Methodology of Security analysis and critical points detention in Railways lines

Enrique Castillo
Zacarías Grande
Aida Calviño
UNIVERSIDAD DE CANTABRIA

Real Academia de Ingeniería

Enrique Castillo
REAL ACADEMIA DE INGENIERIA

University of Cantabria May 27th, 2015

Index of the talk

Background

Background

The main reasons that led to study the safety of railway lines are the following:

1. **Alternate double-single track proposal:** The **alternate double-single track lines require a deeper safety control**, since single track segments provide less flexibility to trains than double track segments. Although safety in single track lines has already been solved a long time ago.
2. **Santiago Railway accident report:** Since PhD Castillo was requested to elaborate a **report on the Ourense-Santiago (Spain) line safety**,because of the unfortunate July 2013 accident PhD Castillo considers that should been developed a new safety analysis model.
3. **Security analyzer method used by ADIF:** This method consist in **Hazard identification, Risk evaluation and Risk management** but the resulting procedure is **qualitative and not very accurate**

Bases of the proposal

Hence, PhD Castillo considered that the current model is an inappropriate methodology and proposed to evaluate the railway lines based on a **probabilistic risk analysis** as he already developed in the Santa María de Garoña Nuclear Plant, the first Spanish nuclear power plant where probabilistic risk analysis were done.

BASES OF THE PROPOSAL

Hence, PhD Castillo considered that the current model is an inappropriate methodology and proposed to evaluate the railway lines based on a **probabilistic risk analysis** as he already developed in the Santa María de Garoña Nuclear Plant, the first Spanish nuclear power plant where probabilistic risk analysis were done.

Due to the fact that **event and fault trees**, though very powerful, they **present certain important limitations**, PhD Castillo preferred the **Bayesian networks**, according to Castillo's background with this extremely important probabilistic representation tool of **multidimensional variables**.

Consequently, we must first **identify and reproduce the most relevant variables** which play a relevant role in the safety of a railway line to **model its multidimensional random behaviour**.

With this aim, we decided to travel in the train cabin to observe and **detect all the possible hazardous situations**.

Hazardous situations in segments without signals

CUTTINGS AND EMBANKMENTS

Among the potential hazards related to cuttings or embankments we mention:

- Falling stones on the line tracks or on the train.
- Ballast pick-up.
- Landslides.

CROSSING VIADUCTS

Among the potential hazards related to crossing viaducts we mention:

- Stiffness changes.
- Structural collapse (accidents or flash flood).
- Derailments due to structural displacement.

Tunnel crossing

Among the potential hazards related to tunnel entries or exits we mention:

- Water or snow accumulation at the exit or entry.
- Stiffness changes between the inside and outside of the tunnel.
- Falling terrain or rock blocks at tunnel entries or exits.
- Material accumulation in narrow spaces between tunnels.

Crossing switches

Among the potential hazards to be considered at crossings we mention:

- Infrastructure failure under the track.
- Ballast wear.
- Switch deterioration.
- Technical or human failure in opening gear switches.

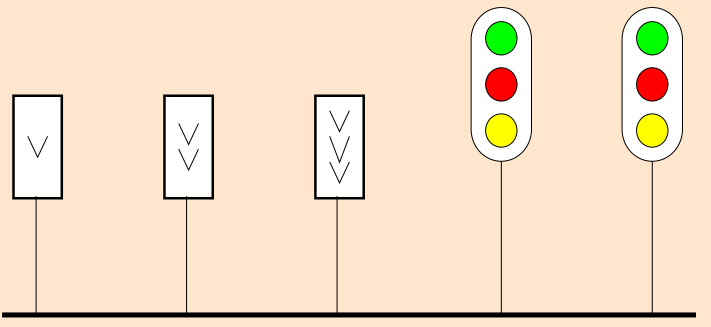
Level crossings

Among the potential hazards related to level crossings we mention:

- Stiffness change in level crossings.
- Track obstruction by vehicles.
- People or animal crossings.

Light and speed limit signals

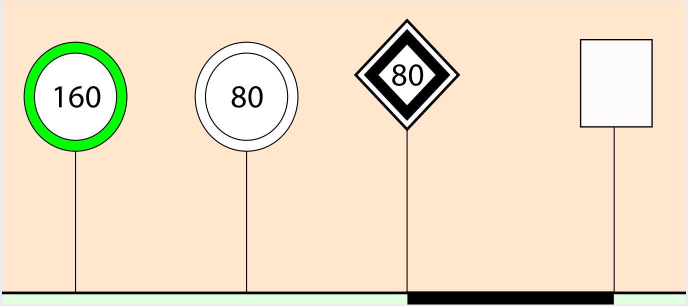
LIGHT SIGNALS



A high speed train requires several kilometers to reduce speed or stop, so speed reductions must be indicated in advance. Hence, any speed reduction or stopping signal **must be preceded by other signal** (advanced signal), which alerts about this situation.

