speed limit signal when the driver is distracted.
ϕ_1 probability of having a minor accident when passing switches or entering or exiting tunnels or viaducts.
ϕ_2 probability of having a moderate accident when passing switches or entering or exiting tunnels or viaducts.
ϕ_3 probability of having a severe accident when passing switches or entering or exiting tunnels or viaducts.
χ probability of having a problem when passing switches or entering or exiting tunnels or viaducts.
ψ Accident time rate due to technical failure, infrastructure or terrain in segments without signals.
ψ_1 Minor accident time rate due to technical failure, infrastructure or terrain in segments without signals.
ψ_2 Moderate accident time rate due to technical failure, infrastructure or terrain in segments without signals.
ψ_3 Severe accident time rate due to technical failure, infrastructure or terrain in segments without signals.

REFERENCES

Al-Basman, M. & Hu, J. (2010), Probability of conflict analysis of 3D aircraft flight based on two-level Markov chain approximation approach, in *Networking, Sensing and Control (ICNSC), 2010 International Conference*, pp. 608–13.

Andersson, A., O'Connor, A. & Karoumi, R. (2015), Passive and adaptive damping systems for vibration mitigation and increased fatigue service life of a tied arch railway bridge. *Computer Aided Civil and Infrastructure Engineering*, DOI: 10.1111/mice.12116.

Arnold, B., Castillo, E. & Sarabia, J. M. (1999), *Conditional Specification of Statistical Models*, Springer Verlag, New York.

Arnold, B. C., Castillo, E. & Sarabia, J. M. (2001), *Conditionally specified distributions: an introduction, Statistical Science*, **16**(3), 249–65.

Beales, L. (2002), *Guidance on the Preparation of Risk Assessments within Railway Safety Cases*. Rail Safety and Standards Board, United Kingdom.

Bearfiel, G. & Marsh, W. (2005), Generalising event trees using Bayesian networks with a case study of train derailment. *Lecture Notes in Computer Sciences*, **3688**, 52–66.

Benjamin, J. R. & Cornell, C. A. (1970), *Probability Statistics and Decision for Civil Engineers*, McGraw-Hill, New York.

Bjorkman, P. (2011), Probabilistic safety assessment using quantitative analysis techniques – application in the heavy automotive industry. PhD thesis, Uppsala University, Sweden.

Castillo, E., Calviño, A., Nogal, M. & Lo, H. K. (2014a), On the probabilistic and physical consistency of traffic random variables and models. *Computer Aided Civil and Infrastructure Engineering*, **29**, 496–517.

Castillo, E., Gallego, I., Sánchez-Cambronero, S., Menéndez, J. M., Rivas, A., Nogal, M. & Grande, Z. (2014b), An alternate double-single track proposal for high speed peripheral railway lines. *Computer Aided Civil and Infrastructure Engineering*, DOI: /10.1111/mice.12083.

Castillo, E., Gallego, I., Ureña, J. M. & Coronado, J. M. (2011), Timetabling optimization of a mixed double and single tracked railway network. *Applied Mathematical Modelling*, **35**(2), 859–78.

Castillo, E., Gutiérrez, J. M. & Hadi, A. (1997a), Sensitivity analysis in discrete Bayesian networks. *IEEE Transactions on Systems, Man and Cybernetics*, **26**(7), 412–23.

Castillo, E., Gutiérrez, J. M. & Hadi, A. S. (1997b), *Expert Systems and Probabilistic Network Models*, Springer-Verlag, New York.

Castillo, E., Sarabia, J. M. Solares, C. & Gómez, P. (1999), Uncertainty analyses in fault trees and Bayesian networks using FORM/SORM methods. *Reliability Engineering and System Safety*, **65**, 29–40.

Dadashi, N., Scott, A., Wilson, J. R. – Mills, A. (2013). *Rail Human Factors: Supporting Reliability, Safety and Cost Reduction*. CRC Press, Taylor and Francis, London.

De Felice, F. & Petrillo, A. (2011), Methodological approach for performing human reliability and error analysis in railway transportation system. *International Journal of Engineering and Technology*, **3**(5), 341–53.

Dhillon, B. S. (1982), Stochastic models for predicting human reliability. *Microelectronics and Reliability*, **25**, 491–96.

Dhillon, B. S. (1983), System reliability evaluation models with human errors. *IEEE Transactions on Reliability*, **32**, 47–48.

Dhillon, B. S. (2007), *Human Reliability and Error in Transportation Systems*. *Springer Series in Reliability Engineering.* Springer London, DOI: 10.1007/978-1-84628-812-8.

Dirección de Seguridad en la Circulación, ADIF, *Sistema de gestión de seguridad en la circulación. Evaluación y gestión de riesgos*. Ref: SGSC/EGR, revisión 3, 5/10/2009.

Doob, J. L. (1953), *Stochastic Processes*, John Wiley and Sons, New York.

Evans, A. W. (2011), Fatal train accidents on European railways: 1980–2009. *Journal of Accident Analysis and Prevention*, **43**(1), 391–401.

Feldmann, F., Hammerl, M. & Schwartz, S. (2008), Questioning human error probabilities in railways, in *System Safety, 2008 3rd IET International Conference*, pp. 1–6.

Flammini, F., Marrone, S., Mazzocca, N. & Vittorini, V. (2006), Modeling system reliability aspects of ERTMS/ETCS by fault trees and Bayesian networks, in *17th European Safety and Reliability Conference (ESREL)*, 2675–83.

