360.revista de alta velocidad
número 5 - junio - 2018. Pág 125 - 147

Probabilistic Safety Analysis of High Speed and Conventional Railway Lines

Grande, Zacarías
Blanco López, Marta
García Tamames, Alberto
Castillo, Enrique

University of Cantabria[1]
Spanish Royal Academy of Engineering

Abstract:

A probabilistic safety analysis methodology based on Bayesian network model is presented, in which all the elements encountered when travelling along a railway line, such as terrain, infrastructure, tunnels, viaducts, light signals, speed limit signs, curves, switches, rolling stock, and any other element related to its safety are reproduced. Especial attention is given to human error and modelling the driver behaviour variables and their time evolution. The conditional probabilities of variables given their parents are given by means of closed formulas, which facilitate the software implementation of the proposed models. The model provides a probabilistic safety assessment of the line such that its most critical elements can be identified and sorted by importance. This permits improving the line safety and optimizing the maintenance program by concentrating on the most critical elements. To reduce the complexity of the problem, a method is given that divides the Bayesian network into small parts such that the complexity of the problem becomes linear in the number of items. In addition, when an accident occurs, a backward inference process allows us to identify the causes of incidents. The case of the real Palencia–Santander and Vitoria-Zaragoza lines together with some other simple examples are used to illustrate the advantages of the proposed methodology.

Keywords: Bayesian networks, Backward analysis, Partition technique.

[1] *Grande, Zacarías. University of Cantabria. Email: zgandrade@gmail.com*
Blanco López, Marta. University of Cantabria. Email: marta.blancolo@alumnos.unican.es
García Tamames, Alberto. University of Cantabria. Email: alberto.garciat@alumnos.unican.es
Castillo, Enrique. Founder Member of the Spanish Royal Academy of Engineering. Email: castie@unican.es

1. Introduction and motivation

Probabilistic safety analyses are mandatory and used regularly in the safety assessment of nuclear power plants because of the serious implications of nuclear accidents. However, this type of analysis is not mandatory in the case of railway lines. In this paper the convenience of performing probabilistic safety assessments of railway lines is analyzed and seriously recommended following the trend of introducing new computational methods in Railway lines initiated by (Amit & Goldfarb, 1971) (Assad, 1980), (Burdett & Kozan, 2010) (Cacchiani & Toth, 2012), (Caprara, et al., 2002) (Carey, 1994) (Carey & Crawford, 2007) (Carey & Lockwood, 1995), (Castillo, et al., 2015) (Castillo, et al., 2011) (Castillo, et al., 2009) (Castillo, et al., 2016) (Cordeau, et al., 1998) (D'Ariano & Pranzo, 2004) (D'Ariano, et al., 2007) (Haghani, 1987) (Haghani, 1987) (Lin & Ku, 2013) (Ouyang, et al., 2009) (Pachl, 2014) (Petersen, et al., 1986) (Sahin, 1999) (Yang & Hayashi, 2002), etc.

The actual protocols to evaluate risk in railway lines start with an evaluation of each possible hazardous event to decide whether or not the associated combination of frequency of occurrence and consequences is important enough to deserve a detailed analysis of such event and decide the required actions if needed. In this context, Table 1 of Risk Assessment, which is taken from the European Standard 50126 and the Spanish UNE-EN-50126, is used.

Table 1 Risk levels considered in the European safety analysis of railway lines

Frequency of occurrence of hazardous event	Risk level			
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	I ntolerable
Occasional	Tolerable	Undesirable	Undesirable	Intolerable
Remote	Insignificant	Tolerable	Undesirable	Undesirable
Improbable	Insignificant	Insignificant	Tolerable	Tolerable
Incredible	Insignificant	Insignificant	Insignificant	Insignificant
	Insignificant	**Minimum**	**Critical**	**Cathastrophic**
	Severity levels of hazard consequences			

Table 1 shows the different risk levels considered in the European and Spanish standards. Though the word risk is normally associated with the probability of occurrence of an event, here the concept of risk is actually the expected damage (product of the probability of occurrence of the event by the damage produced). Since both the frequencies and the severity levels are given by a rather imprecise terminology, in Table 2 the frequency levels according to the ADIF methodology are explained. Although each frequency is defined in two different ways, it is still very imprecise and can lead to different interpretations by different experts, which means that two different experts may assign a different level of frequency and risk level to the same undesirable event. As we shall see, this is rather serious because of its negative consequences on safety.

Table 2 Sets of frequencies used in the standards

Frequency	Description
Frequent	It may happen frequently. The threat will be played continuously.
Probable	It will happen several times. The threat can often be expected to occur.
Occasional	It may happen several times. The threat can be expected to occur several times.
Remote	It may occur during the system life cycle. It can be reasonably assumed that the threat will occur.
Improbable	Slight chance but possible. It can be assumed that the threat can occur exceptionally.
Incredible	Extremely unlikely. It can be assumed that the threat will not occur.

For example, when referring to events that occur frequently or several times, it is not indicated if this refers to one day, one month, one year or the life of the system being analyzed. Similarly, the meaning of slight chance or extremely unlikely are not quantified, which is the only way of avoiding a misinterpretation of the codes.

Once frequencies and severity levels of their consequences of given events are determined, Table 1 allows to determine the risk levels, which can be classified as: Intolerable, Undesirable, Tolerable, and Insignificant.

Table 3 shows the required action to be taken under any risk level, which has a relevant role in the safety assessment of hazardous events. Thus, careful attention must be paid to the different actions to be carried out for each risk level: “Intolerable”, “Undesirable”, “Tolerable” and “Insignificant”, resulting from the combinations of the different frequencies (“Frequent”, “Probable”, “Occasional”, “Remote”, “Unlikely”, or “Incredible”) and severity levels (“Insignificant”, “Minimum”, “Critical” or “Catastrophic”).

Table 3 Required actions associated with the different risk levels

Risk level	Required action
Intolerable	It must be removed
Undesirable	It will be accepted only when the risk reduction is impracticable and in agreement with the Railway Authority (ADIF)
Tolerable	Acceptable with proper control and in agreement with the Railway Authority (ADIF)
Insignificant	Acceptable without any agreement

It is surprising that in Table 1 the levels of “Critical” and “Catastrophic” risk associated with an “Incredible” frequency are associated with an “insignificant” level of risk, that is, a risk acceptable without any agreement. Even “Critical” and “Catastrophic” risk levels associated with “Improbable” occurrence frequencies are associated with a “Tolerable” risk level, that is, acceptable with adequate control. Therefore, events that are "Incredible", that is, extremely unlikely or that it can be assumed that the threat will not occur, are exempted from further verification regardless of their consequences. Events that are "improbable," that is, unlikely but possible or that the threat can be assumed to occur exceptionally, are tolerable under control even if they have very serious consequences.

This highlights the danger of using not only vague and inaccurate, that is, unquantified or grossly quantified frequencies, but also imprecise boundaries between events requiring a safety analysis and those free of it. In other words, it is clear that this methodology, despite of being a recommendation of the European authorities, is not only the most appropriate but should be corrected as soon as possible.

Fortunately, there are recommendations that already correct these defects, such as, for example, the important work of (Beales, 2002). Given that these recommendations imply a major change of the initial content of the rules, in fact they indirectly recognize their serious deficiencies. Thus, an urgent change of the current code is needed.

For the sake of illustration, Table 4 is the table for risk assessment recommended in the document published by the RSSB (Railway Safety Standards Board), which leads to safety analysis of many events not included in Table 3.

Table 4 Table for risk assessment recommended in the document published by the RSSB (Railway Safety Standards Board).

		Consequence				
		2	3		4	5
Frequency		Fatalities/event				
		1 fatality in every 125 events	1 fatality in every 25 events	1 fatality in every 5 events	1 fatality in every event	5 fatalities in every event
	No/year	0.008	0.04	0.2	1	5
7	31.25	0.25 8	1.25 9	6.25 10	31.25 11	156.25 12
6	6.25	0.05 7	0.25 8	1.35 9	6.25 10	31.25 11
5	1.25	0.01 6	0.05 7	0.25 8	1.35 9	6.25 10
4	0.25	0.002 5	0.01 6	0.05 7	0.25 8	1.35 9
3	0.05	0.0004 4	0.002 5	0.01 6	0.05 7	0.25 8
2	0.01	0.00008 3	0.0004 4	0.002 5	0.01 6	0.05 7
1	0.002	0.000016 2	0.00008 3	0.0004 4	0.002 5	0.01 6
Units are fatalities per year						

Note that in Table 4 the frequencies and severity levels of consequences are classified as levels 1 to 7 and 1 to 4, respectively.

