International Journal of Railway Technology
Volume 7, Issue 4, Pages 45-69, 2018.
doi:10.4203/ijrt.7.4.3

SAXE-COBURG
PUBLICATIONS

Probabilistic Safety Analysis of Railway Lines

E. Castillo[1,2], Z. Grande[2], A. Calviño[2,3], M. Nogal[4] and A.J. O'Connor[4]

[1]Royal Academy of Engineering, Spain,
[2]University of Cantabria, Santander, Spain
[3]Complutensis University of Madrid, Spain
[4]Delft University of Technology, The Netherlands

Abstract

A new probabilistic safety assessment method applicable to conventional and high speed railway lines is presented. The main idea consists of reproducing the railway line items which are relevant to safety by means of a Bayesian network as an alternative to more limited event and fault tree structures. The model evaluates the probability of incidents associated with the circulation of trains along the lines with special consideration of human errors. To this end, all the line relevant elements, such as light and speed limit signals, rolling stock failures, falling materials, slope slides in cuttings and embankments, tunnel or viaduct entries or exits, automatic train protection systems and other elements are reproduced with a special consideration of human behavior and human error. Since driver's attention plays a crucial role, its evolution and changes with driving time and due to other factors, such as seeing light signals or receiving acoustic signals are taken into account. The model updates the driver attention level and evaluates the probability of accident associated with the different elements encountered along the line. A continuously increasing risk graph with continuous and sudden changes is obtained indicating where actions must be taken to improve safety. This avoids waste of time and money by concentrating on the items most critical to safety. Finally, some illustrative examples are used to point out the models relevance.

Keywords: Bayesian networks, human error, driver's attention, conditional probabilities, automatic train protection systems.

1 Introduction

As recognized in other areas of knowledge, such as in the nuclear and aerospace fields, probabilistic safety assessments are also necessary in railway lines. Among the existing models used to assess risks and to perform a safety analysis, one of the most relevant and well known is the Safety Risk Model (SRM) proposed by the RSSB (Railway Safety Standard Board). Apart from other important contributions, they quantify the risk associated with some hazardous events leading to injuries or fatalities. In particular, the SRM provides a list of 110 hazardous events to evaluate the global risk measured in terms of collective, individual and societal components. In 2002, [1] estimated a frequency of 138 equivalent fatalities per year for the case of passengers, staff and members of the public under the existing control measures. One of the main contributions of the SRM is the identification of a wide range of failure modes and associated main causes and consequences of potential accidents that arise in regular and non-regular railway operation and maintenance. This information must be considered as a very rich piece of information that is required when performing standard risk assessments.

In many countries safety analyses reduce to qualitative tests or procedures in which events or sequences of events leading to relevant incidents are not identified adequately and the corresponding probabilities of occurrence are not quantified properly. Probabilistic safety analyses (PSA), which are standard procedures in other areas (aeronautical and nuclear industries), have not been incorporated yet as regular procedures to assess railway lines safety and are not mandatory in many countries (see [2]). Though probabilistic risk assessment methods, already developed in other areas of knowledge, have been used in the assessment of railway safety (see [3, 4]), they have not been adapted to the case of railway lines.

As it occurs in many other areas of engineering, human error is the most important factor to be considered in any PSA. On the other hand, quantification of human error probabilities is one of the most difficult problems, which can be solved only with the help of miscellaneous groups of professionals (operators, conductors, railway designers, PSA experts, statisticians, etc.) (see, for example, [5], [6] or [7]).

In this paper we pay special attention to the driver tiredness and attention and how it changes along the line as a function of the driving time, the elements encountered along the line and the help of automatic train protection systems (ATP).

Probabilistic safety analysis of railway lines implies a huge amount of combinations of events (see, for example, [8], [9]). Though fault trees structures (see [10] or [11]) are the most common probabilistic models used in PSA, they have important limitations, specially to consider common causes. Since Bayesian networks have not this limitation, they compete with advantage with fault trees structures as an appropriate tool able to reproduce the random variables involved in the problem. Bayesian networks have no limit in practice to reproduce any statistical or probabilistic dependence structure of the set of variables (see [12]). On the other hand, complex Bayesian network models have been already proposed for probabilistic safety analysis of railway systems by [13] and [14], but with a different orientation. This previous experience is a guarantee when facing the case of railways.

This paper proposes a modern railway line design with a PRA included as an alternative to classical design in which safe operations are guaranteed, but no probabilistic analysis is performed.

In probabilistic safety analysis (PSA) human errors are incorporated and all sequences of events leading to undesired incidents are looked for and, more important, their probabilities of occurrence are estimated in order to guarantee that they are below a small enough threshold value. In this context, Bayesian networks provide an adequate tool to reproduce the random variables and their dependencies not only in their qualitative but in their quantitative aspects.

One of the most difficult steps in Bayesian network construction is the estimation of its high number of parameters. This is a crucial and complicated step that can be done only by a group of experts. To this end, the works [1], [15] and [16], provide important real railway data and a complete statistical analysis of the railway European accidents that occurred during the period 1980-2009, become very relevant.

People working in probabilistic assessment of nuclear power plants, railway lines or highways know about this problem. When undesired events are relatively frequent it is very easy to use standard statistical methods to estimate probabilities of occurrence, however, when events are unfrequent, the associated confidence intervals for the parameters are too wide and we can only have an idea on the order of magnitude of the probabilities of occurrence. There is still an even worse case, in which we need to provide frequencies of occurrence when no previous information exists. In this cases, groups of experts are required to reach a consensus about the required very small frequencies. The long experience in nuclear power plants indicates that in these cases some published tables explaining the type of events being involved and the recommended frequencies for the calculations must be used. Note that more than precise values in these extreme cases we need only an order of magnitude of the risks involved and an idea of how these events can be avoided.

Another important source of information for parameter estimation are the specialized committees with responsibility for investigating railway accidents and their causes and elaborating the corresponding reports and corrections. They exist in many different countries and provide an extremely valuable information for safety analysis.

One of the main sources of motivation for this paper comes from some recent railway accidents which occurred in Spain, in the USA and in France, where excesses of the speed limit in curves and lack of adequate ATP systems were the main causes. An extra motivation comes from the low cost and maintenance alternate double-single track (ADST) lines that we suggested for low demand areas (see [17], [18], [19] or [20]), which suggest a detailed risk analysis must be done, due to the existence of high speed single tracks.

In this paper a PRA methodology is proposed, which uses Bayesian networks (BN) to represent the stochastic structure of the set of all random variables involved in the problem. The following sections describe the set of variables and the links representing direct dependencies among variables, which define the BN qualitative structure, and how the associated conditional probability tables, which reproduce the BN quantitative structure, are defined. Some illustrative examples are also provided. Some uses of these models to highways and roads can be seen in [21], [22] or [23].

This paper is based upon [24], but the current paper includes the following additional research:

1. We discuss in detail how the safety of level crossings can be analyzed in Bayesian networks based on probabilistic safety assessments.

2. We discuss how to incorporate the safety of buffer stops at the end stations in probabilistic safety analyses.

3. We analyze the role of automatic train protection (ATP) systems and how their effect can be limited when other non-protected failures can occur with a large probability.

4. We illustrate the method with new examples.

We finally add that the methodology proposed in this paper is relevant to the probabilistic assessment of railway lines. We also indicate that Bayesian networks outperform clearly to event and fault trees because of the possibility of incorporating common causes without the need of duplications.

