Computation of Importance Measures Using Bayesian Networks for the Reliability and Safety of Complex Systems

S.A. Raza[1*], Q. Mahboob[1], A.A. Khan[1], T.A. Khan[1], J. Hussain[1]

1. Mechanical Department, University of Engineering and Technology (UET), Lahore, Pakistan

Abstract

Modern engineering systems have proven to be quite complex due to the involvement of uncertainties and a number of dependencies among the system components. Shortcoming in the inclusion of such complex features results in the wrong assessment of reliability and safety of the system, ultimately to the incorrect engineering decisions. In this paper, the usefulness of Bayesian Networks (BNs) for achieving improved modeling and reliability and risk analysis is investigated. The calculation of a number of Importance Measures with use of Fault Tree Analysis as well as BNs is provided for a complicated railway operation problem. The BNs based safety risk model is investigated in terms of quantitative reliability and safety analysis as well as for multi dependencies and uncertainty modeling.

Nomenclature

BNs	Bayesian Networks
FTA	Fault Tree Analysis
ETA	Event Tree Analysis
SPAD	Signal Passing At Danger
TPWS	Train Protection and Warning Systems
Te	Top event
IMs	Importance Measures
IMP	Improvement Potential
CIF	Criticality Importance Factor
FUV	Fussell-Vesely
BIM	Birnbaum's Measure
DIF	Diagnostic Importance Factor
RRW	Risk Reduction Worth
RAW	Risk Achievement Worth
COP	Conditional Probability
SRM	Safety Risk Model
CTA	Curve in Track Alignment
HTRS	High Train Speed
FAF	Failure Frequencies
FU	Fixed Unavailability Values
SRM	Safety Risk Model
HTRS	High Train Speed
CPT	Conditional Probability Table
DE	Driver error towards brake Application

* Corresponding Author Email: aownraza217@gmail.com

Introduction

Importance Measures (IMs) may assist the system designers in the recognition of the components requiring improvement, helping the maintenance engineers for improving the maintenance strategies regarding the demanding components and expedite the decision makers regarding discharge of the engineering finances for the safety mechanization. There are a lot of Importance and criticality evaluation measures which are effective in various reliability and safety risk problems [1, 2, 3, 4]. For example, Risk Achievement Worth (RAW) recognizes the system risks increment in the case a specific component downfall in system has taken place. An increment in the occurrence possibility of the downfall of component will result into the increase of Fussel Vesely (FUV) Value.

Event Tree Analysis (ETA) and Fault Tree Analysis (FTA) are the common methods applied to logically represent an engineering system such as a railway system, for the reliability and risk analyses [5, 6, 7, 8]. Generally, both FTA and ETA simplify the calculations by considering logically deterministic combinations of causes. Due to this reason, there exist

shortcomings in modeling of the complex systems [9, 10]. An exponential increase in the structure of FTA is seen in majority of the cases, that is why it becomes very difficult to understand and compute with the increase in common reasons of failure as well as due to multistate events [7]. Due to these shortcomings, it becomes difficult to apply the traditional methods for analyzing complex engineering systems such as the railway system, which is featured by a number of dependencies and uncertainties. Therefore, we require an investigation to use BNs in order to model and analyze the risks and reliability in current railway system. This new method of BNs can handle the complex features of risk and reliability problem in the likes of common cause failures, disjoint events, functional uncertainty, multistate components, failure dependency, time dependence and expert and factual knowledge. During the recent years, BNs have gained good attention and are being utilized for engineering reliability and risk problems [12, 13, 14, 15, 16, 17]. Joint distributions of plenty of random variables can be handled efficiently in the directed acyclic network by the BNs, which are the probabilistic graphical models [18, 19]. Examples of BNs applications to the railway industry are few in number. For example, in [20] using BNs to illustrate a parameterized FTA for Signal Passing At Danger (SPAD); in [21] BNs model has been developed to recognize and classify the bugs in rail system based upon the sensor data; in [22] a BNs perspective has been proposed in order to model the inventive relationships for subway systems amidst the risk factors.The accuracy and certainty problems can be resolved by using combinatorial methods using static fault tree analysis [32]. As a result of some useful studies, it is believed that Bayesian Networks analysis method is one of the most efficient and appropriate one for reliability evaluations of the systems [33].Although, at the moment there exist no research available for modeling risk and reliability within the complex railway systems. This has been characterized by many different modern features which will be described in the section 5 of this paper. Moreover, the calculation of IMs for such complex systems like railway, by using BNs is yet to be explored until now. Therefore, unique and innovative work with respect to calculation of IMs as well as modeling and analysis of such complex features for the railway systems with the use of BNs is present in this article.

Description of the complex engineering problem

Certain combinations of events can lead to railway accidents. SPAD, which means that trains do not stop prior to a signal that shows red light, might be due to a combination of failure in Train Protection and Warning Systems (TPWS), driver errors, slip between rail and wheel and so on. After a train passes a red signal, different scenarios can develop, leading to different consequences. For example, the train or an individual vehicle leave the tracks on which it had been running, or it might collide with infrastructure or another train, leading to the damage to people, assets, environment and the functioning of the railway systems. A lot of severe accidents due to SPAD have occurred in railways in the last decades. According to a recent research, SPAD caused the most lethal collisions and train derailments which took place in European countries since 1980 [23]. SPAD can occur due to a number of factors and failures. SPAD may occur due to faulty brakes, high speed of train, faulty signals and due to the wrong reading and response of train driver to the cautionary signals. For the purpose of SPAD prevention, TPWS and automatic signaling are the mechanisms present in modern railways. Due to the mechanism of automatic signaling, the possibility of proceeding further to the trains is provided and an adequate distance is maintained in between the trains to avert the possibility of an accident. Safe train movement is further ensured with the usage of TPWS which are the mechanisms to automatically apply brakes in case of the train exceeding the permissible or design speed. The event of SPAD can ultimately result into an unfortunate event like train derailment. The event of train derailment can occur in case of not setting up of the turnout/point ahead in overlap length, which might occur if the signal is positioned a bit earlier than the entrance of section which is being protected through it or in case of high train speed and presence of a sharp curve in overlap length. A number of repercussions to the people, environment, operational processes and infrastructure can be caused due to the train derailment. A number of dependencies are present amongst the factors which are sources of the derailment of train. For instance, the high speed of train is regarded as a common reason of failure; slip and the inability to apply brakes are disjoint events; there exists failure dependency between TPWS and the driver errors; the driver errors are not time independent; functional uncertainty exists for the derailment scenarios. In addition, accident scenarios which

originate from the derailment of train, leading towards consequences have dependence due to shared neutralizing factors and barriers.

Definitions of the IMs

In this paper, risk and reliability related IMs have been discussed, that have already appeared in literature [1, 2, 24, 25, 26, 27, 28, 29, 30, 31]. In the definitions in table 1, failure probability of the system is represented with (F_s) which is calculated as the function of components(F_i)'s probability$Pr(F_i)$.