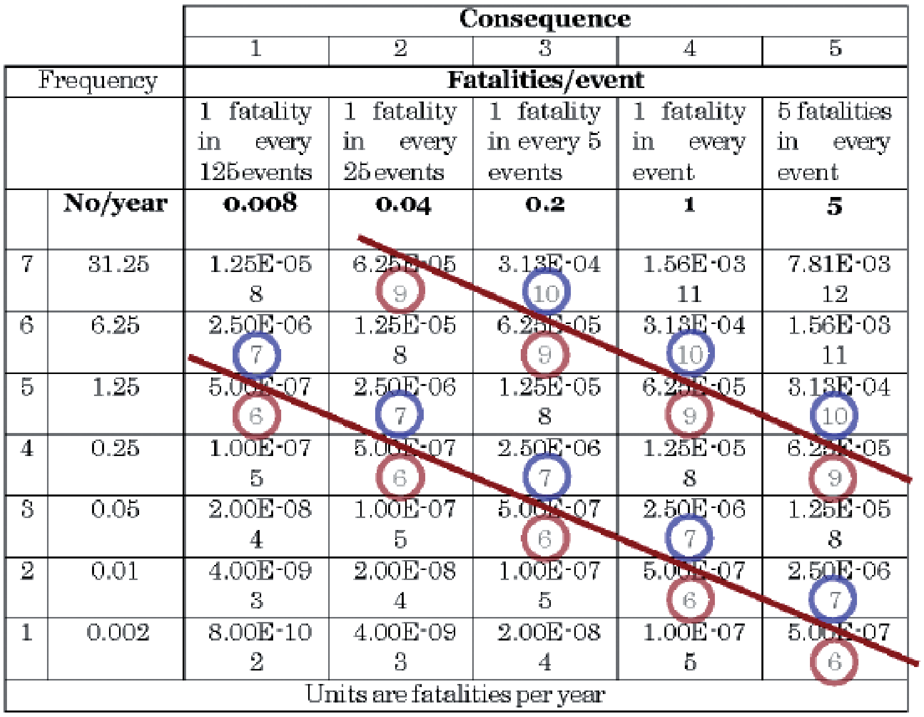
Note that both, frequencies and consequences are quantified in levels related by a factor of 5. In addition, to assign numerical risks of each frequency-consequence combination, instead of multiplying the two row and column entries, they add the levels (exponents of power 5), on the basis that the power product of the same basis is another power with the same basis and the sum of the exponents. In other words, the indices contained within each of the central cells, which take integer values between 2 and 11, are the sum of the levels of their row and column.

Table 4 with the entries multiplied by a factor, which depends on the particular event being analyzed, and two threshold values allows classifying the individual risk, measured in probability of fatality per year, into three regions (see Table 5): the region where risk must be removed, the region where the risk must be mandatory analyzed in detail and the region where no further action is required. One example is Table 5, where the event refers to an accident of a commuter assuming 500 journeys per year and 10E+06 passenger journeys per year. This means that the cell in Table 4, with Frequency 7 and consequence 1, that is, a risk level of 0.25 fatalities per year corresponds:

$$\frac{0.25}{10^6} \cdot 500 = \ 1.25 \cdot 10^5 \text{ fatalities/passenger/year,}$$

Which is the value in the same cell of Table 5

Table 5 Table for risk assessment recommended in the document published by the RSSB (Railway Safety Standards Board).



		Consequence				
		1	2	3	4	5
Frequency		Fatalities/event				
		1 fatality in every 125events	1 fatality in every 25 events	1 fatality in every 5 events	1 fatality in every event	5 fatalities in every event
	No/year	**0.008**	**0.04**	**0.2**	**1**	**5**
7	31.25	1.25E-05 8	6.25E-05 9	3.13E-04 10	1.56E-03 11	7.81E-03 12
6	6.25	2.50E-06 7	1.25E-05 8	6.25E-05 9	3.13E-04 10	1.56E-03 11
5	1.25	5.00E-07 6	2.50E-06 7	1.25E-05 8	6.25E-05 9	3.13E-04 10
4	0.25	1.00E-07 5	5.00E-07 6	2.50E-06 7	1.25E-05 8	6.25E-05 9
3	0.05	2.00E-08 4	1.00E-07 5	5.00E-07 6	2.50E-06 7	1.25E-05 8
2	0.01	4.00E-09 3	2.00E-08 4	1.00E-07 5	5.00E-07 6	2.50E-06 7
1	0.002	8.00E-10 2	4.00E-09 3	2.00E-08 4	1.00E-07 5	5.00E-07 6
Units are fatalities per year						

Note also that the limit between “Tolerable” and “Intolerable”, indicated by the line in red, is between 9 and 10 and that the limit between “Acceptable” and “Tolerable”, indicated by the bottom line in red, is between 6 and 7.

Consequently, the above Table 4 significantly improves the European standard 50126 and the Spanish standard UNE-EN-50126, since:

1. It uses seven frequency levels instead of six.
2. Quantifies the frequencies accurately.
3. It uses frequency levels (proportional to 5^n where n is the level) that multiply by five the frequencies of the previous ones, which allows levels to be associated with frequencies, that is, qualitative with quantitative information, which does not occur neither in European standard 50126 nor in the Spanish UNE-EN-50126.
4. Quantifies the consequences in terms of deaths and using also a factor 5 to pass level, which avoids ambiguities.
5. Declassifies as “acceptable without any agreement” (“Negligible risk”) low frequency cases with serious consequences

Nevertheless, the use of tables, such as Table 5, can also be criticized because they provide a risk per year and this depends on the number of trips per year and its length (the larger the number of trips and its length, the larger the risk). In other words, using this yearly risk discriminates the different events by length and number of trips. In our opinion the risk must be given in fatalities per kilometer. The fact that a user travels more time per year or uses longer or shorter trips should not change the required safety level.

The most important conclusions that can be deduced from the above are:

1. The European standard 50126 and the Spanish UNE-EN-50126 are not the most appropriate, and if used could easily lead to the conclusion that the risks associated with the event, “very unlikely with serious consequences” are “acceptable without any agreement”, that is, do not need a safety analysis, if such event had been considered “Incredible.”
2. This will not occur in the case of using the recommendations indicated by the RSSB, or more modern methodologies, such as those based on fault trees or in Bayesian networks.
3. The imposition of the ADIF methodology, based on European and Spanish regulations, as the only accepted ones, giving as a reason the difficulty of comparing results if different methods were used, should be eliminated, or at least thoroughly reviewed, by the risks which can be overlooked in its application, which is also mandatory.
4. Finally, the risk should be given by km and not per year.

2. Probabilistic Safety Analysis (PSA)

Once the need of a detailed probabilistic safety analysis (PSA) has been detected we have to identify all possible risks and proceed to evaluate the whole risk of the line. To this end, we can use the above method, which is very cumbersome or use an alternative.

In this paper we present a method to simplify the process based on Bayesian networks, which can be used as the main tool for probabilistic representation of multidimensional variables in order to analyze railway safety.

The methodology of the model can be summarized in different stages described below:

The first step is to identify and reproduce the most relevant variables that play an important role in the safety of a railway line to model its multidimensional random behavior.

The second stage consists of reproducing the elements that the driver and the train observe when they travel along the line. Particularly, we reproduce the evolution of the level of attention of the driver, the speed and occurrence of incidents.

2.1 Proposed Bayesian network model

2.1.1 Introduction

As event trees and fault trees, although very powerful present some important limitations, Bayesian networks have been selected, given the previous experience of the authors in this very important tool of representation of the probabilistic structure of multidimensional random variables.

A Bayesian network consists of two elements: A directed acyclic graph and a set of conditional probability tables. In this way, any joint multidimensional probability can be reproduced with no restriction, which implies being able to treat any multidimensional random variable. To properly perform a Probabilistic Safety Analysis (PSA) it is convenient to use the following stages: The first requires to identify and reproduce all the items or elements which are relevant to the safety of a railway line. The second stage must identify the variables that influence the elements previously described and how they influence them. In particular, the evolution of the driver's level of attention (variables M), speed (V variables), the presence of signals of all kinds, tunnels, viaducts, occurrence of accidents (variables A), etc. are required. Finally, the third step must be devoted to define the structure of the model and quantify the conditional probabilities.

With this aim, a video from the train's cabin recording the railway line becomes an essential tool to identify all these possible hazardous items that the engineer encounters when travelling along the railway line. Some elements that can be considered are crossing switches, tunnel crossings, cutting and embankments, viaducts, infrastructure crossings (overpass and underpass), level crossings, landslides, etc. not forgetting the light signals and signs of speed limitations, since a large distance is required to be able to reduce the speed and errors are not always protected by the automatic protection systems (ATP).

2.1.2 Variables used in the model

From the previous discussion, we can identify the following list of variables that are very important to the line safety:

1. *Tr: Driver's tiredness*. Since the driver is subject to an increase of tiredness with driving time a variable is needed to analyze how it changes along the line when travelling. Since tiredness is known to be one important contribution to human error, it must not be forgotten.
2. *D: Driver's attention.* It refers to the driver's attention level that in our model is simplified to three states: distracted, attentive and alert. We assume that an alert situation always leads to a correct decision and that a distracted situation leads to a no action at all. Contrary, an attentive situation is subject to both correct and incorrect actions with given probabilities, such that the probability of the first is much bigger that the probability of the second.

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 (for example, after seeing a warning signal or consulting the railway driver's guide, etc.).

The evolution of driver's attention when driving progresses and different elements along the line encountered must be considered.

3. *S: Speed* It refers to the train speed at the corresponding location and can take a discrete list of values. In the examples considered in this the- sis we have simplified the model using the following list of values.
4. *A: Accident*. It refers to the accident occurrence at the actual location or before and can take the following values: none, minor, medium and severe.