2 Variables and items involved in the model

In this section the set of variables used in the model are described (see more details in [19]).

The first step in modelling railway line safety consists of identifying the variables that are relevant to the problem being reproduced. From a safety point of view, the following variables can be identified as relevant:

- *A: Incident.* Since possible incidents can occur at different locations, different instances of this variable type are used at any location where incidents are possible. We assume that they can take the following values: none, minor, medium and severe.

- *S: Automatic Train Protection (ATP) System.* This variable reproduces the supervising system operating at the considered location of the line. Since in some countries the ATP systems can change along the line, we assume that this variable takes the values:“ERTMS”, “ERTMS-ASFA”, “ASFA-dig”, “ASFA-AV”, “ASFA-Conv”, “ASFA-anal”, “SR” (staff responsible).

- *AS: Light signal decision.* At any location where a light signal exists a decision must be taken. So, we consider a variable with possible values: correct, error I (signal at stop announcement), error II (signal at red). These values refer to the particular signal being studied.

- a_t*: Driver’s tiredness.* At any location where a driver’s decision is required we include a driver’s tiredness variable, which has an important contribution to human error and increases with driving time. To simplify, we have assumed that this increase is a deterministic function.

- *M: Driver's attention.* Driver's attention continuously changes with travel time due to the influence of different elements. Thus, we need to reproduce these changes along the line. To this end, driver's attention variables are used at different locations with three possible values: *distracted*, that is, the driver lacks the necessary attention to react when an action is required and no action is observed, *attentive*, that is, the driver reacts adequately to the required actions but with a small probability of error, and *alert*, that is, the driver always makes the correct decision.

- *DA: Driver's decision at signal.* At signal locations where decision are expected, we include a driver's decision variable with possible values: correct, error (incorrect action of the driver). This variable refers only to the driver's intention that can be correct or incorrect.

- *DE: Driver's decision on speed control.* At some locations the train speed must be controlled by the driver. To control the corresponding driver's decision, a speed variable is used with values: correct, error I (speed remains unchanged when it should be changed), error II (selected speed is not the required speed). This variable refers to the actual driver's action.

- *DS: Driver's decision made at a speed limit signal.* It is a similar variable but used for speed limits signals and with values: correct or error I (fail to reduce speed). It refers to the actual driver's action.

- *Inf: Infrastructure.* This variable reproduces the infrastructure state (rails, sleepers, ballast, plate, maintenance standards, etc.), which has an important role on possible undesired infrastructure failures. Its damage levels are: none, minor, medium and severe.

- *RS: Rolling Stock.* It refers to the rolling stock conditions and includes the damage levels: none, minor, medium and severe. Note that incidents due to rolling stock failures can take place.

- *V: Speed.* At different locations, but mainly where speeds must be controlled, we use a speed variable with values in a discrete list $\mathcal{V}$ of values, which in this paper is simplified to a set $\mathcal{V}$ starting from 0 and ending with 280 km/hour with increments of 20 km/hour. However, if at given locations, some particular values not included in this list are of interest, they will replace the closest values in the list.

- *SS: Light signal state.* Where a light signal is present, we use a variable with values: free, stop announcement or stop. This variable reproduces the signal state when the train passes the signal.

- *T: Terrain.* This variable is used to consider the risk associated with falling stones on the infrastructure or slope slidings in cuttings and embankments and takes values: stable, small, medium and high instability. Terrain failures can lead to undesired uncertain incidents, so that they must be reproduced.

- *TF: Technical failure.* It refers to the possibility of a technical failure: yes or no. For example, a brake failure.

The railway to be analyzed contains a set of items that are encountered sequentially when travelling the line. They include: warning, light and speed limit signals, tunnels and viaducts, switches, over or under pass structures, etc. Each item generates a subset of variables with their corresponding dependencies, that is, Bayesian sub-networks. Similarly, the segments between signals also generate sub-networks, as indicated in Figure 1, where these two sets of sub-networks have been differentiated. All of them were adequately connected to generate the global Bayesian network of the whole line.

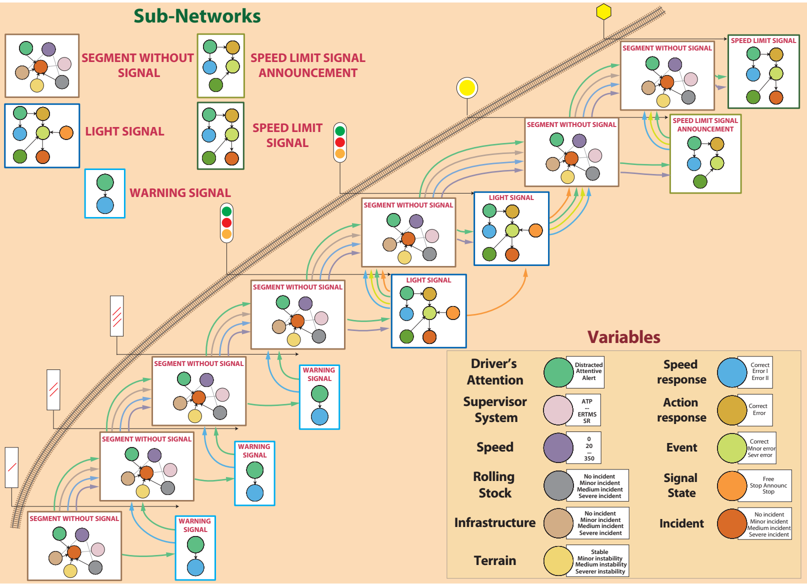


Figure 1: Proposed Bayesian network. Illustration of the Bayesian model showing the subnetworks associated with the different items and segments without signals

The set of all 36 possible combinations of node parents and sons that have been considered in our model are shown in Table 1. This implies that 36 different conditional probability tables need to be defined. In fact we propose 36 closed form formulas for these probabilities.

The following subsections describe some details of the different sub-network components.

2.1 Conditional probability tables

In this section we explain how some of the required conditional probability tables are defined.

2.1.1 M nodes: Driver's attention

The driver's attention M node is connected only to the previous M node if it exists. This means that its states depend on the M node previous nodes states. Their dependencies are modelled by means of a Markov model (see Figure 2) in which the changes from attentive, distracted and alert states are reproduced depending on the location of the corresponding nodes along the line. The sequence of signals, the acoustic alerts received in the cabin, the landscape, etc. have a strong influence on the driver's attention, which must be modelled.

Figure 2 illustrates how the driver's attention oscillates among the three states: alert, attentive and distracted, and the probabilities of any of the possible transitions.

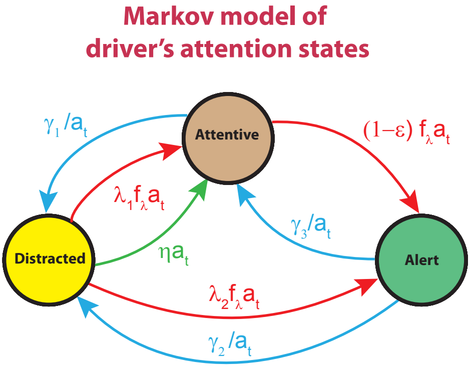

Markov model of
driver's attention states
γ_1/a_t
Attentive
$(1-\varepsilon)\ f_\lambda a_t$
$\lambda_1 f_\lambda a_t$
ηa_t
γ_3/a_t
Distracted
Alert
$\lambda_2 f_\lambda a_t$
γ_2/a_t

Figure 2: Markov model illustrating the transitions among different attention levels showing the transition probabilities for the cases of segments without signals and when a signal is visualized

2.2 Level crossing sub-Bayesian network

In this section we describe in some detail how the level crossings are incorporated to the probabilistic safety analysis.