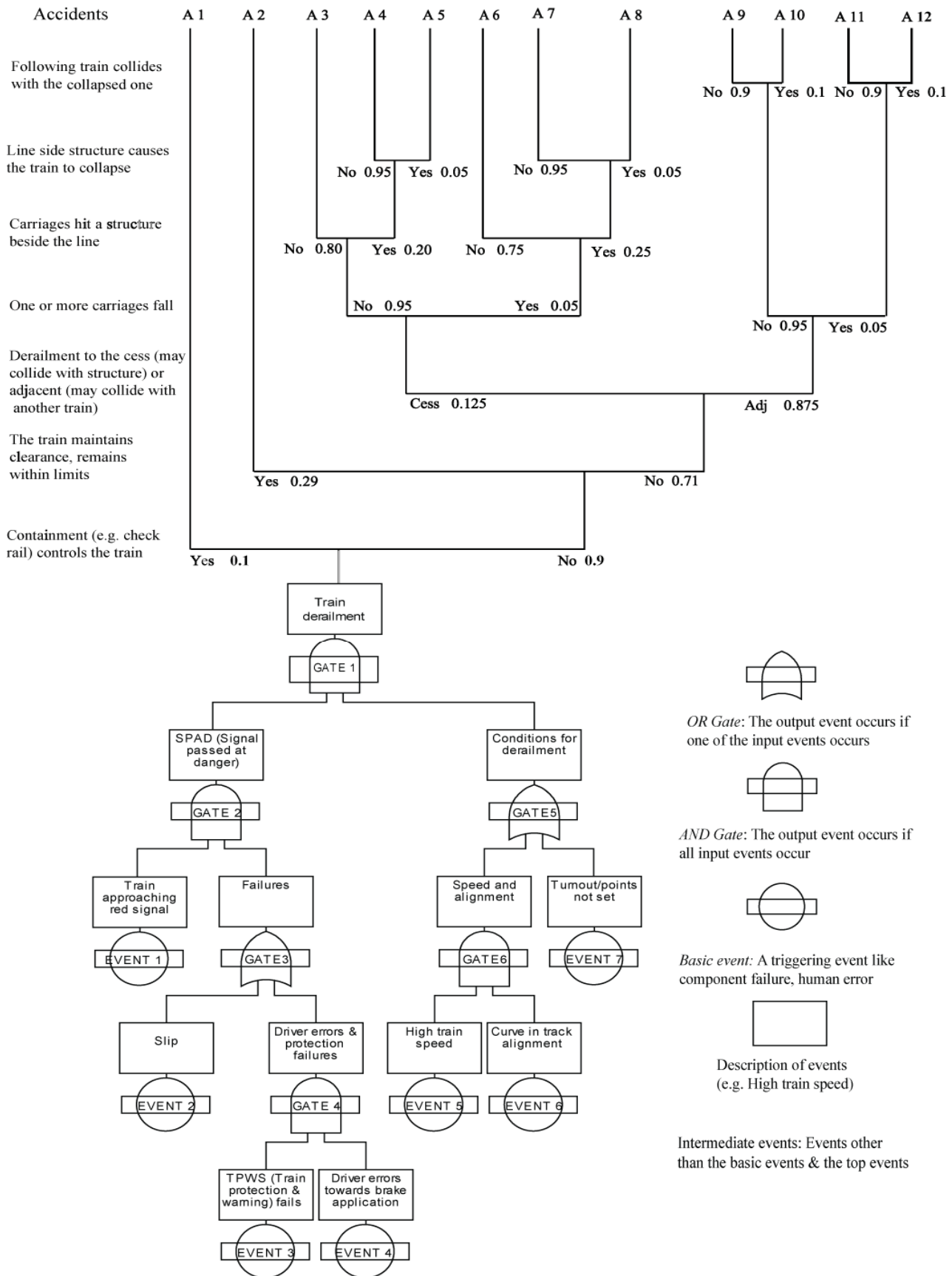**Table 1**. IMs related to Risk and reliability and their definitions.

IMs and their description	Mathematical definitions
Improvement Potential (IMP): It gives improvement capability of the system if failed component within the system is replaced by a perfect one.	$IMP_{(i)} = Pr(F_i) \cdot BIM_{(i)}$
Criticality Importance Factor (CIF): It gives the probability that individual component F_i is the reason of system failure if given$Pr(F_s)$.	$CIF_{(i)} = \dfrac{Pr(F_i)}{Pr(F_s)} \cdot BIM_{(i)}$
Fussell-Vesely (FUV) measure: The standard FusselVesely FUV failure importance measure is the involvement of probability of the component $Pr(F_i)$ to probability of system$Pr(F_s)$. Note that $FUV_{(i)} = 1 - \frac{1}{RRW_{(i)}}$.	$FUV_{(i)} = \dfrac{Pr(F_s) - Pr(F_s\vert\overline{F_i})}{Pr(F_s)}$
Birnbaum's Measure(BIM): It shows the vulnerability of a system unreliability with respect to changes in probability of component $Pr(F_i)$	$BIM_{(i)} = \dfrac{\partial\, Pr(F_s)}{\partial\, Pr(F_i)}$
Diagnostic Importance Factor(DIF):It gives probability of component $Pr(F_i)$if given the probability of system $Pr(F_s)$	$DIF_{(i)} = \dfrac{Pr(F_s \cap F_i)}{Pr(F_s)}$
Risk Reduction Worth(RRW): It calculates the reduction in system unreliability by increasing reliability of component F_i	$RRW_{(i)} = \dfrac{Pr(F_s)}{Pr(F_s\vert\overline{F_i})}$

Risk Achievement Worth (RAW): It calculates the value of the component F_i in attaining existing level of the reliability of the system.	$RAW_{(i)} = \dfrac{Pr(F_s\vert F_i)}{Pr(F_s)}$
Conditional Probability (COP): It gives the $Pr(F_s)$ if given the $Pr(F_i)$	$COP_{(i)} = \dfrac{Pr(F_s \cap F_i)}{Pr(F_i)}$

Techniques for reliability and risk analysis

Fault Tree Analysis (FTA)