   The model assumes that once an accident has occurred at a given location, no accidents can take place in any other forward location.
5. *RS: Rolling Stock*. It refers to the rolling stock conditions and includes the damage levels: none, minor, medium and severe.
6. *Inf: infrastructure.* With this variable the infrastructure state (rails, sleepers, ballast, plate, maintenance standards, etc.) is considered, and it includes the following damage levels: none, minor, medium and severe.
7. *T: Terrain.* This variable is used to consider the risk associated with falling stones on the infrastructure or slope sliding in cuttings and embankments and takes values: stable, small instability, medium instability and high instability.
8. *DE: Driver's decision on speed control*. It refers to the decision made when speed is controlled by the driver, and includes the following levels: correct, error I (speed remains unchanged), error II (selected speed does not coincides with required speed).
9. *DA: Driver's decision at signal.* It refers to the decision made when the train encounters a signal, and includes the following levels: correct, error (incorrect action of the driver).
10. *ATP: Automatic Train Protection System.* This variable refers to the supervising or driving assistance system operating at the considered point of the line. It takes the values:"ERTMS", "ERTMS-ASFA", "ASFA-dig", "ASFA-AV'', "ASFA-Conv", "ASFA- anal", "SR" (staff responsible).
11. *AS: Light signal Decision.* It refers to the possible errors at a light signal: none, error I (stop announcement signal), error II(signal at red).
12. *DS: Driver's decision made at a speed limit signal.* It refers to the possible errors made by the driver at a speed limit signal: none or error I (fail to reduce speed).
13. *SS: Light signal state.* It refers to the light signal: free, stop announcement, stop.
14. *TF: Technical failure.* It refers to the possibility of a technical failure: yes or no. For example, if the driver tries to stop the train and the brakes fail.

2.1.3 Markovian Model

To analyze the driver's attention, we propose a Markovian model that considers only three driver's attention states (distracted, attentive and alert) (see Figure 1). "Distracted" means that the driver does nothing, “alert” means that the driver makes correct decisions, that is, without error, and, finally, “attentive” implies normally a correct decision but some errors with a very small probability.

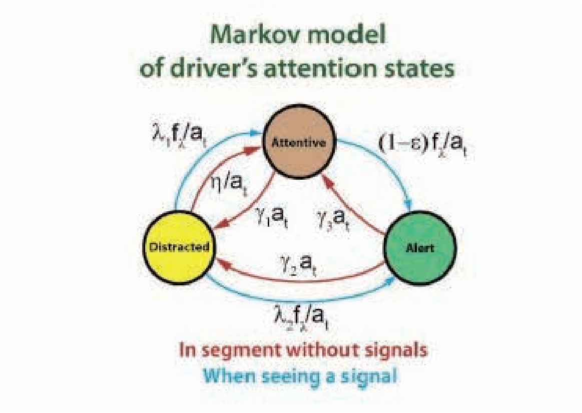

Markov model
of driver’s attention states
$\lambda_1 f_\lambda/a_t$
Attentive
$(1-\varepsilon)f_\lambda/a_t$
η/a_t
$\gamma_1 a_t$
$\gamma_3 a_t$
Distracted
Alert
$\gamma_2 a_t$
$\lambda_2 f_\lambda/a_t$
In segment without signals
When seeing a signal

Figure 1. Illustration of the Markovian model used to model the driver’s attention.

Therefore, the changes of driver’s attention state due to the different line incidences; as well as how erroneous decisions are corrected by the supervisor systems must be modeled.

Since travel times of the different trains circulating along the network or line could be very different and it is not the same a delay of five minutes in a one hour trip than in a three hours trip, we use in our model relative travel times. The relative travel time is defined as the quotient between the actual travel time and the minimum possible travel time, that is, at maximum speed. This means that a relative travel time 1 means that the train travels at maximum speed, and a relative travel time of 1.10 menas that the travel time is 10 % above the minimum travel time. In this way we can combine trains with small and large travel times and also freight trains. In addition a train priority is considered as a factor to be applied to the relative travel time of each train.

2.1.4 Bayesian Network

A Bayesian network consists of two elements:

1. A directed acyclic graph, which includes one node per variable and links which determine from which variables (nodes) each variable directly depends on.
2. Tables of conditional probabilities of each variable given its parents, which quantifies the dependence relations among the variables.

This allow us to reproduce any joint multidimensional probability distribution without any restriction, so that we can model any set of multidimensional variables.

To simplify the Bayesian network building process, it can be divided in parts, each part corresponds to one item or element with its variables and links or to the segment between consecutive items and its variables and links. Figure 2 illustrates how these different parts are assembled in order to obtain the whole Bayesian network from the parts. It contains the real line as it is perceived by users and the mathematical model where the left graphs correspond to segments between items and the right graphs, to the items themselves.

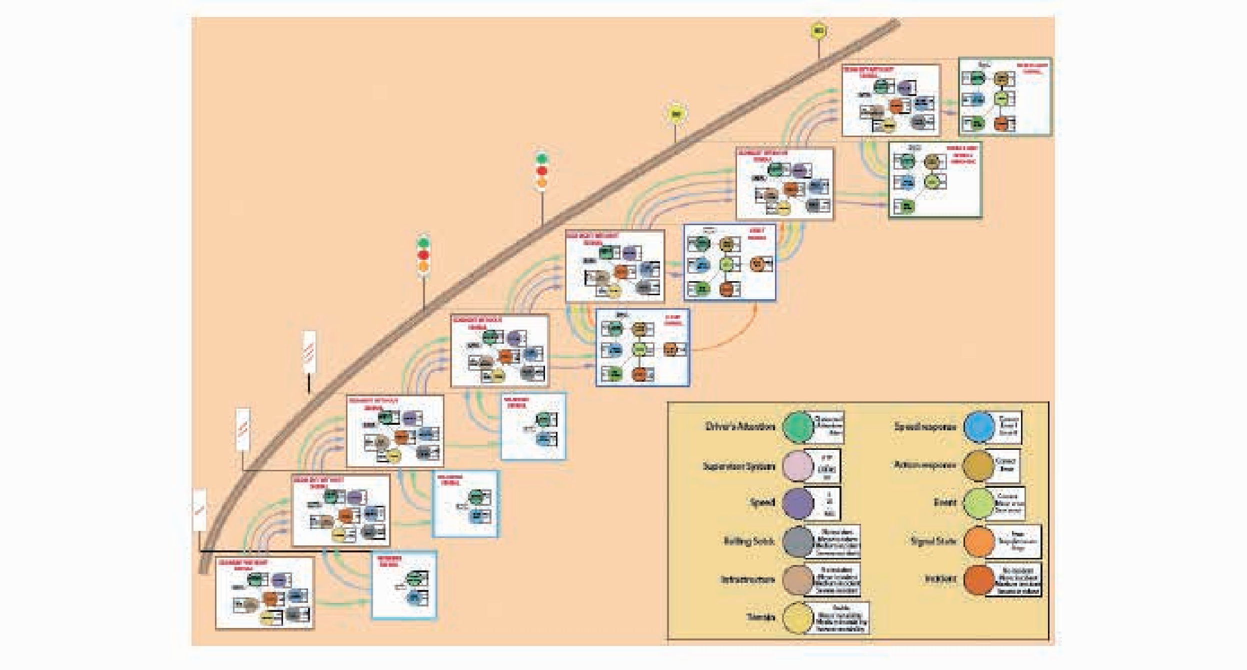


Figure 2. Assembling process of the different parts of the Bayesian network showing the segment between items and the item parts in the left and right locations, respectively.

Figure 3 shows the Bayesian network graph after the assembled process and the corresponding real line.

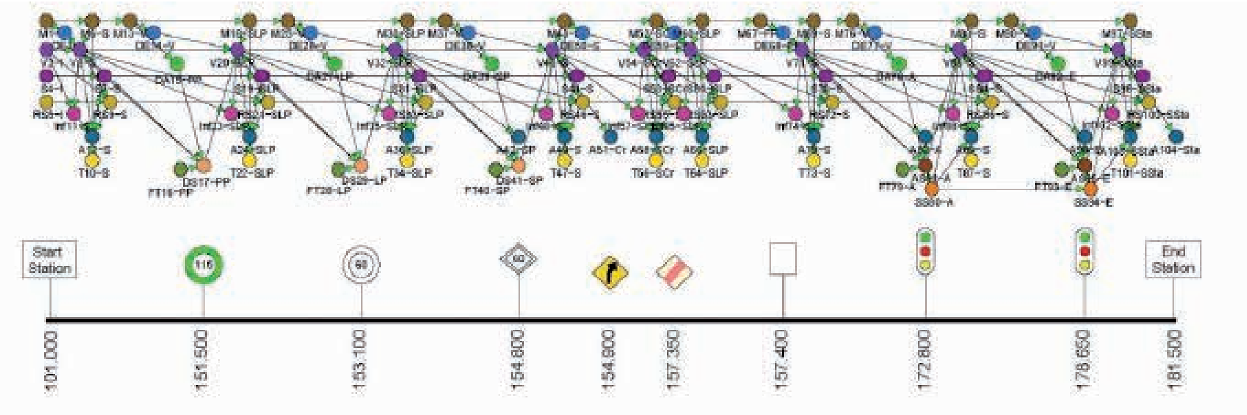


Figure 3. The Bayesian network graph after the assembled process and the corresponding real line.