Evidently human errors may occur at this signal, jeopardizing train safety.

SPEED LIMIT SIGNAL



Permanent speed limit signals form **a four signals group**, including an announcement signal to reduce speed to 160 km/hour, an announcement signal to reduce speed to the speed limit, the effective speed limit signal and the end of speed limit signal, respectively.

An accident derived from speed limit violation may occur only along the effective limitation segment. These **violations are not always protected** by the automatic train protection (ATP) system.

Model description

Identification of variables relevant to the line safety

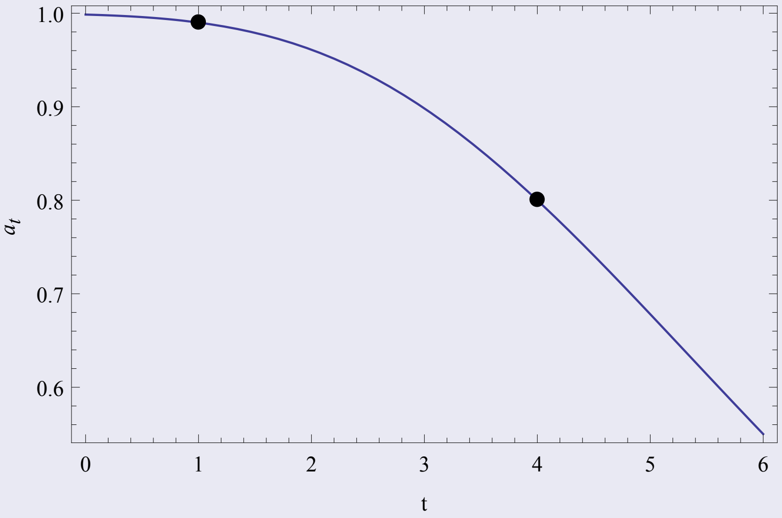
Hence, we can identify the following list of variables which are relevant to line safety:

1. **Driver's tiredness** (Maximum 6 continuous driving hours) .
2. State of **Driver's attention** (It suffers remarkable changes).
3. **Rolling stock failures**.
4. **Terrain failures** (landslides, falling materials, differential settlements, etc).
5. **Infrastructure failures** (sleepers, ballast, plates, connectors, etc)
6. State of speed limit or light **signals**.
7. Driver's **decision and possible errors**.
8. **ATP** Automatic Train Protection used.
9. **Technical failure** in the operation.
10. Minor, medium or severe **accidents** .

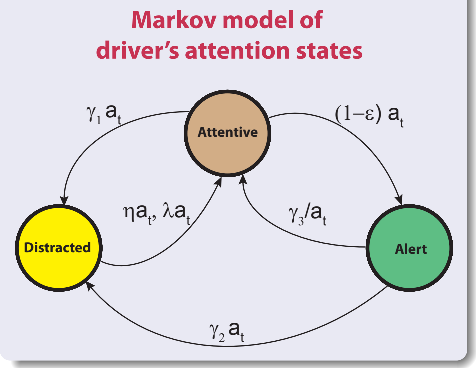
Due to its complexity, a risk evaluation program **must be used**.

Markovian model

Evolution of tiredness with driving time



Markovian model



To analyze the driver's attention we propose a **Markovian model** that consider three driver's attention states (distracted, attentive and alert).

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 modelled.

Bayesian network

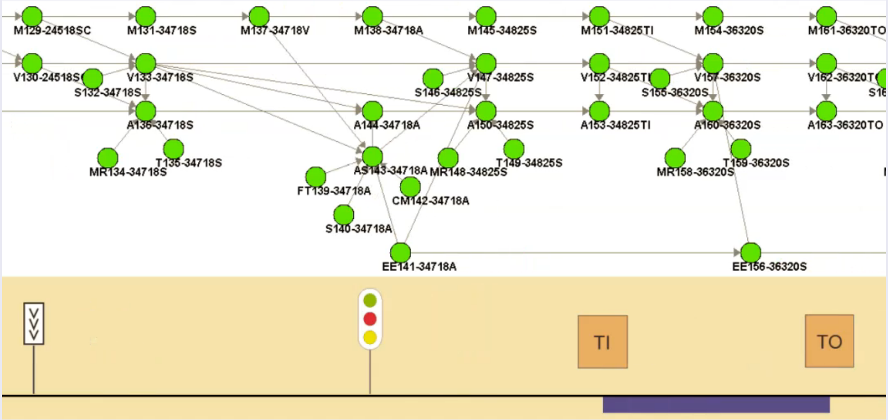
Bayesian network's elements

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.