The FTA is the top-down approach in which a tree structure is used for finding logical combinations of the reasons of Top event (Te). System analysis is done during the context of the environmental conditions and safety and functional requirements. All those combinations of the basic events which lead towards the occurrence of Te are identified. Basic assumptions associated with standard FTA include: (1) Events in the FTA are assumed to represent random variables consisting of two binary states, either occurring or not occurring (2) Basic events are assumed to be statistically independent. In Figure 1, a cause and consequence based Safety Risk Model (SRM) is presented. The causes of train derailment are modelled using FTA while consequences are modelled with the help of ETA. In Figure 1, lower part of Te is FTA, also discussed in [7]. Possible conditions for the occurrence of top event Te are shown in FTA. For instance, an intermediate event of SPAD will take place when the train is moving towards a red signal and also there are: (1) simultaneous failures of TPWS and Driver errors (2) slippage due to inadequate adhesion between rail and wheels. The Te of Train Derailment can take place when two conditions follow the SPAD, which are: (1) a Turnout/point with blocked route (2) presence of a curve in the track alignment (CTA) in addition to the High Train Speed (HTRS). It is considered that the driver is unaware of the slippery track conditions; hence he cannot care for the aspects related to slip during the brake application. Table 2 summarizes the scenarios and frequencies of the basic events which lead towards the occurrence of the Top event. It is worth mentioning that in the FTA, only the Failure Frequencies (FAF) and Fixed Unavailability Values (FU) are used for the basic events. For instance, failure of one driver on demand of 1000 brakes application, Speed limit crossed by 15 out of 100 locomotives while crossing a signal, one failure per 100000 demands of TPWS and failure of pre setting up of each tenth turnout/point.

S.A. Raza, Q. Mahboob, A.A. Khan, T.A. Khan, J. Hussain

Accidents

A 1 A 2 A 3 A 4 A 5 A 6 A 7 A 8 A 9 A 10 A 11 A 12

Following train collides with the collapsed one

No 0.9 Yes 0.1 No 0.9 Yes 0.1

Line side structure causes the train to collapse

No 0.95 Yes 0.05 No 0.95 Yes 0.05

Carriages hit a structure beside the line

No 0.80 Yes 0.20 No 0.75 Yes 0.25

One or more carriages fall

No 0.95 Yes 0.05 No 0.95 Yes 0.05

Derailment to the cess (may collide with structure) or adjacent (may collide with another train)

Cess 0.125 Adj 0.875

The train maintains clearance, remains within limits

Yes 0.29 No 0.71

Containment (e.g. check rail) controls the train

Yes 0.1 No 0.9

Train derailment

GATE 1

SPAD (Signal passed at danger)

GATE 2

Conditions for derailment

GATE 5

Train approaching red signal

Failures

Speed and alignment

Turnout/points not set

EVENT 1

GATE 3

GATE 6

EVENT 7

Slip

Driver errors & protection failures

High train speed

Curve in track alignment

EVENT 2

GATE 4

EVENT 5

EVENT 6

TPWS (Train protection & warning) fails

Driver errors towards brake application

EVENT 3

EVENT 4

OR Gate: The output event occurs if one of the input events occurs

AND Gate: The output event occurs if all input events occur

Basic event: A triggering event like component failure, human error

Description of events (e.g. High train speed)

Intermediate events: Events other than the basic events & the top events

Figurer 1. Train derailment specific Safety risk model [7]

Table 2. Basic events forTrain Derailment's causes and their FAFand FIU

Basic Event	Explanation	FAF& FIU
Train proceeding towards red signal (e_1)	Train is running in the direction of a red signal	5×10^{-02}
Slip (e_2)	Train slides over rails caused by poor adhesion (before red signal)	5×10^{-02}
TPWS fails (e_3)	TPWS failure while passing the signal	1×10^{-05}
Driver errors in the application of brake (e_4)	Driver does not respond to a brake request in time	1×10^{-03}
High speed of the train (e_5)	Train speed greater than 60 miles/hour	15×10^{-05}
Curve in the track alignment (e_6)	After crossing a signal, Railway track is not linear	1×10^{-01}
Unsettled turnout/point (e_7)	A turnout/point averts a route after the red signal	1×10^{-01}

Generally, Probability of the Te, Pr(Te) in FTA is calculated as a function of minimal or least cut sets with the use of inclusion and exclusion principle,

$$\Pr(Te) = \sum_i^n \Pr(C_i)$$
$$- \sum_{i=2}^n \sum_j^{i-1} \Pr(C_i \cap C_j) + \cdots$$
$$+ (-1)^{n-1}$$
$$\cdot \Pr(C_1 \cap C_2 \ldots \cap C_n). \quad (1)$$

In equation above, $\Pr(C_i)$ indicates probability of the happening of least cut set $i$in a FTA and number of least cut sets is denoted by n. To calculate the probability of Te in Figure. 1 as a function of the Probabilities of least cut-sets:

$$\Pr(Te) = \Pr(e_1 \cap e_3 \cap e_4 \cap e_7) + \Pr(e_1 \cap e_2 \cap e_7) + \Pr(e_1 \cap e_3 \cap e_4 \cap e_5 \cap \Pr(e_1 \cap e_2 \cap e_5 \cap e_6) \quad (2)$$
$$= 2.837 \times 10^{-04}.$$

One can calculate the IMs by using equation (2) in Table 1. Here are shown only the calculations of all. IMs for basic event 1 denoted bye_1.

Improvement Potential (IMP): To calculate the improvement potential for the basic event 1, $\text{BIM}_{(e_1)}$is multiplied with the$\Pr(e_1)$. So, we get $\text{IMP}_{(e_1)} = 2.88 \times 10^{-04}$.

Criticality Importance Factor (CIF): For the calculation of CIF for event 1, all the values are available. So, we get CIF for the basic event as 1.

Fussell-Vesely Measure (FUV): We are concerned with minimal cut sets which involve a particular event in the standard FUV. Hence, Failure importance is calculated by considering the contribution of event e_i to overall failure of the system. The failure importance measure of FUV is calculated to be 1 for the basic evente_i.

Birnbaum's Measure (BIM): By taking partial derivative of equation (2) corresponding with$\Pr(e_i)$ gives$\text{BIM}_{(e_1)} = 5.75 \times 10^{-03}$.

Diagnostic Importance Factor (DIF): We can extend mathematical definition of the DIF which is given in Table 1 by replacing term $\Pr(Te \cap e_i)$with$\Pr(te|e_i) \cdot \Pr(e_i)$. We find $\text{DIF}_{(e_1)} = 1$.

Risk Reduction worth (RRW): We insert $\Pr(e_1) = 0$ in the equation (2) for $\Pr(Te|\bar{e}_1)$ and get $\text{RRW}_{(e_1)}$ as ∞.

Risk Achievement Worth (RAW): It is straightforward to calculate RAW for an individual basic event because of the availability of all values for it. So we calculated $\text{RAW}_{(e_1)} = 20$.

Conditional Probability (COP): For calculating$\Pr(Te|e_1)$, we use $\Pr(e_1) = 1$ in equation (2) and as a result, get $\Pr(Te|e_1) = 5.75 \times 10^{-03}$.

Values of IMs calculated from FTA are shown in the Table 3.