2.1.5 Sub-Bayesian networks

2.1.5.1 Light signal

In this example a light signal composed of three warning signals, an advanced signal and an entry signal is modeled showing the associated influential variables (see Figure 4):

- Driver's attention state
- Speed
- Accidents
- Rolling stock
- Terrain and infrastructure failures
- Driver's decision
- Technical failure
- Supervisor
- Signal state
- Driver's tiredness

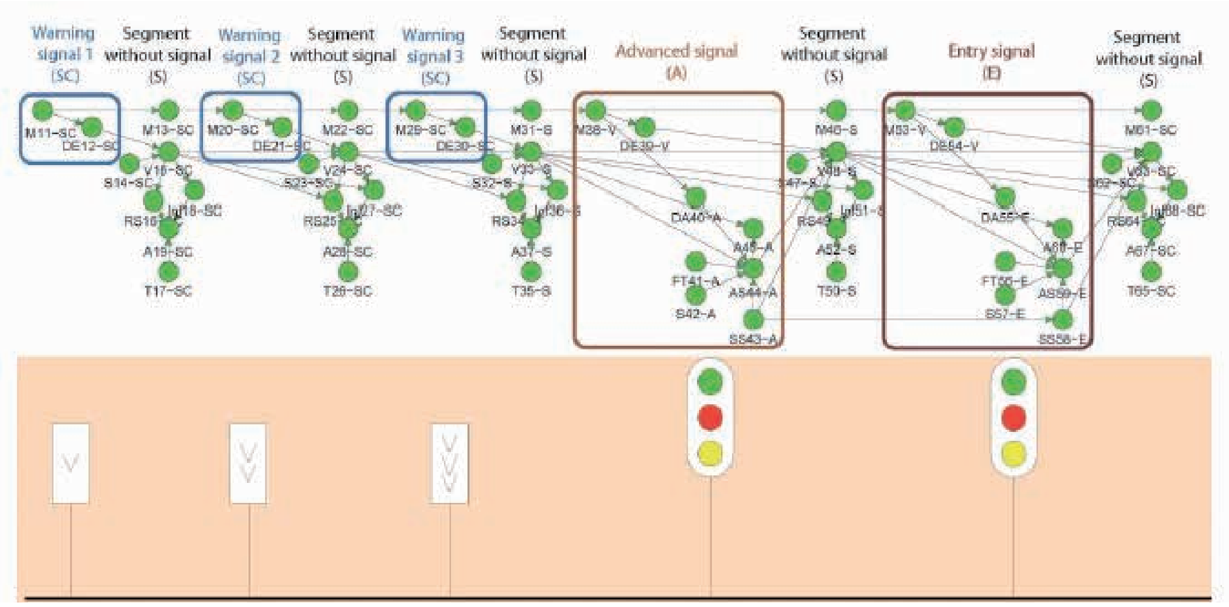


Figure 4. Illustration of the sub-Bayesian networks associated with warning and light signs showing the corresponding variables and links.

2.1.5.2 Temporal speed limit signal

Temporal speed limit signals consist of four signals (preannouncement, announcement, effective speed limit and end of limitation signals) and are related to their influential variables:

- Driver's attention state
- Speeds
- Accidents
- Rolling stock
- Terrain and infrastructure failures
- Driver's decision
- Technical failure
- Supervisor
- Signal state
- Driver's tiredness

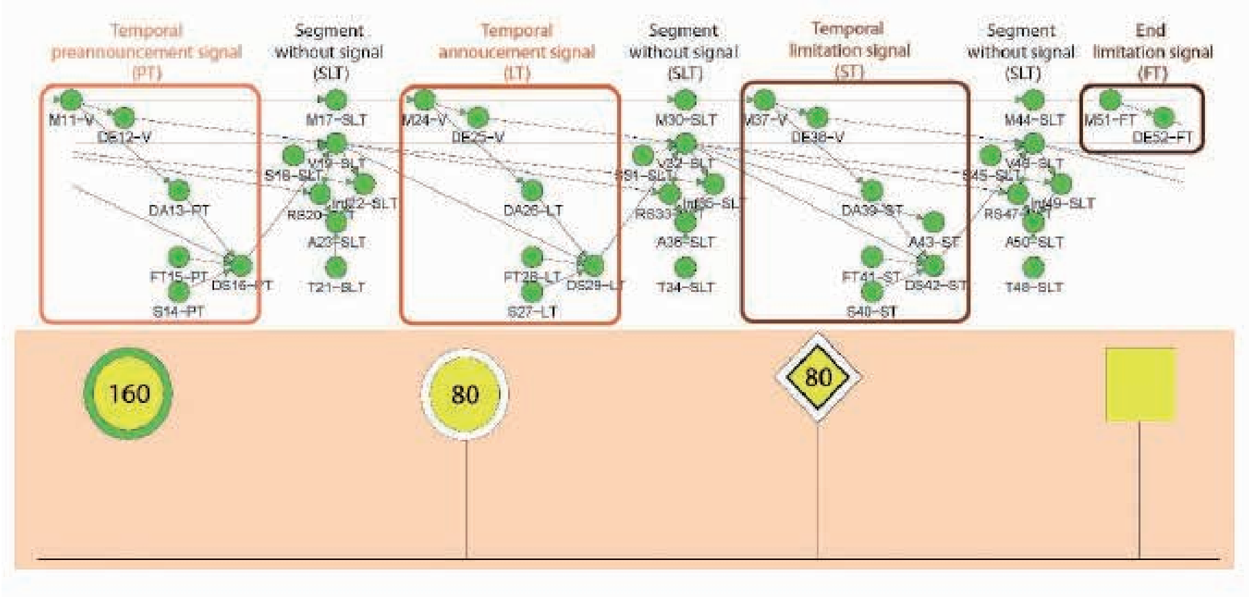


Figure 5. Illustration of the sub-Bayesian networks associated with temporal speed limit signs showing the corresponding variables and links.

2.2 Quantitative information of the Bayesian network. Conditional proba bilities.

Once the qualitative information of the Bayesian network is given, which includes the list of variables with the corresponding values and the lists of parents of each variable, we need to supply the quantitative information, which consists of a list of conditional probability tables, one per node, and contains the probabilities of each node given its parents.

One example is given in Figure 6, where the node Speed V is connected to its parents, nodes DE, Vp, S, AS and SS. This means that we need to give the probability of all combinations of the possible values of the child and the parents. To simplify this process it is convenient to provide a closed formula for the calculation of these probabilities in terms of a given set of parameters.

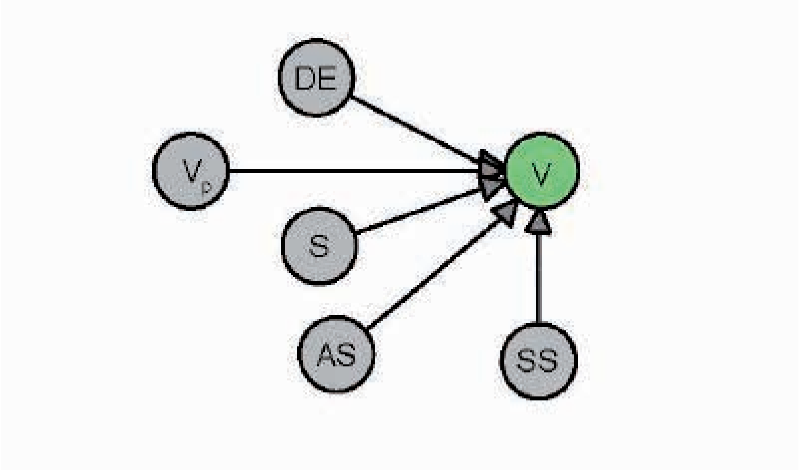


Figure 6. Speed node, V, connected to five parents (DE, Vp, S, AS and SS)

An example of closed formula for the conditional probability

$$p_{\mathrm{a,b,c,d,e,f}}(s) = P(\mathrm{V} = \mathrm{a} | \mathrm{V_p} = \mathrm{b}, \mathrm{DE} = \mathrm{c}, \mathrm{SS} = \mathrm{d}, \mathrm{AS} = \mathrm{e}, \mathrm{S} = \mathrm{f})$$

Is the following:

$$\begin{aligned} p_{\mathrm{a,b,c,d,e,f}}(s) \quad = \quad & \delta_{\mathrm{e},1} \left[\delta_{\mathrm{c},1} \delta_{\mathrm{a},s} + \delta_{\mathrm{c},2} \left((1-\rho_{\mathrm{f}}) \delta_{\mathrm{a},s} + \rho_{\mathrm{f}} \delta_{\mathrm{a,b}} \right) \right. \\ & \quad + \delta_{\mathrm{c},3} \left(\kappa_1 \rho_{\mathrm{f}} \delta_{\mathrm{a},\max(1,s-1)} + (1 - \rho_{\mathrm{f}}(\kappa_1 + \kappa_2)) \delta_{\mathrm{a},s} \right. \\ & \left. \left. + \kappa_2 \rho_{\mathrm{f}} \delta_{\mathrm{a},\min(n,s+1)} \right) \right] + (\delta_{\mathrm{d},2} \delta_{\mathrm{e},2} + \delta_{\mathrm{d},3} \delta_{\mathrm{e},3}) \left((1 - \rho_{\mathrm{f}}) \delta_{\mathrm{a},s} \right. \end{aligned}$$

Where the deltas are Kronecker's deltas and the rest are parameters.

2.3 Partition Technique

As the complexity of the problem grows with the square of the number of variables N and this number is normally above several thousands, it is convenient to partition the Bayesian network into much smaller subnets, so that the complexity grows linearly with N. In order to analyze the possible partitions it is enough to use the acyclic directed graph and to study the conditional independence between subnetworks. Figure 7 Illustrates how the Bayesian network can be partitioned in order to allow for the complexity to become linear in the number of variables and provide results in reasonable CPU times.