There are three different types of level crossings:

1. *Protected with or without crossing gate:* In this case the train can circulate at a maximum speed of 155 Km/h.

Node	Parents	Node	Parents
A	M, S, V, RS	RS	-
A	M, S, V, RS, T, Inf	RS	M, S, SS, V
A	SS, M, S, V, RS	RS	M, S, V
A	SS, M, S, V, RS, T, Inf	RS	SS, M, S, V
A	V	RS	V, RS, V
A	V, AS	S	-
AS	S, V, DA, FT, SS	S	M
DA	M	S	S
DE	M	S	SS, M
DS	S, V, DA, FT	T	-
FT	-	V	-
Inf	V, V	V	M, S
M	-	V	M, S, SS
M	M	V	V, DE, DS, M, S
M	SS	V	V, DE, DS, M, S, SS
SS	-	V	V, DE, M, S
SS	M, S	V	V, DE, M, S, SS
SS	SS	V	V, DE, SS, AS, M, S

Table 1: Set of all possible combinations of node parents and sons

2. *Protected with or without crossing gate but with an announced problem:* Since there is a safety problem at the level crossing, the train must reduce its speed such that stop at the level crossing can be possible.

3. *Unprotected:* In this case the train must reduce its speed such that stop at the level crossing is possible in case of any obstruction.

Each level crossing type is announced by the presence of its distinctive signal.

Figure 3 shows the subnetwork associated with the level crossing network, which is formed by a level crossing announcement (left green subnetwork) and at least a level crossing (right green subnetwork).

The level crossing announcement network is shown in Figure 3 and the associated conditional probabilities are given below. They differ only in the controlled speed to which the driver must attain that, as previously mentioned, depends on the level crossing type.

The level crossing subnetwork is modelled as two parts:

- *Level crossing announcement signal.* The first considers the visualization of the level crossing announcement signal, and consequently the driver's attention M is modified and a driver's decision DE is activated.

- *Level crossing itself.* In the second part the incident, node A is analyzed.

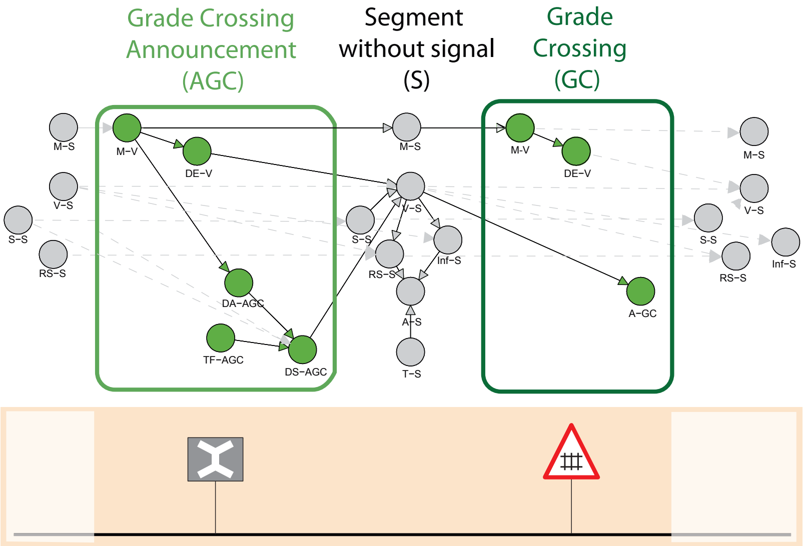


Figure 3: Set of variables involved in the level crossing subnetwork

2.2.1 Level crossing announcement signal

This is described on the left hand side of Figure 3.

We need to define the following conditional probability tables $P(DE|M)$, $P(DA|M)$ and $P(DS|V_p, DA, S, TF)$.

Since the DE node with possible a values $\{correct, error\ I, error\ II\}$ has as its single parent a driver attention node with possible b values $\{distracted, attentive, alert\}$, the conditional probabilities for this node are given by the closed formula:

$$P(DE = a|M = b) = \begin{pmatrix} \delta_{a,1} & \delta_{a,2} & \delta_{a,3} \end{pmatrix} \begin{pmatrix} 0 & 1-(1-\tau_a)a_t & 1 \\ 1 & \theta(1-\tau_a)a_t & 0 \\ 0 & (1-\theta)(1-\tau_a)a_t & 0 \end{pmatrix} \begin{pmatrix} \delta_{b,1} \\ \delta_{b,2} \\ \delta_{b,3} \end{pmatrix} \tag{1}$$

where $\delta_{a,b}$ are the Kronecker's deltas, τ_a is the probability of a correct decision when the driver is attentive and tiredness is null ($a_t = 1$), θ and $1 - \theta$ are the probabilities of making errors I and II, respectively, once an error has been made by the driver, and $a_t > 1$ is the driver's tiredness reduction factor, which is defined as:

$$a_t = \exp\left(\delta t^2\right), \quad t \geq 0 \tag{2}$$

where δ is a parameter, which in the presented examples is assumed to be $\delta = 0.02$. This means that any probability of making right decisions by the driver must be reduced by dividing this value by the corresponding reduction factor a_t.

Since the DA node with possible values $\{correct, incorrect\}$ has as its single parent a driver attention node with possible values $\{distracted, attentive, alert\}$ (see Figure 3), the associated conditional probability $p(DE = a|M = b)$ becomes:

$$p(DA = a|M = b) = \begin{pmatrix} \delta_{a,1} & \delta_{a,2} \end{pmatrix} \begin{pmatrix} 0 & 1-(1-\tau_a)a_t & 1 \\ 1 & (1-\tau_a)a_t & 0 \end{pmatrix} \begin{pmatrix} \delta_{b,1} \\ \delta_{b,2} \\ \delta_{b,3} \end{pmatrix} \tag{3}$$

The node DS with two possible values (correct and error I) refers to the final decision after the driver's signal decision, the action of the ATP system and a possible technical failure. This node has four parents V, DA, S and TF (see Figure 3).

To calculate the values $p_{a,b,c,d,e}$ of the conditional probability

$$p_{a,b,c,d,e} = P(DS = a|V_a = b, DA = c, S = d, TF = e)$$

we define first a speed dependent row $Q^s(b)$ matrix:

$$Q^s(b) = \begin{pmatrix} v(b) < v_{lim} & v_{lim} < (v(b) \leq v_{max} & v(b) > v_{max}) \end{pmatrix} \tag{4}$$

where v_{lim} and v_{max} are the speed limit and the maximum speed that allows the speed limit to be attained, respectively, and whose three elements $q_i^s(b)$ refer to the cases: (a) the speed limit is already satisfied at the signal location, (b) the speed limit is not satisfied but attainable, and (c) the speed limit is unattainable, respectively.