Table 3. Important Measures IMs calculated from FTA in Figure (1)

IMs	Event (e_1)	Event (e_2)	Event(e_3)	Event(e_4)	Event(e_5)	Event(e_6)	Event(e_7)
Improvement Potential (IMP)	2.88×10^{-04}	2.88×10^{-04}	9.50×10^{-09}	9.50×10^{-09}	3.75×10^{-05}	3.75×10^{-05}	2.50×10^{-04}
Criticality Importance Factor (CIF)	1	1	3.30×10^{-05}	3.30×10^{-05}	1.30×10^{-01}	1.30×10^{-01}	8.70×10^{-01}

S.A. Raza, Q. Mahboob, A.A. Khan, T.A. Khan, J. Hussain

Fussell-Vesely measure (FUV)	1	1	1.31×10^{-02}	1.31×10^{-02}	1.30×10^{-01}	1.30×10^{-01}	8.70×10^{-01}
Birnbaum Measure (BIM)	5.75×10^{-03}	5.75×10^{-03}	9.50×10^{-06}	9.50×10^{-06}	2.50×10^{-04}	3.75×10^{-04}	2.50×10^{-03}
Diagnostic Importance Factor (DIF)	1	1	1.02×10^{-03}	1.02×10^{-03}	2.61×10^{-01}	2.17×10^{-01}	8.83×10^{-01}
Risk Reduction Worth (RRW)	∞	5.07×10^{04}	1.01	1.01	1.15	1.15	7.67
Risk Achievement Worth (RAW)	20	20	1.02	1.02	1.74	2.17	8.83
Conditional probability (COP)	5.75×10^{-03}	5.75×10^{-03}	2.93×10^{-04}	2.93×10^{-04}	5.00×10^{-04}	6.25×10^{-04}	2.54×10^{-03}

Event Tree Analysis (ETA)

The ETA is a bottom-up method which is used to develop and analyze event situations that can arise from the Te, also known as the initiating event in the ETA and result into several potential consequences. The ETA shown here is adopted from [6] in which train derailment accidents for UK railways are analyzed. This work extends the ETA for train derailment with the introduction of Safety Integrity Levels (SIL), neutralizing factors and barriers for the different consequences. Classification of accidents is done on the basis of their severity levels. Such classification is compulsory in order to differentiate among the fatal, significant and insignificant accidents. Please refer to Table 4.

Table 4. SIL for the various consequences of the Te of train derailment

Severity class	SIL	Consequences
Disastrous corresponds to 100 or more than 100	4	A5, A8, A10 and A12

fatalities		
Catastrophic corresponds to up to 10 fatalities	3	A4, A7
Critical corresponds to up to 1 fatality	2	A11
Marginal corresponds to Major injuries	1	A6
Insignificant corresponds to Minor injuries	0	A1, A2, A3, A9

Probability of initiating event is multiplied by the probabilities of events which define each scenario in order to calculate the probability of the initiating event. For instance, Probability of the accident A5 is computed as:

$$2.837 \times 10^{-04} \cdot 0.900 \cdot 0.710 \cdot 0.125 \cdot 0.950 \\ \cdot 0.200 \cdot 0.050 \qquad (3) \\ = 2.153 \times 10^{-07}$$

Bayesian Networks (BNs)
BNs are comprised of a set of ellipses or nodes, corresponding to the continuous or discrete random variables in analyzed system and set of the directed links or arrows, representing probabilistic dependencies between the variables [18, 19]. Take the example of BNs which are shown in Figure. 2, which models the dependences between six random variables $X= [X_1, ..., X_6]$. In case the BNs comprise of the discrete random variables, each node will consist of a set of collective exhaustive and mutually exclusive states. The Conditional probability table is in a connection with a child node, used to describe conditional probability mass function of the discrete random variable if all of mutually exclusive states from its ancestors are given. The effect of dependent nodes on each other is specified by conditional probability tables. A node without any parents/ancestors will be having the unconditional or marginal probability table.
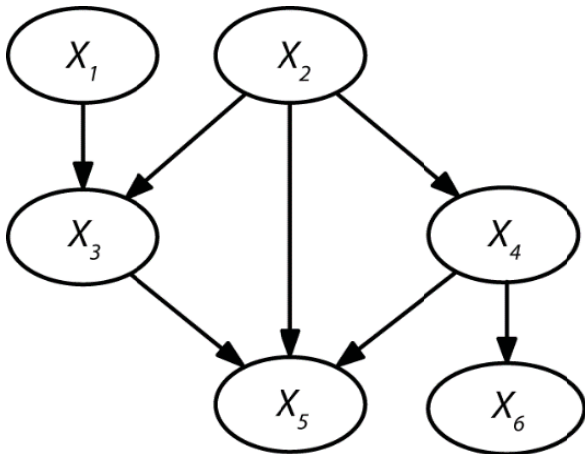
Figure 2. A simple Bayesian Network.

BNs provide a thorough depiction of joint probability distribution$p(x)$ of each variable in the network. The probability of each variable is defined depending on its parents and joint probability distribution of the BNs is given as a product of these conditional probabilities. For a generic case, this joint probability distribution is written as:

$$p(x) = p(x_1, ..., x_n) = \prod_{i=1}^{n} p[x_i \mid pa(x_i)] \qquad (4)$$

In the above equation, $pa(x_i)$ is a set of the realizations of ancestors of random variablesX_i. Numerical and graphical tasks are required for the construction of BNs. Defining the graphical model with regard to its nodes and causal relations or dependencies, is included in the graphical task. For instance, Figure. 2 shows the graphical model with its nodes and their structure of dependence.

Mapping of the risk models based on the FTA and ETA to the BNs: Parts of BNs and FTA are used for numerical and graphical mappings; Figure. 3 presents a simplified procedure of it. Nodes in BNs are classified in the following manner for better perception of mapping process, also shown in [9].

Root node of BNs: Root node is used for the representation of the basic events of FTA alongside the neutralizing factors and barriers of ETA. Barriers can be described by the occurrence, functionality and their effectiveness.