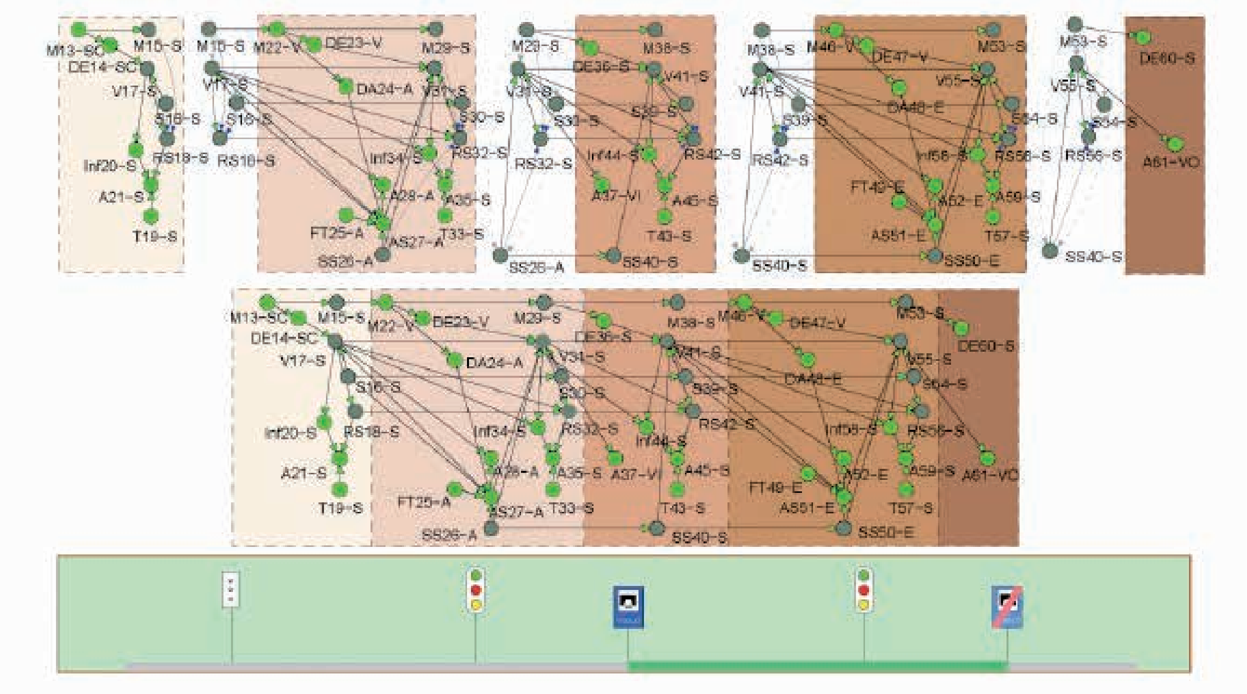


Figure 7. Illustration of how the Bayesian network can be partitioned in order to allow for the complexity to become linear in the number of variables and provide results in reasonable CPU times.

2.4 Backward analysis

The Bayesian network also allows to determine the causes of a given incident by proceeding backwards using available information and modifying the probabilities accordingly. Figure 8 shows the conditional probability tables before any information is supplied. For example, the probability of a severe accident number 33 is as low as 9.01 x 10^{-6}, signal 31 is in red 15% of the times, the probability of the driver to make an erroneous decision 14 is r, not obeying the sign, the speed was 220 km/h, there was a driver's erroneous decision14 "error I" is 6.01 x 10^{-5}, and the probability of the driver to be distracted was 2.84 x 10^{-7}.

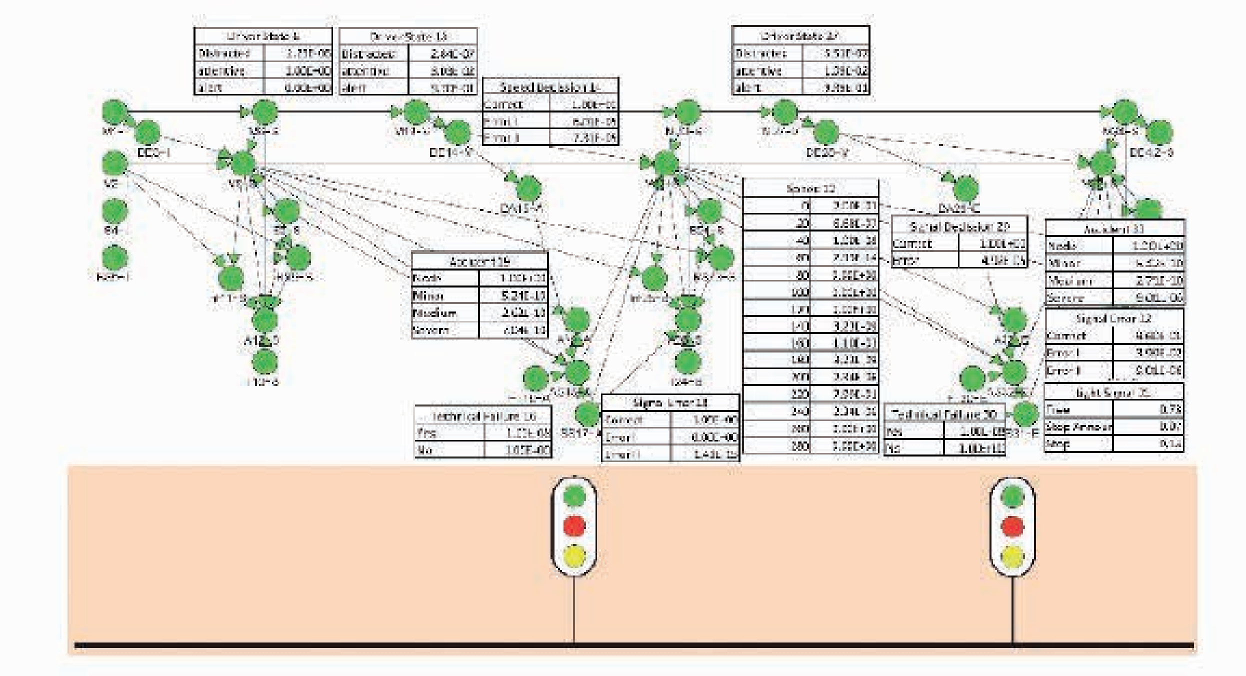


Figure 8. Conditional probability tables before any information is supplied.

However, after an accident 33 has occurred and evidence is obtained about the no occurrence of technical failures 16 and 30, their probabilities become one, as indicated in Figure 9 The Bayesian network techniques permit recalculating the probabilities of all other variables and consequently, provide the probabilities of any other event having information about the causes of accident 33. For example, Figure 9 informs us that signal 31 was in red, the driver made an error, not obeying the sign, the speed was 220 km/h, there was a driver's erroneous decision14 "error I", and this could be due to a distracted state or to an attentive state, but the later seems to be more probable.

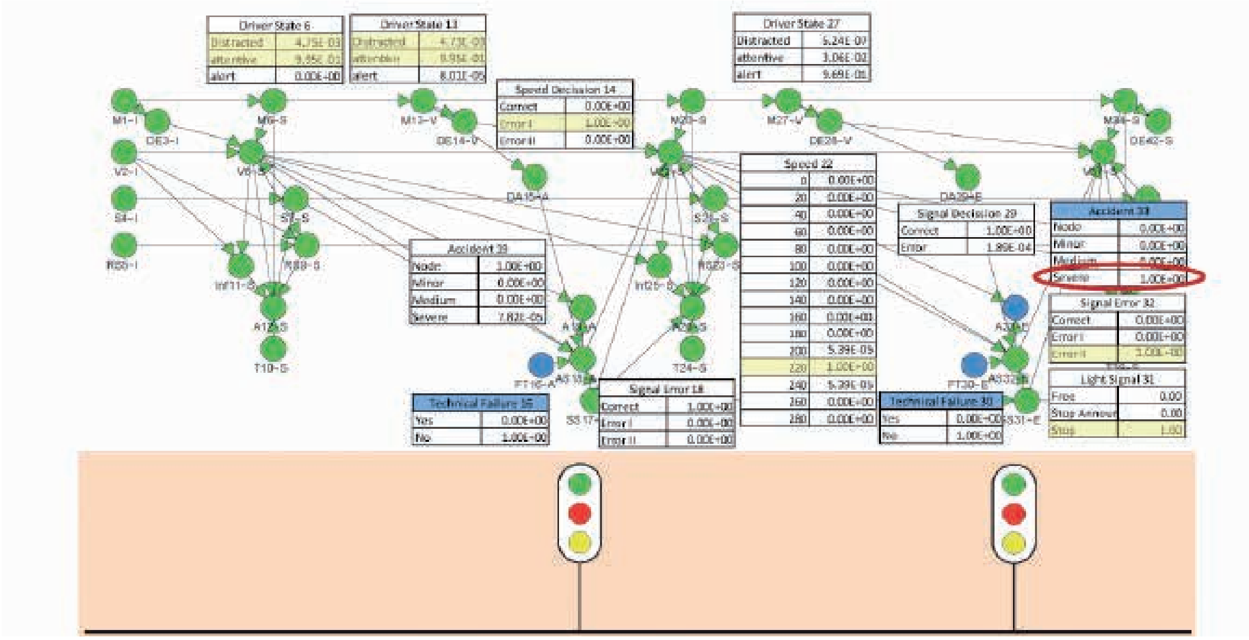


Figure 9. Conditional probability tables after a severe accident has occurred and no technical failures took place at two given locations close to the accident location.

All this shows that the power of Bayesian networks to facilitate a cause analysis study is really important.

2.5 Software development and provided information

The above described model has been implemented into a software package that allow us to perform the following tasks and provides the following information:

1. Check the input data for correctness and completeness.
2. Build the Directed acyclic graph of the Bayesian network including all variables and links.
3. Plot the Bayesian network.
4. Plot a scheme or diagram of the railway line including all its elements and corresponding Pks.
5. Calculate the marginal probabilities of the incident nodes and evaluate the ENSI (expected number of severe equivalent incidents) values of all items.
6. Plot the cumulated graph of ENSI values for identifying the most risky items.
7. Provide tables, sorted under different criteria, with the ENSI values and probabilities of all incidents along the line.