For this node DS we have the following conditional probability:

$$p_{a,b,c,d,e} = \delta_{a,1}p_{1bcde} + \delta_{a,2}(1 - p_{1bcde}) \tag{5}$$

where the probability of a correct decision is

$$p_{1bcde} = (1 - \delta_{e,1})q_2^s(b)(1-\rho(d)\delta_{c,2}) + q_1^s(b) \tag{6}$$

where the three factors in the first term refer to the case of a correct decision DS due to no technical failure (factor $(1 - \delta_{e,1})$), attainable speed limit (factor $q_2^s(b)$) and both correct decision DA and erroneous decision DA but corrected by the supervisor (factor $(1-\rho(d)\delta_{c,2})$). The second term refers to the case of a correct decision because the speed limits are already satisfied.

2.2.2 Level crossing itself

This is described on the right hand side of Figure 3, which shows the accident node A and its parent V in a level crossing.

The conditional probability of the incident node A given the speed node V is given by

$$\begin{aligned} P(A = a|V = b) \quad = \quad & \delta_{a,1}(1 - \varrho F_{N(v_{ref}/2, v_{ref}/4)}(v(b))) \\ & +\delta_{a,2}\varrho(F_{N(v_{ref}/2, v_{ref}/4)}(v(b)) - F_{N(v_{ref}, v_{ref}/4)}(v(b))) \\ & +\delta_{a,3}\varrho(F_{N(v_{ref}, v_{ref}/4)}(v(b)) - F_{N(3v_{ref}/2, v_{ref}/4)}(v(b))) \\ & +\delta_{a,4}\varrho F_{N(3v_{ref}/2, v_{ref}/4)}(v(b)) \end{aligned} \tag{7}$$

where v_{ref} is the reference speed and ϱ is the probability of a obstruction to occur at the level crossing, which both depend on the indicated above type of level crossing.

In Figure 4 the Formula (7) is illustrated, where cdfs of normal random variables have been used to get the accident level but without any probabilistic or statistic interpretation. The vertical line at 53 km/h indicates how the probability associated with the none, minor, medium and severe accidents can be calculated as the length, of different segments in each of the indicated areas. Obviously, they add up to one.

In Formula (7) the four lines correspond to the probabilities of the incident node to take values: none, minor, medium and severe, given the value of node V. The case of $A = none$ takes place in all cases but those in which there is an obstruction, with probability ρ, and this is minor, medium or severe, with probability $F_{N(v_{ref}/2, v_{ref}/4)}(v(b))$, that is, with a probability $1 - \varrho F_{N(v_{ref}/2, v_{ref}/4)}(v(b))$, as indicated.

The case of $A = minor$ takes place if and only if there is an obstruction, with probability ρ, and this is minor, with probability $F_{N(v_{ref}/2, v_{ref}/4)}(v(b)) - F_{N(v_{ref}, v_{ref}/4)}(v(b))$, that is, with a probability $\varrho(F_{N(v_{ref}/2, v_{ref}/4)}(v(b)) - F_{N(v_{ref}, v_{ref}/4)}(v(b)))$, as indicated.

Similarly, the terms in lines three and four correspond to the probabilities of an obstruction and this to be medium or severe.

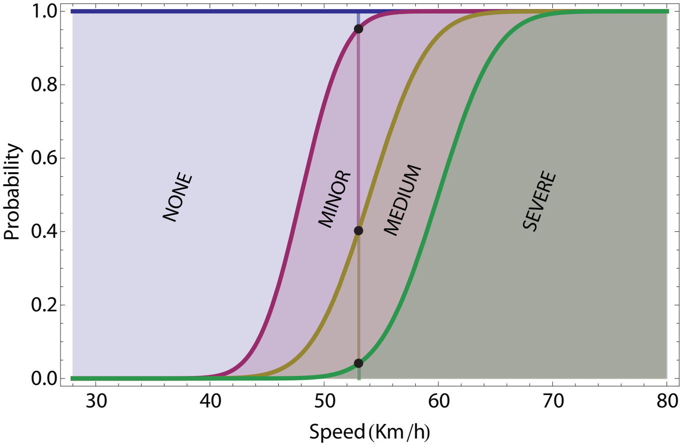


Figure 4: Illustration of the probabilities associated with different accident levels as a function of the speed at the level crossing

2.3 The end station Bayesian subnetwork

This subsection is used to consider incidents at the end station consisting in a collision with the end buffer stops. Figure 5 shows the end station Bayesian subnetwork. There are two Bayesian subnetworks, the one corresponding to the end station announcement signal and the one associated with the buffer stop itself, where the incident can take place.

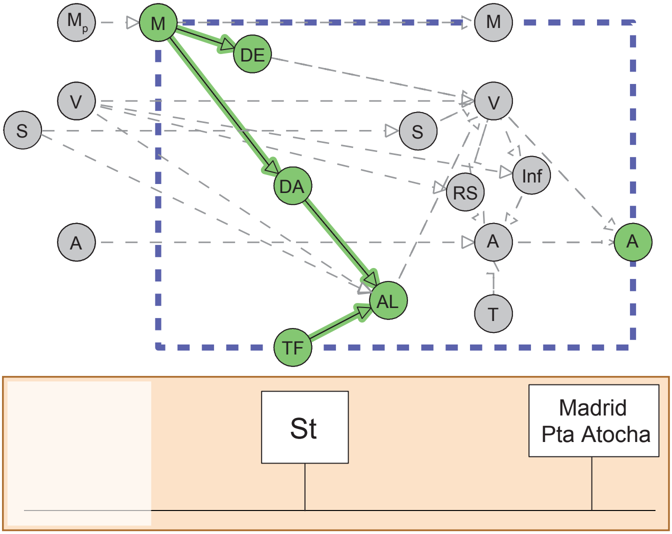


Figure 5: End station sub-Bayesian network

2.3.1 The buffer stop announcement Bayesian subnetwork

This subnetwork is represented on the left hand side of Figure 5 and contains nodes M, DE, DA, TF and AL. The corresponding conditional probabilities are very similar to those described for the level crossing announcement signal.

2.3.2 The buffer stop Bayesian subnetwork

This Bayesian subnetwork, represented on the right hand side of Figure 5, contains a unique node A with one parent V variable and its conditional probability can be written as:

$$P(A = a|V = b) = \delta_{a,1}q_1^s(b) + g(a,b)q_2^s(b), \tag{8}$$

where

$$\begin{aligned} g(a,b) \quad = \quad & \delta_{a,1}(1 - F_{N(v_{minor},\sigma)}(v(b))) \\ & +\delta_{a,2}(F_{N(v_{minor},\sigma)}(v(b)) - F_{N(v_{medium},\sigma)}(v(b))) \\ & +\delta_{a,3}(F_{N(v_{medium},\sigma)}(v(b)) - F_{N(v_{severe},\sigma}(v(b))) \\ & +\delta_{a,4}F_{N(v_{severe},\sigma)}(v(b)), \end{aligned} \tag{9}$$

where v_{minor},v_{medium},v_{severe} are the speeds that produce a minor, medium and severe incident, respectively, at a stop station, and $v(b)$ is the speed associated with speed level b. We consider several types of stations (I intermediate or T terminal station), and σ is the deviation of the cumulative normal distribution.

Figure 6 illustrates the probabilities associated with a collision with buffer stop for the different accident levels as a function of the speed at the end station.