Neutralizing factors: which are also known as lucky circumstances, prevent the growth of hazard to an accident after barriers failure.
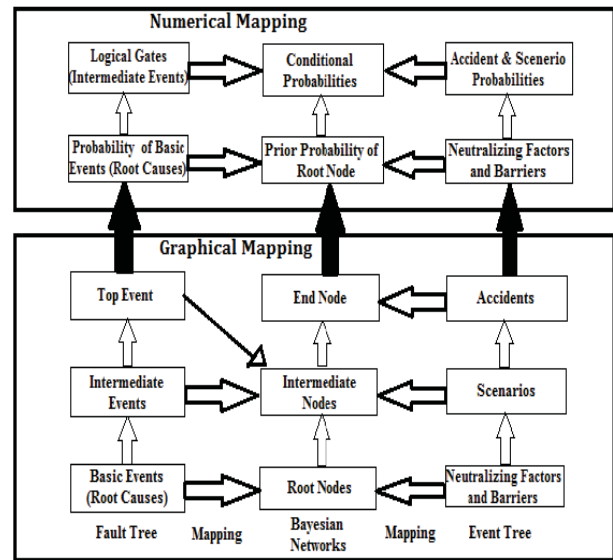

Figure 3. Mapping of the risk models based on the FTA and ETA to the BNs

Intermediate node of BNs:Intermediate scenarios in ETA and intermediate events in the FTA are represented through the Intermediate nodes of BNs.
Complete risk model of Figure. 1 is represented in BNs based model (Figure 4). Shorter names of the random variables are used for simplicity in BNs, 'fall' is said for at least one or more than one carriages fall. AND logic among the random variables, CTA and HTRS is presented in Table 5 for the Speed & Alignment (SA). To calculate the probability of SA=Yes:

$$\Pr(SA = Yes)$$
$$= \sum_{CTA,HTS} \Pr(SA = Yes \mid CTA \cap HTRS) \qquad (5)$$
$$\cdot \Pr(CTA \cap HTRS) \times 1.5 \times 10^{-02}$$

In equation (4), the basic events HTRS and CTAare statistically independent; which means that
$$\Pr(CTA \cap HTRS) = \Pr(CTA).\Pr(HTRS)$$

Table 5. Numerical mapping of the AND gate for the *SA* in FTA to an analogous probability table in the BNs

CTA	Yes		No	
HTRS	Yes	No	Yes	No
No	0	1	1	1
Yes	1	0	0	0

Calculation of the IMs by using BNs: In order to respond to the joint and marginal probabilities of

random variables in the BNs related questions, we put together standard Bayesian inference by using the variable elimination algorithm. Until this, BNs shown in Figure. 4 give the identical probability of Te and values of IMs as shown in Table 3.
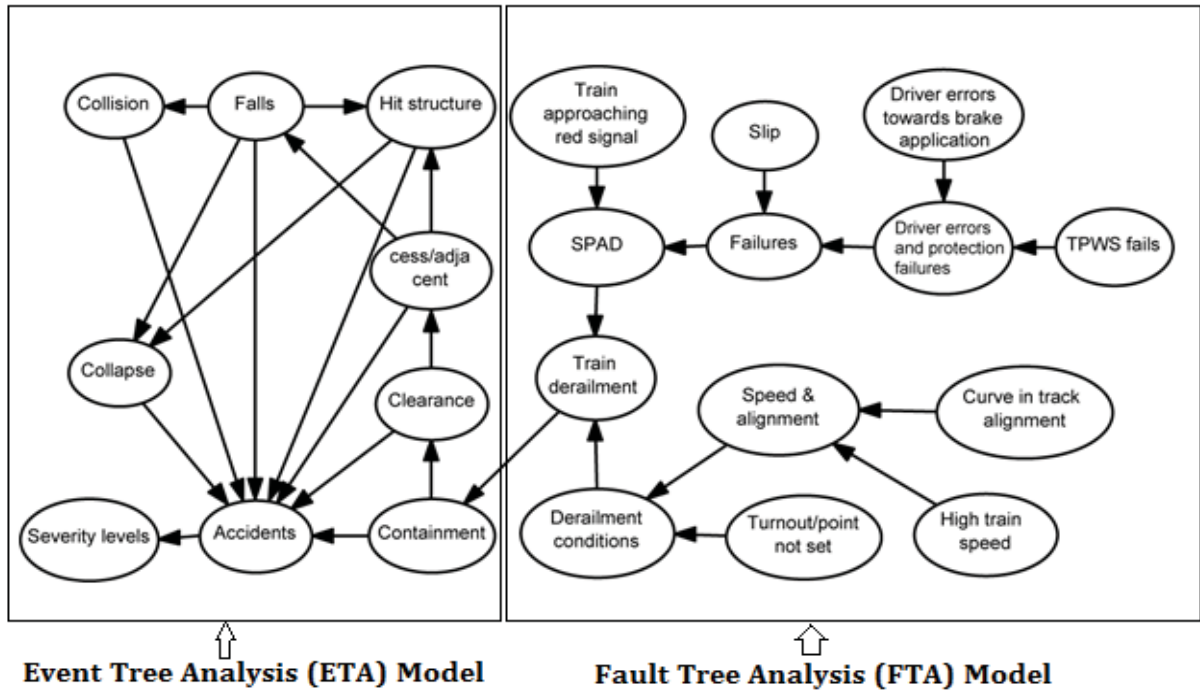

Figure 4. The BNs model equivalent to FTA & ETA based model in Figure 1

Quantification of the risk

Next step involves the calculation of the numerical values of *Individual Risk of Fatality (IRF)*. It is expressed with regard to *annual fatality rate* of someone (person) who gets vulnerable to a given condition at the given point of time. It is calculated as:

$$IRF = \sum_j N \left[HR_j(D_j + E_j) \sum_k (C_j^k F^k) \right] \qquad (6)$$

- N= Times an individual gets vulnerable to the hazards of the system
- j= Number of the hazards/risks
- HR_j= Rate for j^{th} hazard/risk(top event in the FTA)
- D_j= Time duration of the hazard j
- E_j= Vulnerability Time of an individual regarding the hazard$j$
- k = Total number of accidents
- $\sum_k(C_j^k F^k)$ =Parameters of risk reduction (C_j^k is the factor of risk reduction for the kth accident due to the jth hazard and F^k is probability of the fatality in kthaccident). Factor of the risk reduction is calculatedfrom consequence

models, i.e., Event Tree for the train derailment consequences.

Fatalities are most specific aspects to look for in the railway risks, hence; in Table 6, just factor of risk reduction C_j^k for those accidents which correspond to the severity levels 2, 3and 4 (0.0278 + 0.0170 + 0.063 = 0.1078) are given thought for IRF. SIL 0 and SIL 1 are the categories which are averted during calculation because they do not result in the human fatalities apparently.

Table 6. Risk reduction factors calculated from models in Figure. 1 and Figure 5

Class of severity	SIL	C_j^k
Disastrous corresponds to up to 100 or more fatalities	4	0.063
Catastrophic corresponds to up to 10 fatalities	3	0.0170
Critical corresponds to1 fatality	2	0.0278
Marginal corresponds to Major injuries	1	0.0033
Insignificant corresponds to Minor injuries	0	0.889

Following are the extra numerical values for IRF: $HR = 2.837 \times 10^{-04}$ from FTA, $N = 600$ times/year. Usually, an individual makes use of the train twice each day and 300 days a year), $j = 1$ (one hazard or Top event (Te), $D_j = 5$ hours (average maintenance or negating time for the hazard situations because of failure), $E_j = 0.05$ hour (time to observe and cross a red signal and an overlap length), $C_j^k = 0.1078$ and $F^k = 0.01$. Numeric value of IRF is 9.28×10^{-04} Per year. Until then, numeric valueof IRF is equal to risk models in Figure 4 and Figure 1as they are comparable.