Fukuyama, H., Inutsuka, F., Tachi, M. & Ishige, T. (2008), Application of risk assessment method in railway. *Sociotechnica*, **1**(5), 163–71.

Fuqua, N. B. (2007), *The Applicability of Markov Analysis Methods to Reliability, Maintainability, and Safety*, Volume **10**. Available at: https://src.alionscience.com/pdf/MARKOV.pdf, accessed April 2015.

Gibson, H. (2012), *Railway Action Reliability Assessment User Manual*. Rail Safety and Standards Board, United Kingdom.

Haan, L. & Sinha, A. (1999), Estimating the probability of a rare event. *The Annals of Statistics*, **27**(2), 732–59.

Hammerl, M. & Vanderhaegen, F. (2012), Human factors in the railway system safety analysis process, in J. R. Wilson, A. Mills, T. Clarke, J. Rajan, and N. Dadashi (eds.), *Rail Human Factors Around the World: Impacts on and of People for Successful Rail Operations*, Taylor & Francis, pp. 73–84.

Henley, E. J. & Kumamoto, H. (1992), *Probabilistic Risk Assessment; Reliability Engineering, Design, and Analysis*, IEEE Press, New York.

Instituto Nacional de Seguridad e Higiene en el Trabajo. *Norma CENELEC 50126*.

Kawakami, S. (2014), Application of a systems-theoretic approach to risk analysis of high-speed rail project management in the US. PhD thesis, Massachusetts Institute of Technology, Cambridge, Massachusetts.

Kijima, M. (1997), *Markov Processes for Stochastic Modeling*, 1st edn. Chapman & Hall, Cambridge.

Kim, D. S., Baek, D. H. & Yoon, W. C. (2010), Development and evaluation of a computer-aided system for analyzing human error in railway operations. *Reliability Engineering & System Safety*, **95**(2), 87–98.

Kokkings, S. J. & Snyder, E. (1997), *Case Studies in Collision Safety*. Report, DOT/FRA/ORD-96/01, Federal Railroad Administration, Washington DC.

Kumar, A. & Sinha, P. K. (2008), Human error control in railways. *Jordan Journal of Mechanical and Industrial Engineering*, **2**(4), 183–90.

Lahrech, Y. (1999), Development and application of a probabilistic risk assessment model for evaluating advanced train control technologies. Master thesis, Massachusetts Institute of Technology, Cambridge, Massachusetts.

Masanori, T. & Fumiaki, F. (2008), A study about risk evaluation of JR East. *Eighth World Congress on Railway Research*, Seoul, Korea, pp. 1–9.

Massaiu, S. (2009), Integrating Human Factors in Risk Analysis. Available at: http://docupalace.com/file/1XSn/integrating-human-factors-in-risk-analysis.html, accessed April 2015.

Ministerio de Trabajo y Asuntos Sociales (2010), *Notas Técnicas de Prevención (NTP) 330: Sistema simplificado de evaluación de riesgos de accidente*.

Miyashita, N. (2010), 2013 Safety vision. *JR EAST Technical Review*, **15**(1), 163–71.

Mokkapati, C., Tse, T. & Rao, A. (2009), *A Practical Risk Assessment Methodology for Safety-Critical Train Control Systems*. Technical Report DOT/FRA/ORD-09/15, U.S. Department of Transportation, Washington DC.

Muttram, R. I. (2002), Railway safety's safety risk model. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, **216**(2), 71–79.

Pen, F. & Ouyang, Y. (2014), Optimal clustering of railroad track maintenance jobs. *Computer Aided Civil and Infrastructure Engineering*, **29**(4), 235–47.

Peterman, D. R., Frittelli, J. & Mallet, W. (2009), *High Speed Rail (HSR) in the United States*. CSR Report for Congress. R40973, Congress of the US.

Slovak, R., Kassev, K., Stoytcheva, N., Ivanov, E. & Schnieder, E. (2007), General stochastic modelling for quantitative safety analysis using Markov chains and Petri nets. *Information Technologies and Control*, **2**, 17–30.

Spurgin, A. J. (2009), Human error: anatomies of accidents. *IEEE Section Meeting*.

Sussman, J. M. (1996), Industry/academic cooperation in transportation: the partnership of JR east and MIT. *Japan Railway & Transport Review*, **7**, 26–33.

Suyama, K. & Kosugi, N. (2009), Probabilistic safety assessment and management of control laws based on strict Markov analysis, in *Industrial Electronics, 2009. IECON'09. 35th Annual Conference of IEEE*, pp. 1706–11.

Todorovich, H. P. & Hagler, Y. (2011), *High Speed Rail in America*. Technical report, America 2050.

Veneziano, D. & Papadimitriou, A. G. (2001), *Optimizing the Seismic Early Warning System for the Tohoku Shinkansen*. Springer Verlag, New York.

Wreathall, J., Roth, E., Bley, D. & Multer, J. (2003), *Human Reliability Analysis in Support of Risk Assessment for Positive Train Control*. Technical Report DOT/FRA/ORD-03/15, U.S. Department of Transportation, Cambridge, MA.

Zeilstra, M. P. & Van der Weide, R. (2013), Humans as an asset in a system consideration on the contribution of humans to system performance and system safety, in N. Dadashi, A. Scott, J. R. Wilson, and A. Mills (eds.), *Rail Human Factors: Supporting Reliability, Safety and Cost Reduction*, Taylor and Francis, London, pp. 473–82.