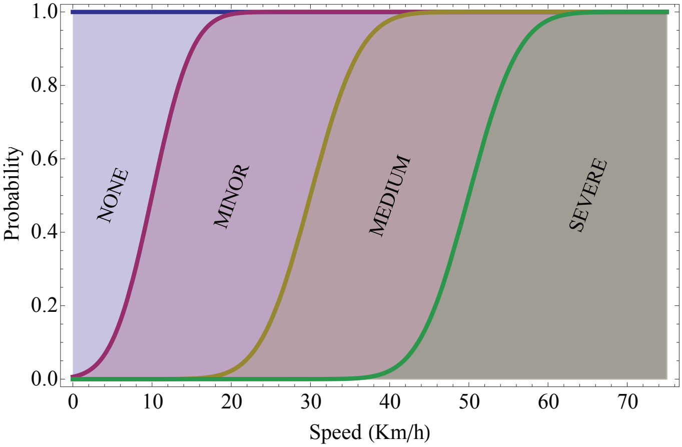


Figure 6: Illustration of the probabilities associated with a collision with buffer stop for the different accident levels as a function of the speed at the end station

3 Network partition

In this section we show how the complexity of the calculations can be reduced by partitioning the networks in small parts.

A real line generates a Bayesian network model with a very high number of variables. To illustrate, the case of the Palencia-Santander line in [14] with a little more than 200 km, contains 7820 variables, a high enough number leading to memory and cpu problems if conventional Bayesian network packages are used.

In order to solve this important problem, [14] presents a powerful technique that allows us to reduce memory and cpu requirements. Its main idea consists in partitioning the Bayesian network in several small subnetworks without altering the quantitative dependence structure in the initial Bayesian network. One example is shown in Figure 7 where the Bayesian network associated with the set of signals indicated in the lower part of the figure is given. The upper plot shows how it can be partitioned into five subnetworks. Note that, in order to keep the dependence structure four and five artificial nodes (duplicated from their previous subnetworks) have been added to the second to fifth subnetworks, respectively, but no node is added to the first one.

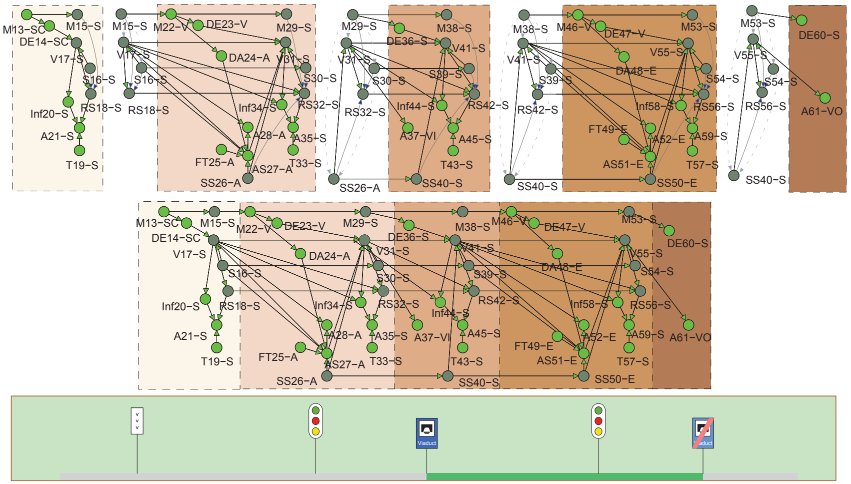


Figure 7: Illustration of how a Bayesian network can be partitioned into a sequence of Bayesian subnetworks to obtain the marginal probabilities (forward process)

The basic idea behind this technique consists of using sets of separators (subset of nodes) such that the conditional probability of the set of posterior nodes becomes independent on the set of previous nodes given the separator subset (see [12]). To facilitate the calculations, some added artificial links are used to convert the separator into a clique. This technique significantly reduces the computation time, and more important, the associated complexity becomes linear in the number of nodes.

Fortunately, and thanks to this technique of partitioning the line in small pieces, without loosing any precision there is no limit in the line scale, because the complexity is linear in the line length. This is one of the main advantages of the proposed method.

4 Examples of applications

To facilitate the understanding of the proposed methodology, some illustrative examples are included in this section. More precisely, we give three basic examples, which have been carefully selected to clarify some of the concepts developed in previous sections.

4.1 Nested permanent and temporal speed limit signals example

In this example we present a case of nested permanent and temporal speed limit signals with the aim of illustrating: (a) the capacity of the Bayesian network to detect design errors, (b) the role of ATP systems in improving the safety of a railway line, and (c) how possible design failures not covered by ATP systems can diminish the relevance of these ATP systems.

The example is described in Figure 8 (second plot from the top) and consists of:

1. A permanent speed limit set of signals, at locations 388.500 (speed limit announcement), 389.800 (mandatory signal) and 390.680 (end of speed limit). It corresponds to the initial line design.

2. A temporal speed limit set of signals, at locations 388.550 (speed limit announcement), 390.350 (mandatory signal) and 390.700 (end of speed limit). It corresponds to some temporal changes in the line.

3. A tunnel located between locations 389.600 and 389.980.

4. A viaduct located between locations 389.990 and 390.200.

5. Two blackspots (possible rock cutting failures close to the track) at locations 390.400 and 390.605.

6. A light signal at location 389.500.

7. An end of speed limit signal at 389.020 and a temporal speed limit announcement at 389.400. It appears that the temporal speed limit (30 km/h) at 388.550 was changed to 60km/h, but the corresponding mandatory signal at 390.350 was not changed from 30 km/h to 60 km/h.

In the top plot of Figure 8 the Bayesian network graph associated with the items above described is shown. The direct dependencies among the different variables are shown providing a clear idea of the qualitative structure of the multidimensional random variable and the role played by each variable.

The input supplied to the computer program for performing the PRA of the nested permanent and temporal speed limit signals example is:

```
Trip = {{'Start', 297.0},...
   {'AnnouncementP', 388.50, 0, 80}, ...
   {'AnnouncementT', 388.55, 0, 30}, ...
   {'SignalFT', 389.02, 0, 30,'To be removed'}, ...
   {'AnnouncementT', 389.4, 0, 60,'To be removed'}, ...
   {'SignalC', 389.500}, ...
   {'TunnelIn', 389.600, 0, 'Tunnel'}, ...
   {'SignalP', 389.800, 0, 80}, ...
   {'TunnelOut', 389.980, 0, 'Tunnel'}, ...
```