Complex aspects of the engineering problem

Complex aspect # 01: Common causes of failure
The FTA in Figure 1 takes for granted that basic events are statistically independent. It is not true. Occurrence of slip requires a high speed of the train. Hence, HTRS is a mutual Cause, also known as the common cause failure. Not paying attention to such common causes results in two types of risks, which are either (1) Overestimated in case of dominance by the series (OR gate) components, or (2) Underestimated in case FTA having a large number of components in the parallel (AND gate).

Complex aspect # 02: Disjoint events
Basic event of *Slip* and the intermediate event of the *Driver Errors and Protection Failures* cannot take place together, because prior application of brakes is required for slip to occur. These are mutually exclusive or disjoint events and hence, are statistically not independent.

Complex aspect # 03: Multistate system and components
Events of the standard FTA correlate with the random variables having binary states i.e. fail/success. It is not possible to directly model the mutually exclusive system states or multistate components using FTA. For example, for derailment of the train due to SPAD, we need to differentiate two different states of the system or situations. *Situation 1:* SPAD takes place because of the slip effectbrought about by the poor adhesion. It implies that while passing a red signal, brakes are applied. In this condition, Top event of the train derailment will only take place if distance between turnout point in overlap length and the signal is adequately small. Else, train will stop before turnout point. Train derailment because of the curvature in track is minor considering the prior train speed limitation due to the brake application. *Situation 2:* SPAD takes place because of not applying the brakes, like the occurrence ofintermediate event *of Driver errors and protection failures*. In this condition, top event takes place independent of the overlap length because of: (1) a turnout in subsequent section with blocked route (2) a curve in subsequent section. It means that in addition,

two basic events are required for the modeling of multistate system (See Table 7).

Table 7. Basic events to model multistate event for the train derailment model

Event	Description	FAF & FIU
Poor adhesion	Absence of the adequate adhesive forces among the rails and train wheels.	0.03
Shorter overlap length	Distance between turnout ahead and (last) signal is ≤ 200 m	0.005

Complex aspect # 04: Dependency of the Failure
Failure of a single component can result into the increased or decreased trend for other components in the system to fail. For instance, it is logical to believe that probability of the intermediate event *Driver errors & protection failures* will be increased in case TPWS failEarlier than the driver errors. Secondly, in case of TPWS Failures, probability of the driver errors will be increased.

Complex aspect #05: Dependencies of the Time
Time dependent event is present there in the FTA. The probability of the driver to commit errors enhances over time, specifically when driver needs to carry out longer than routine duty hours. It means, probability of e_4 changes with time, which also affects probability of the Te in time.

Complex aspect# 06: Uncertainty about the Function and factual knowledge
Uncertainty of the failure emerges in case of track section, involving both turnout/point and curve in track alignment not set. Tendency for derailment will be increased in case train enters within this section, after SPAD has taken place. Furthermore, the actions of replacement, repair and maintenance which have been taken in past inform that no overlap length exists having both *Turnout/point* and *Curve in track alignment.* Hence, failure logic OR must be replaced by XOR for the *Conditions for derailment* (see Table 8).

Table 8. XOR logic for the derailment Conditions

Speed and alignment (SA)	Yes		No	
Turnout/point not set	Yes	No	Yes	No
No	1	0	0	1
Yes	0	1	1	0

Complex aspect #07: Uncertainty in the expert knowledge
In the absence of enough historical data for the risks quantification, estimation of the occurrence probability of some events is done by consulting the experts in field.

At times, experts disagree on probability of the occurrence of an event. For instance, two experts have dissimilar opinion on probability of the *CTA* which will result into the Te.

Complex aspect #08: Dependencies and Simplifications in the ETA

The ETA shown in Figure 1 is used to simplify the event scenarios resulting into the consequences, hence it is unable to include several barriers and the neutralizing factors. According to the system characteristics, some barriers and neutralizing factors might exist in ETA which are evenly valid for FTA. Also, dependencies between the barriers and neutralizing factors are not given thought here.

Some of the aforementioned complex aspects addressed above can be applied by using the complex FTA techniques [10]. By incorporating three complex aspects:

Disjoint events, multistate system and common causes into the model, structure of FTA explodes and becomes non-intuitive as shown in Figure. 5. Also, by introducing a new common cause, structure of the FTA may become different. Quantitative analysis of the FTA becomes computationally challenging and needs the help of computerized techniques for its evaluation.

For instance, because of the repetition of gates in Figure 5, common causes have enhanced up to six. Thus, 2^6 common cause event spaces are required for the computation of probability of Te. Thereby, Total probability theorem will then be used to compute the probability of Te:

$$\Pr(Te) = \sum_{i=1}^{2^6} \Pr(te|CCE_i) \cdot \Pr(CCE_i) \qquad (7)$$

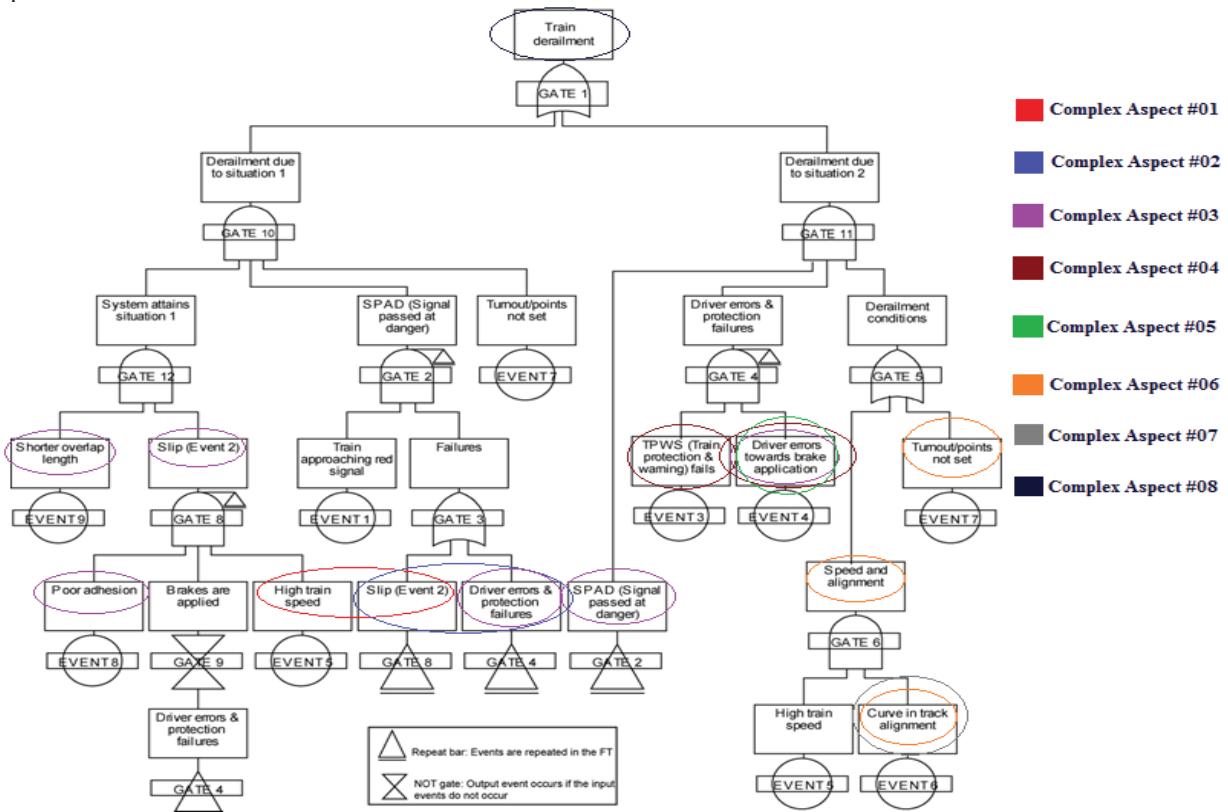Above and other constraints are avoidable using BNs.