8. Plot the trace of the line with the location of the most risky items.
9. Provide tables with the circumstances that produce the most risky incidents in order to address the corrections to the real circumstances.

2.5.1 Necessary Information

The software for the probabilistic safety analysis (PSA) needs the following elements of information or input data:

1. *Railway regulations to be applied.*
2. *Line description.* A detailed description including the location and characteristics of switches, signals, level crossings, tunnels, viaducts, curves, etc.
3. *Driver's booklets.* With the characteristic safety regulations for each train and line including detailed maximum speeds, timing, etc.
4. *Train characteristics.* Power, maximum speeds, lengths, maximum accelerations and decelerations, etc.
5. *A video taken from the cabin in both directions*. These two videos are very important to identify risks and make decisions about the line safety.

Each element must be modeled properly by providing a line of code with the corresponding information, as shown below:

```
'Underpass', 370.35,'T', ...
'AnnouncementP', 375.0, 0, 85, ...
'AnnouncementGradeCrossing', 376.0, 'P',2,...
'SignalP', 376.105, 1, 85, ...
'CurveIn', 376.215, 350,'R', ...
'GradeCrossing', 376.350,'P', ...
'SignalA', 378.2, ...
'AnnouncementGradeCrossing',379.765, 'P',1,..
'CurveOut', 379.768, 350, ...
'SignalFP', 379.775, 0, 85, ...
'GradeCrossing', 380.7,'P', ...
'ContinuousOFF',380.85, ...
```

3. Examples

Next, several examples of application are presented to illustrate the possibilities of the proposed methodology. In particular, the safety problems are identified and resolved with a quantification of the safety level previously and after the corrections have been done. This quantifications makes one of the mean differences of the proposed methods with respect to existing ones.

3.1 Example of the line Zaragoza-Miranda

After performing the probabilistic safety analysis of the Zaragoza-Miranda line, the worst identified location corresponds to a permanent speed limit sign of 30 km/h, without the preannouncement sign, as illustrated in Figure 10, with an ENSI value of 0.244, which is extremely high. Since there is an end of speed limit (corresponding to a speed of 10 km/h) at PK 337.950, the driver will start to increase speed at this location to reach the maximum speed, which in this case is 160 km/h. However, since the distance to the speed limit sign is 1.050 km the train can reach only 60 km/h. Fortunately, the speed is limited to this low value, reducing the possible risk.

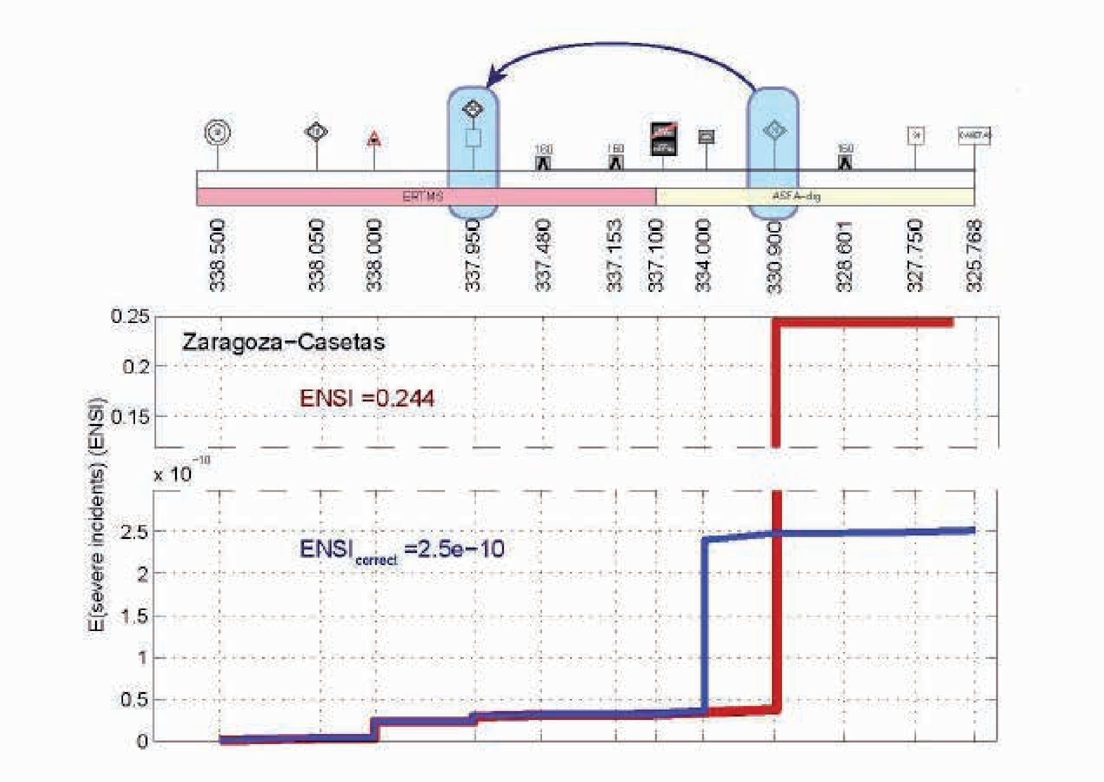


Figure 10. Probabilistic safety analysis of the Zaragoza-Casetas line

To correct this problem we move this speed limit sign 30km/h to PK 337.950, and remove the final speed limit sign at that location. In this way, the speed will be maintained at 30km/h without no increase and the problem is solved, as illustrated in Figure 10

3.2 Example of the line Palencia-Santander

After performing the probabilistic safety analysis of the Palencia-Santander line, one of the worst locations corresponds to a light signal located at PK 384.100 (see Figure 11). The main cause is an incorrect location of the advanced signal, which is too close to this light signal (at 258 m). Thus, the correction consists of moving this advanced signal to PK 382.916 (at 926m). By repeating the PSA the ENSI reduces from 4.77E-08 to 5.84E-12.

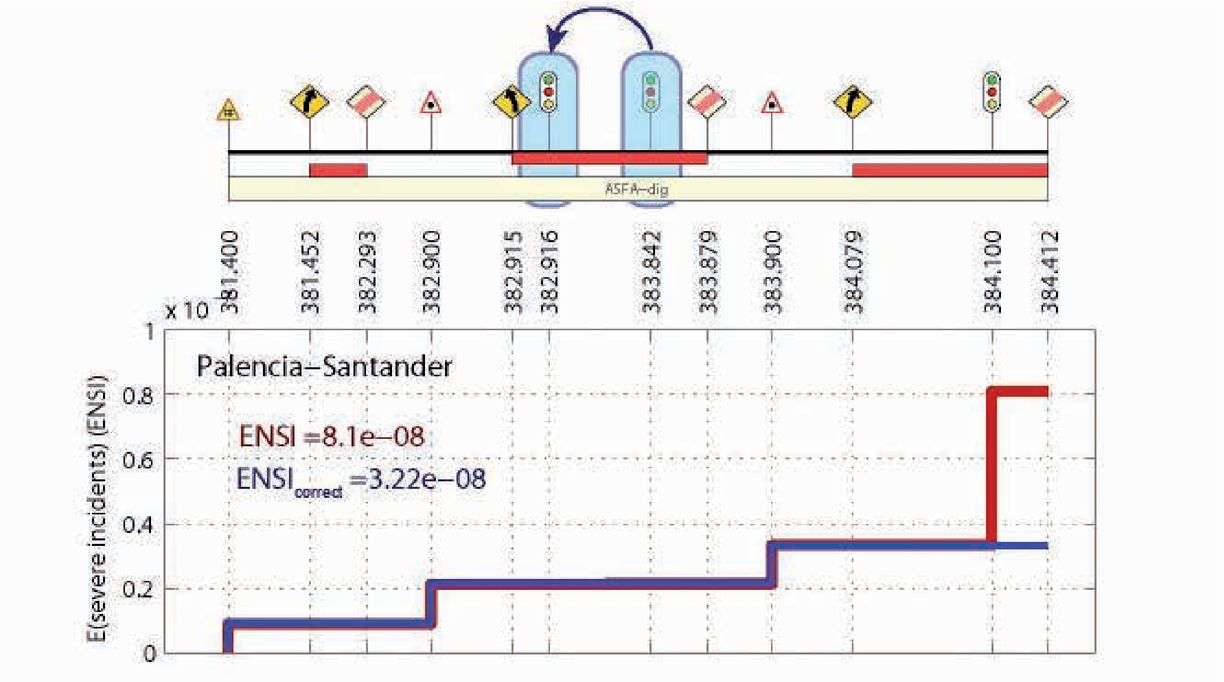


Figure 11. Probabilistic safety analysis of the Palencia-Santander line

3.3 Safety correction at a curve

In this example a safety problem due to an speed excess at a curve is corrected by means of the adequate speed limit signs. It can be seen in Figure 12 that the ENSI reduces from 0.00035 to 3.14 x 10 $^{-16}$. We note that speed excesses at a curve have been the main cause of important accidents in recent years, not only in Spain but in other countries of the EU and the United states of America. In particular, the responsibility cannot be given only to the driver (engineer or conductor) and ATP systems must be incorporated to avoid this type of accidents.