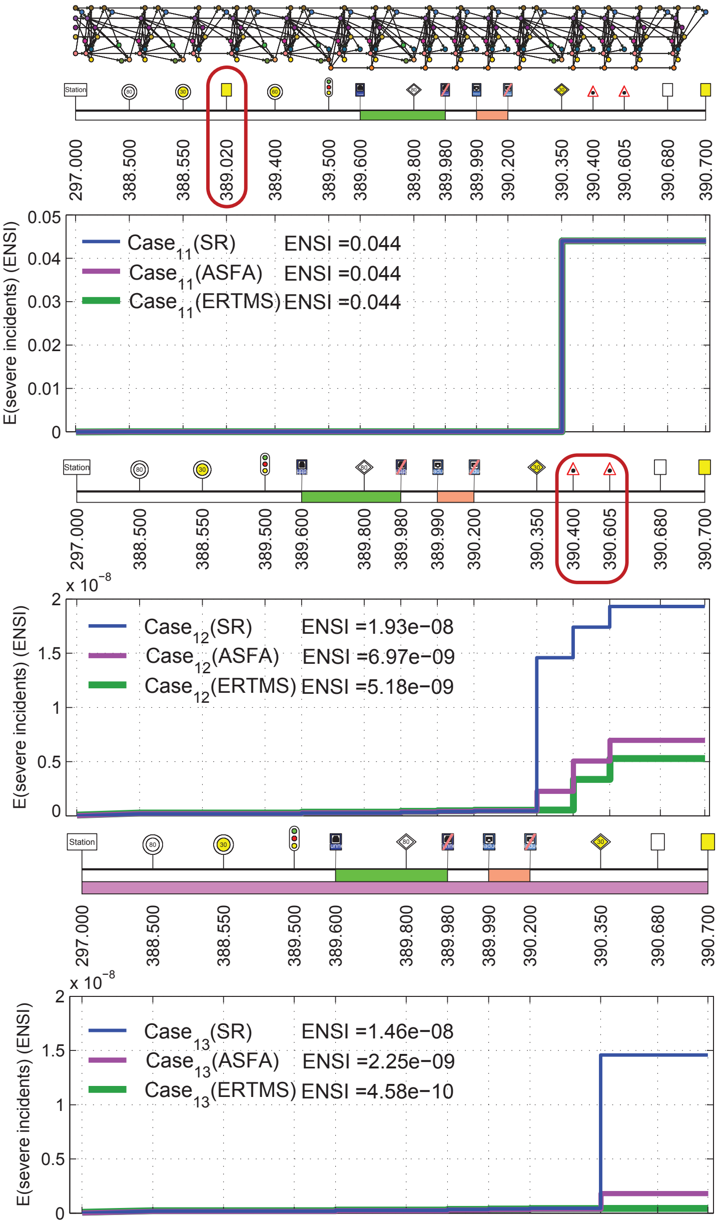


Figure 8: Nested permanent and temporal speed limit signals example

```
    {'ViaductIn', 389.990, 0}, ...
    {'ViaductOut', 390.200, 0}, ...
    {'SignalT', 390.350, 0, 30,'Sin baliza'}, ...
    {'Blackspot', 390.4,3},...
    {'Blackspot', 390.605,2},...
    {'SignalFP', 390.680, 0, 80,'Añadida'}, ...
    {'SignalFT', 390.70, 0, 30}, ...
    };
```

We note that, apart from this information, the values of the model parameters must be given too. To this end, the participation of a group of people and specialists is required so that the parameter values reflect the real behavior of the driver and the line.

The computer program: (a) builds the Bayesian subnetworks, (b) evaluates the expected number of severe incidents, and (c) provides a sorted list, such as the one indicated in Table 2, where the most dangerous items in the line for the cases of SR, $ASFA$ and $ERTMS$ can be identified and corrected if it is necessary.

			Severe Incident Frequency		
item	**item name**	**PK**	**Staff Resp.**	**ASFA**	**ERTMS**
Case11 (With signals and blackspot errors)					
12	SignalT	390.350	0.044	0.044	0.044
13	Blackspot	390.400	4.75e-09	4.75e-09	4.75e-09
14	Blackspot	390.605	1.92e-09	1.92e-09	1.92e-09
Case12 (With blackspot errors)					
12	SignalT	390.350	1.41e-08	1.65e-09	1.4e-11
13	Blackspot	390.400	2.81e-09	2.81e-09	2.81e-09
14	Blackspot	390.605	1.92e-09	1.92e-09	1.92e-09
Case13 (With corrected errors)					
12	SignalT	390.350	1.41e-08	1.65e-09	1.4e-11

Table 2: Critical list: List of items of Case$_1$ (ERTMS) with the corresponding PK, accident nodes and probabilities (local and cumulated)

This computer program has been written by some of the authors of this paper in Matlab. It uses the BNT software for dealing with Bayesian networks, and automatically writes the code for the JavaBayes software (written in Java) in order to perform a double check of the results.

The program uses a specially designed user interface that facilitates the railway line representation, and generates automatically the input data and a report with all the plots and tables of frequencies of incidents sorted by importance. The plots and tables shown in this paper come from this report.

The third plot in Figure 8 shows the cumulative expected value of having a severe incident when travelling the line and passing the different items with a clear indication of where the most safety relevant items are and how these expected values (probabilities) are affected by the ATP systems. In our case, all three ATP situations (staff responsible (SR), and the ASFA and ERTMS systems) point to the mandatory speed limit signal location as the responsible for a high expected value (probability or frequency) (0.044) of a severe incident but lead to the same frequency because this is due to an erroneous design placement of the set of signals, which is not controlled by ATP systems. The reason for such a high value is due to the fact that a speed limit signal of 60 km /h is announced when the real one corresponds to 30 km/h and there is a high chance of not having enough time to reduce the speed.

In the fourth plot from the top the two previous erroneous signals, located at 389.020 and 389.400 have been removed. It can be seen that this correction produces the expected and desired effects, with a significant reduction of expected values (below $1.93e - 08$) in the frequency of a severe incident. We note that the ATP systems reduce this frequency to $6.97e-09$ and $5.18e-09$ for ASFA and ERTMS, respectively.

It is interesting to indicate that the effect of the ATP is much more reduced than expected because of the presence of two blackspots at locations 390.400 and 390.605.

If a repair of the rock environment is done, as shown in the last two plots in Figure 8, the beneficial effects of the ATP are magnified. This is a clear indication of the fact that safety improvements must be addressed first to the items causing the highest probabilities.

4.2 End station buffer stop example

In this example we show an end station buffer stop example in which an inappropriate location of an end of speed limit signal appears to decrease safety.

The example is shown in Figure 9 (second plot from the top) and consists of:

1. A permanent speed limit set of signals, at locations 84.538 (speed limit announcement), 87.273 (mandatory signal) and 89.915 (end of speed limit). It corresponds to the initial line design.

2. Two light signals at locations 86.600 (advanced signal) and 88.953.

3. A final station signal at location 93.600.

4. An end of the line at location 94.600.

In the top plot of Figure 9 the Bayesian network graph associated with the items above described is shown, where the direct dependencies among the different variables are shown providing a clear idea of the qualitative structure of the multidimensional random variable and the role played by each variable.

The third plot in Figure 9 shows the cumulative expected value of having a severe incident when travelling the line and passing the different items with a clear indication of where the most safety relevant items are and how these expected values (probabilities) are affected by the ATP systems. In our case, all three ATP situations (staff