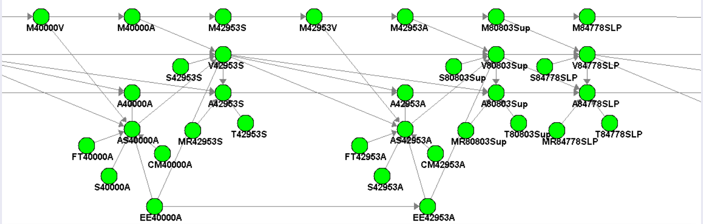
This allow us to reproduce any **joint multidimensional probability distribution** without any restriction, so that we can model any set of multidimensional variables.

General view



Information supplied by Bayesian network

Conditional probability tables



Edit Function

p(AS42953A | V42953S, M42953V, FT42953A, S42953A, EE42953A, CM42953A)

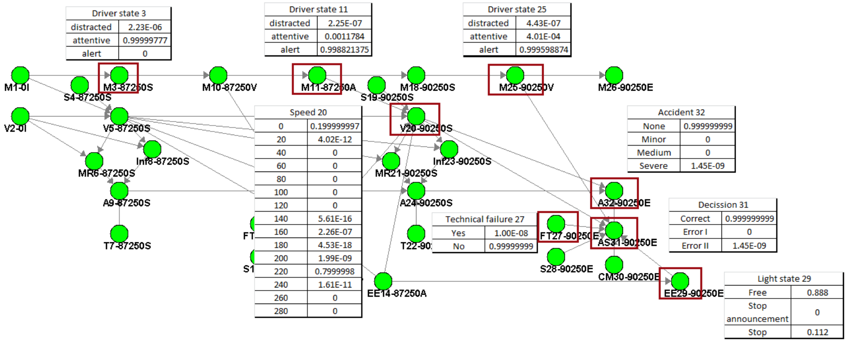
Values for parents:

M42953V	attentive
FT42953A	no
S42953A	ERTMS
EE42953A	stop_announcement
CM42953A	fixed

V42953S	0	20	40	60	80	100	120	140	160	180	200	220	240	260	280
correct	1.0	1.0	1.0	0.999998	0.999998	0.999998	0.999998	0.999998	0.999998	0.999998	0.999998	0.999998	0.999998	0.999998	0.999998
error_I	0.0	0.0	0.0	2.06579E-6	2.06579E-6	2.06579E-6	2.06579E-6	2.06579E-6	2.06579E-6	2.06579E-6	2.06579E-6	2.06579E-6	2.06579E-6	2.06579E-6	2.06579E-6
error_II	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0

Apply Dismiss

Joint probability table without observation



Driver state 3	
distracted	2.23E-06
attentive	0.99999777
alert	0

Driver state 11	
distracted	2.25E-07
attentive	0.0011784
alert	0.998821375

Driver state 25	
distracted	4.43E-07
attentive	4.01E-04
alert	0.999598874

Speed 20	
0	0.199999997
20	4.02E-12
40	0
60	0
80	0
100	0
120	0
140	5.61E-16
160	2.26E-07
180	4.53E-18
200	1.99E-09
220	0.7999998
240	1.61E-11
260	0
280	0

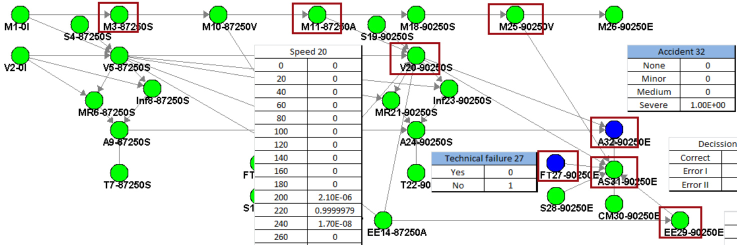
Accident 32	
None	0.999999999
Minor	0
Medium	0
Severe	1.45E-09

Technical failure 27	
Yes	1.00E-08
No	0.99999999

Decission 31	
Correct	0.999999999
Error I	0
Error II	1.45E-09

Light state 29	
Free	0.888
Stop announcement	0
Stop	0.112

JOINT PROBABILITY TABLE AFTER OBSERVED EVENTS (INFERENCE)



Driver state 3	
distracted	3.49E-02
attentive	0.96507544
alert	0

Driver state 11	
distracted	3.48E-02
attentive	0.1946209
alert	0.770602704

Driver state 25	
distracted	3.05E-04
attentive	1.78E-03
alert	0.997915744

Speed 20	
0	0
20	0
40	0
60	0
80	0
100	0
120	0
140	0
160	0
180	0
200	2.10E-06
220	0.9999979
240	1.70E-08
260	0
280	0

Accident 32	
None	0
Minor	0
Medium	0
Severe	1.00E+00

Technical failure 27	
Yes	0
No	1

Decission 31	
Correct	0
Error I	0
Error II	1

Light state 29	
Free	0
Stop announcement	0
Stop	1

INFORMATION ELEMENTS OBTAINED FROM THE BAYESIAN NETWORK

1. **All marginal probabilities of the variables** (nodes). Particularly, the model gives the probabilities of speed excesses, driver's errors, distraction human errors and accidents.