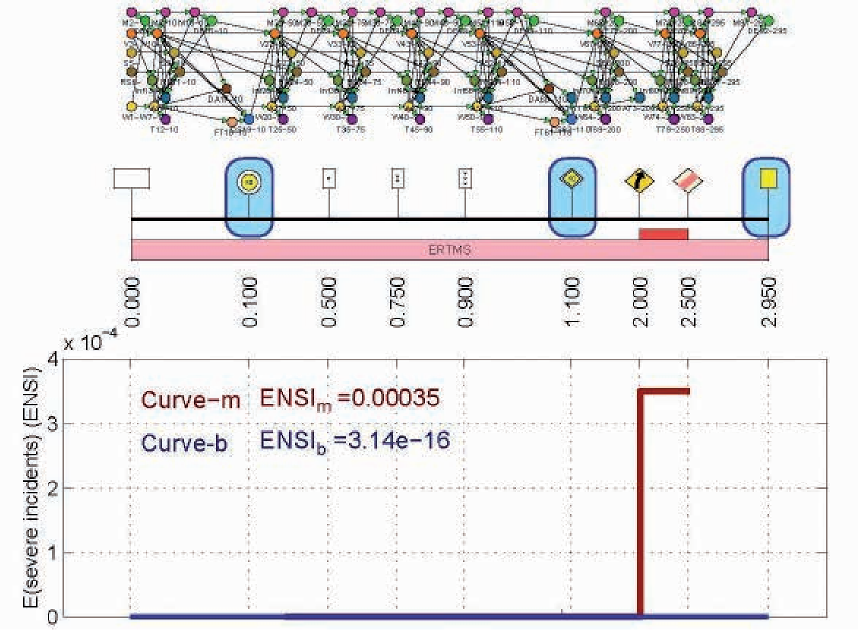


Figure 12. Illustration of how the safety improves at a curve when the speed limit is reduced.

3.4 Safety correction at a grade crossing

In this example a safety problem due to an insufficient announcement of a grade crossing is corrected by means of an adequate announcement sign and corresponding protection. It can be seen in Figure 13 that the ENSI reduces from 3.42 x 10 $^{-9}$ to 4.81 x 10 $^{-10}$. Grade crossing are known to be responsible for a large number of rail accidents and if possible thsy must be eliminated. On the other hand they produce important increases in travel times because of the deceleration and acceleration phases required when approaching grade crossing locations.

3.5 Safety improvement at a light signal

In this example the safety at a light signal is improved first by means of warning signs and later by the ERTMS (an ATP system). It can be seen in Figure 14 that the ENSI reduces from $1.09\cdot10^{-9}$ to $1.24\cdot10^{10}$ due to the warning signs and later to 6.48 x 10 $^{-14}$ due to the ERTMS. The light signal was initially under SR (staff responsible) protection and after after installing the warning signs it improves safety in one order of magnitude. Finally, installing the ERTMS safety improves in more than three orders of magnitude. It is important to enphasize the role played by the three warning signs, which produce an important improvement of the driver attention and thus increase safety substantially.

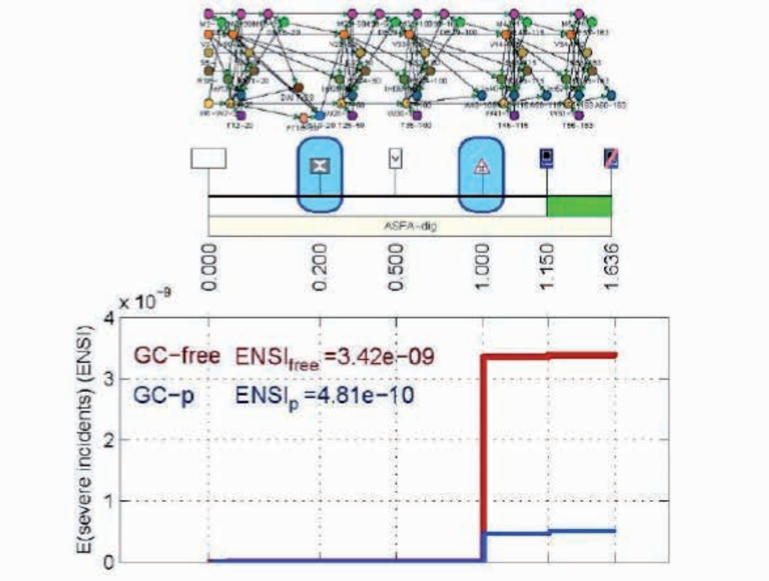


Figure 13. Illustration of how the safety improves at a grade crossing when by protection.

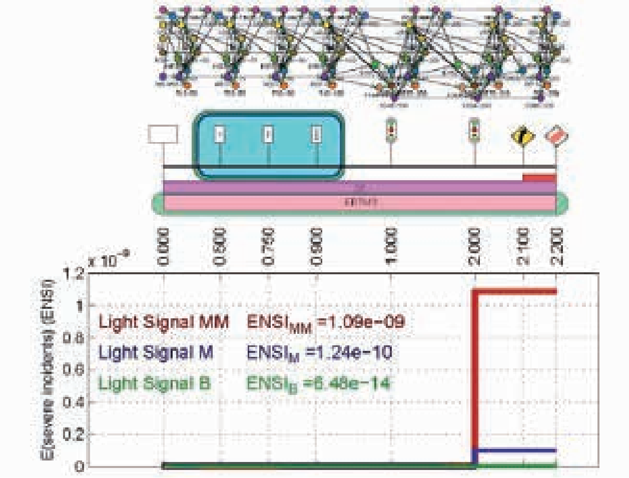


Figure 14. Illustration of how safety improves at a light signal by warning signs and the ERTMS.

3.6 Safety correction of a speed limit signal

In this example the safety at a speed limit signal is improved. Initially an erroneous announcement of a 120 km/h speed instead of 80 km/h causes the safety problem leading to an ENSI value of 0.145, which is extremely high (see Figure 15). This is due to the fact that the ASFAdig does not cover the speed excesses. To correct this sittuation, an additional announcement of 80km/h has been incorporated (see the blue shadowed plot in Figure 15) leading to an ENSI value of 3.52 x 10 $^{-9,}$ which is satisfactory. In addition if the ASFA-dig is replaced by the ERTMS, the ENSI reduces further to a value of 1.58 x 10 $^{-12}$, which is three orders of magnitude smaller (see the green shadowed plot in Figure 15). This example illustrates the importance of speed limit signs, which can be permanent or temporal. The fact that permanent signs are not covered by certain ATP systems should be corrected to avoid accidents. In addition, the location of the sequences of speed limit signs must be done very carefully.

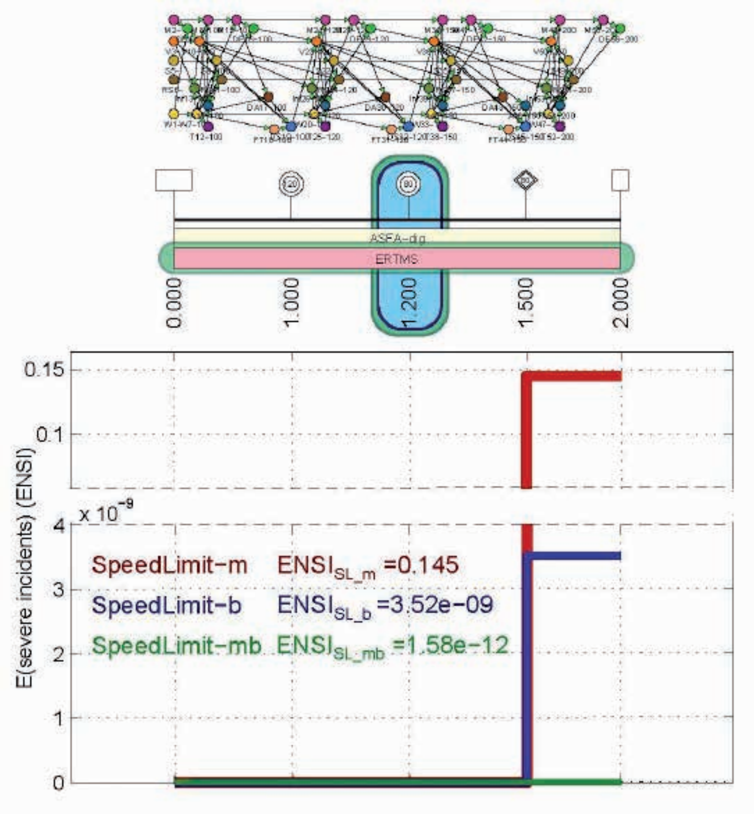
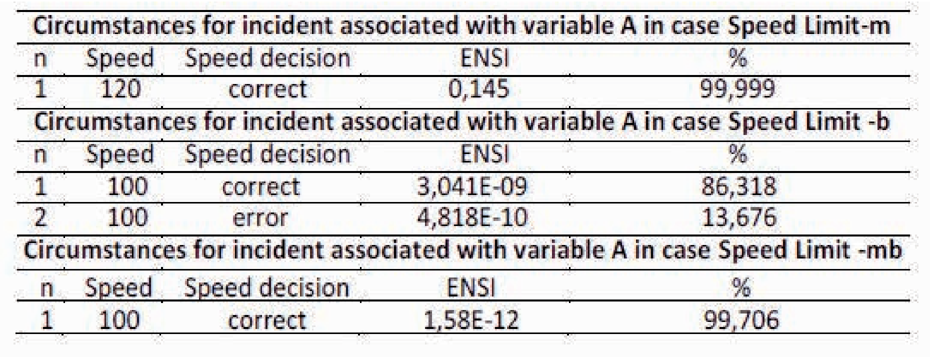


Figure 15. Illustration of how the safety improves at a speed limit signal by correcting errors.