Figure 5. Train Derailment's FTA after considering the complex aspects

Implementation of complex aspects of train derailment model by using BNs

In BNs, we can directly introduce the common causes with the addition of relevant links, without duplicating the nodes. We consider the common cause of *HTRS* with the introduction of the link from HTRS to SA and *Slip*. Disjoint events are directed to be modeled with the addition of a link among relevant random variables and

afterwards consequently placing values in conditional probability table of child node. For instance, events of *driver errors and TPWS failure* and *slip* are exclusive with each other, as elaborated in the section 5. A link is introduced from node *Drive errors and TPWS failure*, and probability of the slip is set to zero, given *Driver errors and TPWS failure* (in Table 9, compare column 2 and 3).

Table 9. Conditional probability table for the *Slip* node.

High Train Speed (HTRS)	Yes				No			
Poor adhesion	Yes		No		Yes		No	
Driver errors & TPWS failures	Yes	No	Yes	No	Yes	No	Yes	No
No slip	1	0	1	1	1	1	1	1
Slip	0	1	0	0	0	0	0	0

We can directly represent the multistate system with the introduction of the relevant random variablesituationsin BNs. Table 10 shows a Conditional Probability Table (CPT) for two conditions. CPT connected with child nodes can also be used to manage the failure dependency between system components i.e. random variable in the BNs. For instance, increased tendency of happening of *Driver errors and TPWS failure* is shown in column 3 of the Table 11,when the event of *TPWS failure* takes place before *driver errors.* Formerly, it was used as an AND gate in FT model presented in Figure 1.

Table 10. CPT for the node *Situations*

Overlap length	Yes				No			
Driver errors &TPWS fails	Yes		No		Yes		No	
Slip	Yes	No	Yes	No	Yes	No	Yes	No
Situation 1	-	0	1	0	-	0	0	0
Situation 2	-	1	0	0	-	1	0	0

Table 11. CPT for Driver errors& TPWS failures

TPWS Fails	Yes		No	
Driver errors towards brake application	Yes	No	Yes	No
No	0	0.95	1	1
Yes	1	0.05	0	0

The temporal node named Driver error towards the brake application (DE) is establishedwith the conditional probability table, which develops over time and is used to model the transition probability. Period of transition is supposed to be about 10 minutes which is equal to the 10th order Markov chain in BNs in the Figure 6. Here, $p(DE_{t-10}) = 1$ andp$\left(\underline{DE_{t-10}}\right) = 0.005$. In order to model the functional uncertainty, conditional probability valuep(Train derailment | SPAD, Speed &*alignment, Turnout point not set*) = 0.1 is allocated to a table connected with node *Train derailment*. Modeling of the factual information by using BNs is unequivocal, by connecting a conditional probability table with node *Derailment conditions* byusing XORlogic gate as shown in the Table 8. A node named as *Expert knowledge* is initiated in BNs and probabilities of the *CTA* subject to states of the node are described. Probabilities of the *CTA* provided *Expert* 1 and *Expert* 2 are 0.1 and 0.2, accordingly. Furthermore, we can include the reliabilities of two experts on their decision. For instance, someone thinks the expert 1 as more reliable than expert 2, hence, assigns their respective probabilities as per 0.55 and 0.45. The resultant BNs after the application of complex aspects is illustrated in Figure 6.
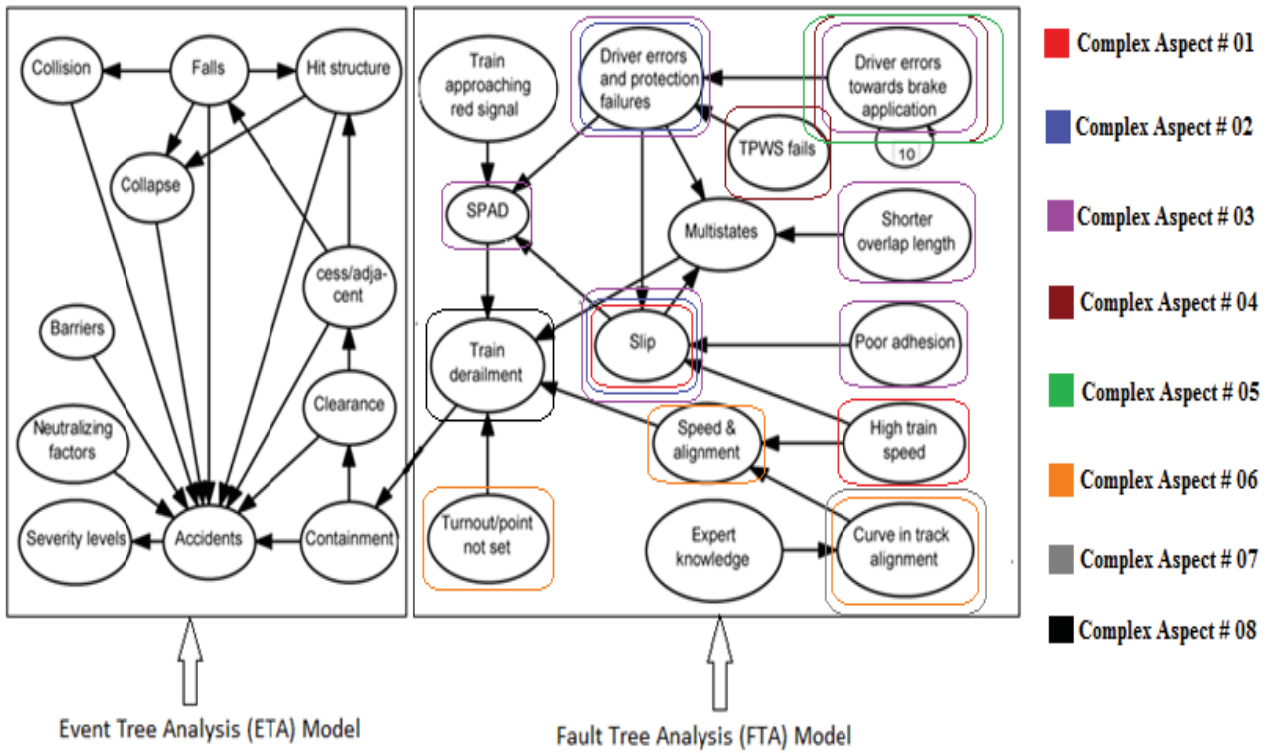
Figure 6. Safety risk model based on the BNs including the complex aspects of FTA & ETA based safety risk model