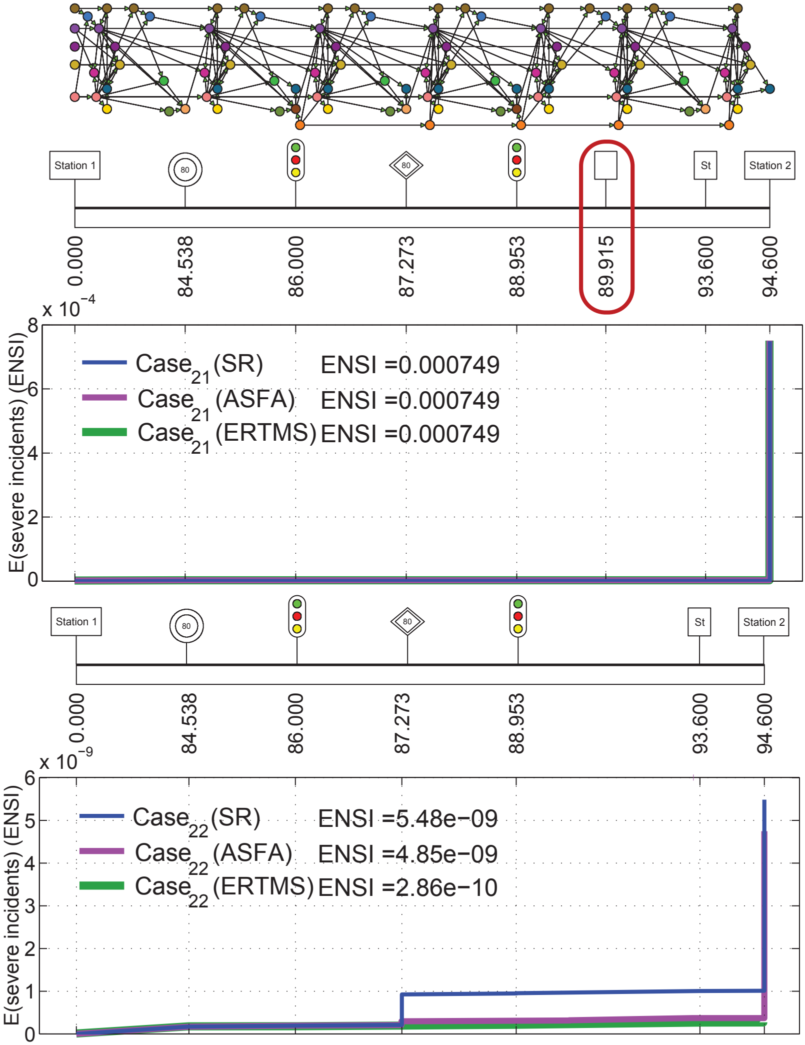


Figure 9: End station buffer stop example

responsible (SR), and the ASFA and ERTMS systems) point to the mandatory speed limit signal location as the responsible for a rather high expected value (probability or frequency) (0.000749) of a severe incident but lead to the same frequency because this is due to an erroneous placement of the end of speed limit signal, which is not controlled by ATP systems. The reason for such a high value is due to the fact that when seeing an end of speed limit signal the driver is invited to increase the speed and this is not indicated here because of the end station proximity.

In the fourth plot from the top the end of speed limit signal located at 89.915 has been removed. It can be seen that this correction produces the expected and desired effects, with a significative reduction of severe incident expected values (below $5.48e-09$) in the frequency of a severe incident. We note that the ATP systems reduce this frequency to $4.85e-09$ and $2.86e-10$ for ASFA and ERTMS, respectively.

It is interesting to indicate that the effect of the ATP in this case is limited because of the possibility of an error at location 87.273, where the mandatory speed limit signal is located.

We finally note that frequencies below $10e-09$ are recognized by the RSSB (Rail Safety and Standards Board) as a very low frequency below which we should not be concerned.

4.3 Level crossing example

In this final example the safety associated with a level crossing is analyzed. The example is described in Figure 10 (second plot from the top) and consists of:

1. A tunnel located between locations 2.835 and 3.185.
2. A level crossing announcement signal located at 10.150.
3. A level crossing located at 12.000.
4. A viaduct located between locations 21.150 and 21.850.

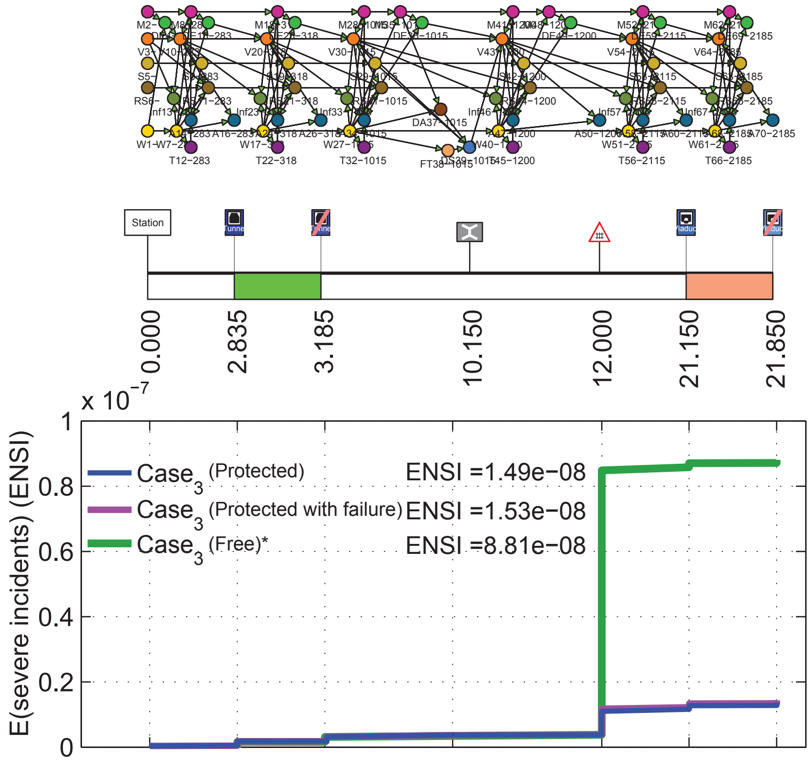
In the top plot of Figure 10 the Bayesian network graph associated with the items above described is shown. The direct dependencies among the different variables are shown providing a clear idea of the qualitative structure of the multidimensional random variable and the role played by each variable.

The third plot in Figure 10 shows the cumulative expected value of having a severe incident when travelling the line and passing the different items with a clear indication of where the most safety relevant items are and how these expected values (probabilities) are affected by the level crossing type. In our case, all three ATP situations (staff responsible (SR), and the ASFA and ERTMS systems) provide very similar results.

The results point to the free or unprotected level crossing as the most dangerous ones, with frequencies of severe incidents that can be up to more than 6 times for unprotected level crossings when compared with protected ones.

In addition, it can be seen that the frequencies of severe incidents associated with tunnels and viaducts are much smaller than those associated with level crossings.

As indicated, the parameter values of the model must be estimated based on existing data, the opinion of experts and mainly by validation. Our experience reflects that when erroneous values (very high or very low) are selected, the resulting number



* Without previous announcement

Figure 10: Level crossing example

of expected corresponding events has no sense (too high or too low) and you can immediately correct them. In fact we have used this methodology to reach reasonable estimates for some parameters related to very unusual events.

4.4 Real cases

The examples in the previous section were small illustrative examples that facilitate the understanding of how the proposed model works. However, this methodology has also been applied to several real lines including the Palencia-Santander, the Vitoria-Zaragoza and the Pamplona Castejón lines in Spain and the Dublin-Cork in Ireland, involving several thousands of variables. Unfortunately, due to confidentiality reasons, we cannot provide specific details. However, we can indicate that in the sorted list of the most risky elements found in our analysis, some events and sequences of events were identified that in our opinion would be hardly identified by other means. In the opinion of independent railway experts the identification and the corresponding quantification of failure probabilities of all events can be considered as relevant findings with respect to safety of the analyzed railway lines.

When the proposed method was used to evaluate the Santiago accident, causing 80 casualties, it was able to detect the need of a correction at the accident location, that almost surely could have avoided the accident.

4.5 Final comments

First, the partitioning technique is not an approximate but an exact method to calculate probabilities in the whole Bayesian network. Thus, with sufficient precision, the results associated with using or not the partition technique must be the same. However, due to the reduction in complexity, the results could be more precise with the partitioning technique.

Second, the complexity associated with the use of the partitioning technique is linear in the length of the line. In fact, this is possible because the railway line is linear itself, but this is normally not exploited by standard methods used in Bayesian networks, as can be demonstrated using standard software packages.