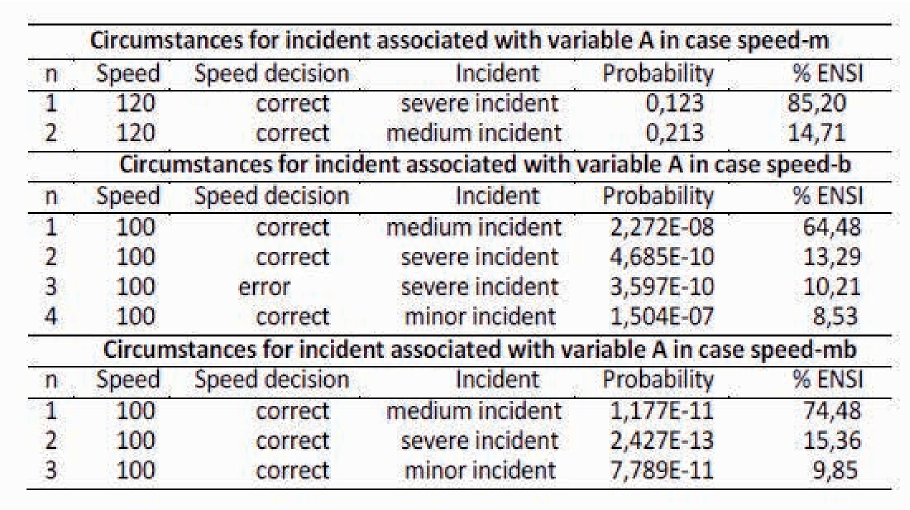
In Table 6 the circumstances under which the incidents at the speed limit signs are shown for the cases speed-m, speed-b and speed-mb, respectively. It is interesting to see that the case speed-m in which an erroneous announcement was located, the incident occurs, as expected, at this speed, with no error in the driver decision at practically all cases. In case speed-b, the speed reduces to 100 km/h and the driver decision remains correct in 86,318 % of the cases, but erroneous in 13,676% of the cases. Finally, in case speed-mb we have again no error and a speed of 100 km/h in almost all cases.

Table 6. Circumstances for incidents associated with variables incident for cases speed-m, speed-b and speed-mb showing the associated ENSI and corresponding percentages.



Circumstances for incident associated with variable A in case Speed Limit-m				
n	Speed	Speed decision	ENSI	%
1	120	correct	0,145	99,999
Circumstances for incident associated with variable A in case Speed Limit -b				
n	Speed	Speed decision	ENSI	%
1	100	correct	3,041E-09	86,318
2	100	error	4,818E-10	13,676
Circumstances for incident associated with variable A in case Speed Limit -mb				
n	Speed	Speed decision	ENSI	%
1	100	correct	1,58E-12	99,706

Table 7. Circumstances for incidents associated with variables incident for cases speed-m, speed-b and speed-mb showing the Probabilities and % ENSI values.



Circumstances for incident associated with variable A in case speed-m					
n	Speed	Speed decision	Incident	Probability	% ENSI
1	120	correct	severe incident	0,123	85,20
2	120	correct	medium incident	0,213	14,71
Circumstances for incident associated with variable A in case speed-b					
n	Speed	Speed decision	Incident	Probability	% ENSI
1	100	correct	medium incident	2,272E-08	64,48
2	100	correct	severe incident	4,685E-10	13,29
3	100	error	severe incident	3,597E-10	10,21
4	100	correct	minor incident	1,504E-07	8,53
Circumstances for incident associated with variable A in case speed-mb					
n	Speed	Speed decision	Incident	Probability	% ENSI
1	100	correct	medium incident	1,177E-11	74,48
2	100	correct	severe incident	2,427E-13	15,36
3	100	correct	minor incident	7,789E-11	9,85

Table 7 is very similar, but now we include a column with the probability for each incident severity and the corresponding ENSI percentage. It is interesting to see the probabilities of minor, medium and severe incidents for each case. As expected minor incidents occur at the speed limit sign more frequent than medium and these more frequently than severe incidents.

4. Conclusions

Bayesian network models provide an important tool to perform a probabilistic safety assessment of railway lines, and are more powerful than the commonly used fault and event trees, especially when common causes are present.

The proposed model reproduces all the variables involved in the problem, including their qualitative dependencies and the quantification of the associated conditional probabilities.

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.

A simple list of items can be given for a computer program to build the acyclic graph associated with the Bayesian network automatically.

The proposed partitioning technique reduces the initial nonlinear complexity to a complexity which is linear with the number of nodes.

The examples analyzed in this article show that the method is able to identify and quantify relevant incidents and their probabilities of occurrence.

The backward possibilities of the Bayesian network permits to analyze the causes of incidents and especially those leading to fatal accidents.

The most critical part of the proposed model is the parameter estimation and calibration, which must be done with the collaboration of various groups of experts.

5. Bibliography

- Amit, I. & Goldfarb, D., 1971. The timetable problem for railways. *Developments in Operations Research,* Volume 2, pp. 379-387.
- Assad, A., 1980. Models for rail transportation. *Transportation Research Part A,* Volume 14, pp. 205-220.
- Beales, L., 2002. *Guidance on the Preparation of Risk Assessments within Railway Safety Cases,* s.l.: RSSB.
- Burdett, R. L. & Kozan, E., 2010. A disjunctive graph model and framework for constructing new train schedules. *European Journal of Operational Research,* Volume 2010, pp. 85-98.
- Cacchiani, V. & Toth, P., 2012. Nominal and Robust Train Timetabling Problems. *European Journal of Operational Research,* Volume 219, pp. 727-737.
- Caprara, A., Fischetti, M. & Toth, P., 2002. Modeling and solving the train timetabling problem. *Operations Research,* Volume 50, pp. 851-861.
- Carey, M., 1994. A model and strategy for train pathing with choice of lines, platforms and routes. *Transportation Research Part B,* Volume 28, pp. 333-353.
- Carey, M. & Crawford, I., 2007. Scheduling trains on a network of busy complex stations. *Transportation Research Part B,* Volume 41, pp. 159-178.
- Carey, M. & Lockwood, D., 1995. A model, algorithms and strategy for train pathing. *Journal of the Operational Research Society,* Volume 46, pp. 988-1005.
- Castillo, E. et al., 2015. An alternate double-single track proposal for high-speed peripheral railway lines. *Computer Aided Civil and Infrastructure Engineering,* Volume 30, pp. 181201.
- Castillo, E., Gallego, I., Ureña, J. M. & Coronado, J. M., 2009. Timetabling optimization of a single railway track line with sensitivity analysis. *TOP,* Volume 17, pp. 256-287.
- 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,* Volume 35, pp. 859-878.
- Castillo, E., Grande, Z., Moraga, P. & Sánchez Vizcano, J., 2016. A time partitioning technique for railway line design and timetable optimization. *Computer Aided Civil And Infrastructure Engineering,* Volume 31, pp. 599-616.
- Cordeau, J. F., Toth, P. & Vigo, D., 1998. A survey of optimization models for train routing

and scheduling. *Transportation Science,* Volume 32, pp. 380-404.

- D'Ariano, A., Pacciarelli, D. & Pranzo, M., 2007. A branch and bound algorithm for scheduling trains in a railway network. *European Journal of Operational Research,* Volume 183, pp. 643-657.
- D'Ariano, A. & Pranzo, M., 2004. *A real time train dispatching system based on blocking time theory.* Delft, DUP Science, pp. 129-152.
- D'Ariano, A., Pranzo, M. & Hansen, I. A., 2007. Conflict Resolution and Train Speed Coordination for Solving Real-Time Timetable Perturbations. *IEEE Transactions on Intelligent Transportation Systems,* Volume 8.
- Haghani, A. E., 1987. Rail freight transportation: a review of recent optimization models for train routing and empty car distribution. *Journal of Advanced Transportation,* Volume 21, pp. 14-172.
- Hellström, P., 1998. *Analysis and evaluation of systems and algorithms for computer-aided train dispatching,* Sweden: s.n.
- Higgins, A., Kozan, E. & Ferreira, L., 1996. Optimal scheduling of trains on a single line track. *Transportation Research Part B,* Volume 30, pp. 147-161.
- Jia, L. M. & Zhang, X. D., 1993. Distributed intelligent railway traffic control based on fuzzy decision making. *Fuzzy Sets and Systems,* Volume 62, pp. 255-265.
- Kraay, D. R. & Harker, P. T., 1995. Real-time scheduling of freight railroads. *Transportation Research Part B,* Volume 29, pp. 213-229.
- Lin, D. Y. & Ku, Y. H., 2013. Using Genetic Algorithms to Optimize Stopping Patterns for Passenger Rail Transportation. *Computer-Aided Civil and Infrastructure Engineering,* pp. n/a--n/a.
- Ouyang, Y. et al., 2009. Optimal Locations of Railroad Wayside Defect Detection Installations. *Computer-Aided Civil and Infrastructure Engineering,* Volume 24, pp. 309-319.
- Pachl, J., 2014. Railway Timetabling and Operations. Analysis - Modelling - Optimisation - Simulation - Performance Evaluation. In: Hamburg(): Eurailpress, pp. 23-24.
- Petersen, E. R., Taylor, A. J. & Martland, C. D., 1986. An introduction to computer aided train dispatching. *Journal of Advanced Transportation,* Volume 20, pp. 63-72.
- Sahin, I., 1999. Railway traffic control and train scheduling based on inter-train conflict management. *Transportation Research Part B,* Volume 33, pp. 511-534.
- Yang, Z. & Hayashi, Y., 2002. GIS-Based Analysis of Railways Origin/Destination Path-Selecting Behavior. *Computer-Aided Civil and Infrastructure Engineering,* Volume 17, pp. 221-226.