Table 12. Values of the IMs from BNs after considering complex aspects

IMs	Event(e_1)	Event(e_2)	Event(e_3)	Event(e_4)	Event(e_5)	Event(e_6)	Event(e_7)
Improvement Potential (IMP)	4.02×10^{-07}	1.07×10^{-06}	3.05×10^{-07}	5.68×10^{-09}	1.48×10^{-07}	2.43×10^{-08}	3.47×10^{-07}
Criticality Importance Factor (CIF)	1	2.66	7.57×10^{-01}	1.41×10^{-02}	3.67×10^{-01}	6.03×10^{-02}	8.62×10^{-01}
Fussell-Vesely measure (FUV)	1	2.40×10^{-01}	7.57×10^{-01}	1.41×10^{-02}	3.67×10^{-01}	8.74×10^{-02}	8.62×10^{-01}
Birnbaum Measure (BIM)	8.05×10^{-06}	2.14×10^{-05}	3.05×10^{-04}	5.68×10^{-06}	9.85×10^{-07}	2.43×10^{-07}	3.47×10^{-06}
Diagnostic Importance Factor (DIF)	1	2.70	7.57×10^{-01}	1.51×10^{-02}	4.62×10^{-01}	1.52×10^{-01}	8.76×10^{-01}
Risk Reduction Worth (RRW)	∞	1.32	4.11	1.01	1.58	1.10	7.26
Risk Achievement Worth (RAW)	20	5.40×10^{01}	7.57×10^{02}	1.51×10^{01}	3.08	1.52	8.76
Conditional probability (COP)	8.05×10^{-06}	2.17×10^{-05}	3.05×10^{-04}	6.08×10^{-06}	1.24×10^{-06}	6.10×10^{-07}	3.53×10^{-06}

IMs values related to the reliability and risk of a number of events in BNs shown in Figure. 6 have got updated. Diagnostic analysis or backward updating which provides important information regarding most probable purpose of a specific Te i.e.$\Pr(e_1 \mid e_6)$ cannot be done with the FTA. Apart from the fact that BNs offered the calculation of IMs for a complex system model, the extra edge while using the BNs was the complex modeling of the joint distribution of random variables which resulted in the brief visualization of the reliability and risk problem. BNs can update the probabilities, nominal beliefs of all the random variables in BNs, through bidirectional (backward and forward) transmission of the evidence through whole network. This bidirectional updating helps the BNs to tackle several Te in the same model.

Conclusions

A number of complex aspects and their consequences on quantitative reliability and safety analysis of complex engineering system from the field of railways were considered. The probabilities of Te and IRF per year were reduced by considering complex aspects of the railway operations. The BNs with complex aspects resulted in lower values of Importance Measures and fatality risks. The application of complex aspects using BNs was possible and an improved calculation of the importance measures for complicated system was achieved. It is concluded that system risks were overestimated by safety models in the absence of the complex aspects, which were complicated to model using Fault Tree and Event Tree based risk models.

References

[1] Olde Keizer, M., Flapper, S., Teunter, R., "Condition-based maintenance policies for systems with multiple dependent components: a review, "*European Journal of Operational Research*, 261(2): pp. 405-420, 2017.

[2] de Jonge, B., Klingenberg, W., Teunter, R., Tinga, T., "Reducing cost by clustering maintenance activities for multiple critical units, "*Reliability Engineering and System Safety*,145: pp. 93-103, 2016.

[3] Do, P., Voisin, A., Levrat, E., Iung, B.,"A proactive condition-based maintenance strategy with both perfect and imperfect maintenance actions,*" Reliability Engineering and System Safety,* 133, pp. 22–32, 2016.

[4] Rasay, h., Fallahnezhad, M.S., zaremehjerdi, Y., "Application of multivariate control charts for condition based maintenance, "*International Journal Of Engineering*, 31(4): pp. 597-604,2018.

[5] Zhang, X., Zeng, J., "A general modeling method for opportunistic maintenance modeling of multi-unit systems, "*Reliability Engineering and System Safety*, 140: pp. 176–190, 2015.

[6] Ahmadi, R., Newby, M., "Maintenance scheduling of a manufacturing system subjected to deterioration, "*Reliability Engineering & System Safety*, 96: pp. 1411-1420, 2011.

[7] Zhao, J., Chan, A.H.C., Roberts, C., Madelin, K.B., "Reliability evaluation and optimization of imperfect inspections for a component with multi-defects, " *Reliability Engineering & System Safety*, 92: pp. 65-73, 2017.

[8] Liu, Y., Huang, H.Z.,"Optimal replacement policy for multi-state system under Imperfect Maintenance, "*IEEE Transactions on Reliability*, 59: pp. 483-495, 2011.

[9] Zhang, Z., Shen, J., Ma, Y., "Optimal maintenance policy considering imperfect repairs and non-constant probabilities of inspection errors," *Reliability Engineering & System Safety*,193: pp. 106-118, 2020.

[10] Pham, H., Wang, H.,"Imperfect maintenance*, " European journal operation research*, 94: pp. 425-38, 1996.

[11] Wu, S., Zuo, J.M.,"Linear and nonlinear preventive maintenance models, "*IEEE Transactions on Reliability,* 59(1): pp. 242-9, 2010.

[12] Wang, L.,"A survey of maintenance policies of deteriorating systems, " *European Journal of Operational Research*, 139 (3), pp. 469-489, 2002.

[13] Shafiee, M., Finkelstein, M., "A proactive group maintenance policy for continuously monitored deteriorating systems: Application to offshore wind turbines, " *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability,* 229 (5): pp. 373-384, 2015.

[14] Shafiee, M., Finkelstein, M., Berenguer, C., " An opportunistic condition-base maintenance policy for offshore wind turbin blades subjected to degradation and environmental shocks, "*Reliability Engineering and System Safety*, 142: pp. 463-471, 2015.