Finally, we have used this method in several real lines, and have had no problem at all with the length of the lines. We have experimentally proved that CPU time increases linearly with the line length. Even though we have analyzed long lines with our computer program (not optimized for CPU time) the calculations never reached 30 minutes.

5 Conclusions

The following conclusions can be drawn from the above analysis and considerations:

1. Bayesian networks permit the reproduction of the railway line structure and to quantify the probabilities of undesired events. The Bayesian network structure is obtained in a very natural way by simply identifying and reproducing all elements that are encountered when travelling the line and that jeopardize safety.

2. As it has been shown in this paper, the required conditional probability tables of the son variables given the parent variables can be obtained in closed form. This, apart from permitting a simpler sensitivity analysis, facilitates the Bayesian network construction.

3. The proposed method allows us to integrate human errors, which are demonstrated crucial in railway safety, with other variables in the model. In particular, the driver's tiredness and attention variables and decision variables, where

different types of errors can be included. This permits the evaluation of the associated probabilities of occurrence and their influence on other variables.

4. Thanks to the proposed partitioning technique, Bayesian networks associated with large railway lines can be partitioned in small networks. This leads to an important complexity reduction. More precisely, the resulting complexity increases linearly (instead of non-linearly) with the number of items in the line. Otherwise, the cpu times required to solve real problems can become prohibitive.

5. The examples given in this paper show that the highest risk locations can be easily identified, so that any corrections can be directly addressed to the adequate items with important savings in costs.

6. Application of the proposed methodology to the case of real lines (not given in the paper) has shown that interesting sequences of failures can be identified and their probabilities of occurrence evaluated. Once corrections are introduced, use of the model permits guaranteeing that the line satisfies the required safety level.

References

[1] R.I. Muttram, “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, 2002.

[2] C. Martani, N. Papathanasiou, B.T. Adey, “A review of the state-of-the-art in railway risk management”, *Journal of Railway*, 10(1):5–11, 2017.

[3] G. Bearfield, W. Marsh, “Generalising event trees using Bayesian networks with a case study of train derailment”, *Lecture Notes in Computer Sciences*, 3688:52–66, 2005.

[4] F. Flammini, S. Marrone, N. Mazzocca, V. Vittorini, “Modeling system reliability aspects of ertms/etcs by fault trees and Bayesian networks”, In *17th European Safety and Reliability Conference (ESREL)*, 2675–2683, 2006.

[5] N. Dadashi, A. Scott, J.R. Wilson, A. Mills, *“Rail Human Factors: Supporting reliability, safety and cost reduction”*, CRC Press, Taylor and Francis, London, 2013.

[6] J. Wreathall, E. Roth, D. Bley, J. Multer, “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 02142, June 2003.

[7] M.P. Zeilstra, R. van del Weide, “Human as an asset in a system consideration on the contribution of humans to system performance and system safety”, In *Rail Human Factors: Supporting reliability, safety and cost reduction*, 473–482, 2013.

[8] D. Mizutani, B.T. Adey, C. Martani, M. Burkhalter, V. Ramdas, “Initial investigations into the use of three heuristic algorithms to determine optimal interven-

tion programs for multiple railway objects", *International Journal of Architecture, Engineering and Construction*, 6(3):1–20, 2017.

[9] N. Papathanasiou, B.T. Adey, C. Martani, "Risk assessment process for railway networks with focus on infrastructure objects", In *1st Asian Conference on Railway Infrastructure and Transportation*, 2016.

[10] Y. Lahrech, "Development and application of a probabilistic risk assessment model for evaluating advanced train control technologies. Master thesis, Massachussetts Institute of Technology, Cambridge, Massachusetts, February 1999.

[11] M. Burkhalter, C. Martani, B.T. Adey, "Determination of risk reducing intervention programs for railway lines and the significance of simplifications", *Journal of Infrastructure Systems*, (04017038):1–17, 2018.

[12] E. Castillo, J. M. Gutiérrez, A. S. Hadi, *"Expert Systems and Probabilistic Network Models"* Springer Verlag, New York, 1997.

[13] E. Castillo, A. Calviño, Z. Grande, S. Sánchez-Cambronero, I. Gallego, A. Rivas, J.M. Menéndez, "A Markovian-Bayesian network for risk analysis of high speed and conventional railway lines integrating human errors", *Computer Aided Civil and Infrastructure Engineering*, 31(3):193–218, 2016.

[14] E. Castillo, Z. Grande, A. Calviño, "Bayesian networks based probabilistic risk analysis for railway lines", *Computer Aided Civil and Infrastructure Engineering*, doi: 10.1111/mice.12195(31):681–700, 2016.

[15] S.J. Kokkings, "Case studies in collision safety", Report DOT/FRA/ORD-96/01, Federal railroad administration, Washington, D. C., August 1997.

[16] A.W. Evans, "Fatal train accidents on Europe's railways: 1980-2009", *Journal of Accident Analysis and Prevention*, 43(1):391–401, 2011.

[17] E. Castillo, I. Gallego, S. Sánchez-Cambronero, J.M. Menéndez, A. Rivas, M. Nogal, Z. Grande, "An alternate double-single track proposal for high-speed peripheral railway lines", *Computer Aided Civil and Infrastructure Engineering*, 30:181–201, 2015.

[18] E. Castillo, Z. Grande, P. Moraga, M. Nogal, A. O'Connor, "Alternate double single track proposals for low demand high-speed railway lines", In J. Pombo, editor, *Proceedings of the Third International Conference on Railway Technology: Research, Development and Maintenance*, number Paper 283, Stirlingshire, UK, 2016. Civil-Comp Press, doi:10.4203/ccp.110.283

[19] E. Castillo, Z. Grande, P. Moraga, J. Sánchez-Vizcaíno, "A time partitioning technique for railway line design and timetable scheduling and for re-scheduling due to disruptions", *Computer Aided Civil and Infrastructure Engineering*, DOI: 10.1111/mice.12194, 2016.

[20] E. Castillo, Gallego I., J.M. Ureña, J.M. Coronado, "Timetabling optimization of a mixed double- and single-tracked railway network", *Applied Mathematical Modelling*, 35:859–878, 2011.

[21] Z. Grande, E. Castillo, E. Mora, H.K. Lo, "Highway and road probabilistic safety assessment based on bayesian network models", *Computer-Aided Civil and Infrastructure Engineering*, 32(5):379–396, 2017.

[22] E. Castillo, Z. Grande, E. Mora, H.K. Lo, X, Xu, "Complexity reduction and

sensitivity analysis in road probabilistic safety assessment bayesian network models", *Computer-Aided Civil and Infrastructure Engineering*, 32(7):546–561, 2017.

[23] E. Castillo, Z. Grande, E. Mora, X. Xu, H.K. Lo. "Proactive, backward analysis and learning in road probabilistic bayesian network models", *Computer-Aided Civil and Infrastructure Engineering*, 32(10):820–835, 2017.

[24] E. Castillo, Z. Grande, A. Calviño, M. Nogal, and A. O'Connor. Probabilistic safety analysis of high speed railway lines including human errors. In J. Pombo, editor, *Proceedings of the Third International Conference on Railway Technology: Research, Development and Maintenance*, number Paper 73, Stirlingshire, UK, 2016. Civil-Comp Press, doi:10.4203/ccp.110.73