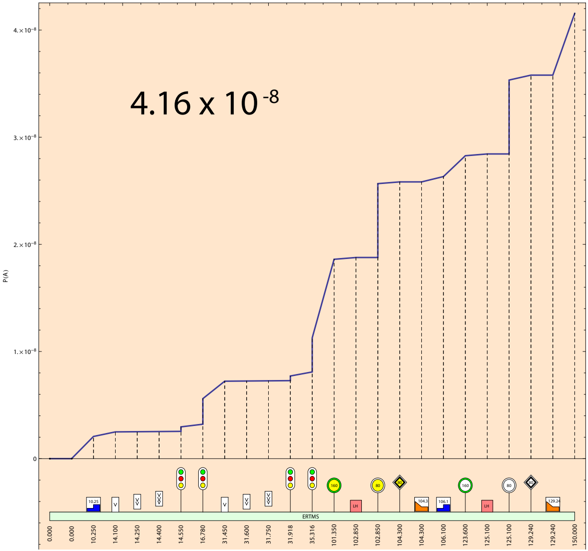
Information elements obtained from the Bayesian network

1. **All marginal probabilities of the variables** (nodes). Particularly, the model gives the probabilities of speed excesses, driver's errors, distraction human errors and accidents.
2. **Joint probabilities of any subset of variables**, which allow us to analyze variable dependencies.

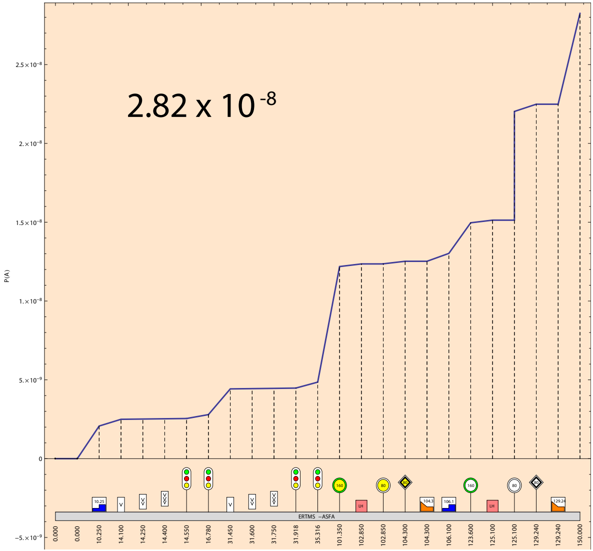
Information elements obtained from the Bayesian network

1. **All marginal probabilities of the variables** (nodes). Particularly, the model gives the probabilities of speed excesses, driver's errors, distraction human errors and accidents.
2. **Joint probabilities of any subset of variables**, which allow us to analyze variable dependencies.
3. **Clarifying the causes of different events or set of events**.

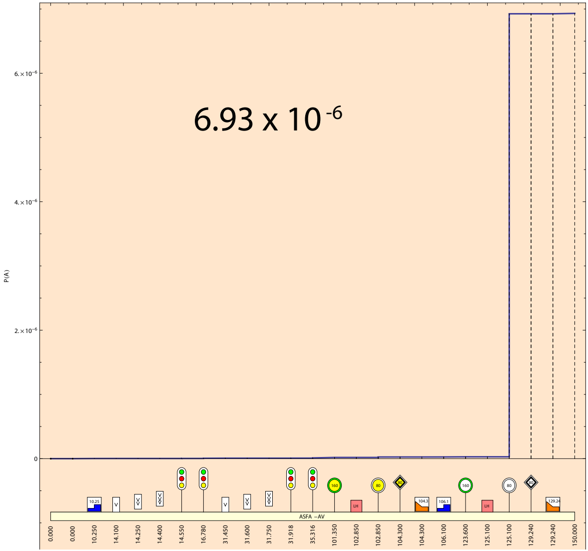
Examples of application



Since the **ERTMS** corrects the errors due to light and speed limit signals, the accident associated probabilities (vertical jumps in the graph) are small.



If both ATP systems ERTMS and ASFA are simultaneously used, the accident probability due to pass at red signals would be very small because both systems correct the errors.



In this case, **since permanent limit speed signals are not covered by the ASFA system**, the accident probability due to these dominates and hides those due to light signals or to train circulation in segments without signals.

MANY THANKS

THANKS