Comparison of Fault Tree and Bayesian Networks for Modeling Safety Critical Components in Railway Systems

Q. Mahboob
Pakistan Railways, Lahore, Pakistan

D. Straub
Engineering Risk Analysis Group, TU München

ABSTRACT: In spite of reliable signaling and train protection and warning systems, trains are still passing red signals even in modern railway systems. These so-called SPAD events can lead to train derailment, head on collisions with other trains, collisions with infrastructure and other adverse consequences. The classical way of modeling such events is by means of Fault Tree (FT) analysis. However, the FT methodology has limitations when modeling complex systems. This motivates an investigation into the use of Bayesian Networks (BN) for modeling and analyzing SPAD and other safety critical events in railway systems. BN allows combining systematic, expert and factual knowledge about the system and is a flexible and compact form of system representation. In this paper, it is studied by means of the SPAD example whether the use of BN provides significant advantages over the FT methodology for modeling safety risks in railway systems. The causes of train derailment due to SPAD are summarized and the FT and BN methods are compared with respect to different modeling and analysis aspects that are relevant for railway systems.

1 INTRODUCTION

Modern railway systems are equipped with automatic signaling and train protection and warning systems (TPWS) that control train movement and ensure the attention of the driver. In spite of reliable signaling and TPWS, trains are still passing signals at dangers (so-called SPAD events) (Duffey, et al., 2003). These SPAD events can lead to train derailment, head on collision with another train, collision with infrastructure and other adverse consequences. A significant number of severe accidents caused by SPAD occurred in the recent past (Whittingham, 2004). A recent study shows that the most fatal collisions and train derailments in Europe since 1980 were caused by SPAD (Evans, 2011).

Investigations have been carried out to identify the critical components that lead to SPAD and train derailment due to it. The classical way of modeling such events is by means of Fault Tree (FT) analysis, which allows modeling and analyzing safety critical components in engineering systems. It is a top-down approach, which provides a logical framework for understanding and assessing the scenarios leading to system failure. The FT method is well explained in (Limnios, 2007) and (NASA, 2002). Examples of FT applied to railway systems include the modeling of errors made by train drivers (Dhillon, 2007), reliability evaluations of railway power supply (Chen, Ho, & Mao, 2007) and safety analysis of railway brake system (Heilmann, et al., 2007).

The FT methodology has limitations in modeling complex systems. This motivates an investigation into the use of Bayesian Networks (BNs) for modeling and analyzing SPAD and other safety critical events in railway systems. BNs are probabilistic models that enable a concise representation of the dependence among random variables. The BN allows combining systematic, expert and factual knowledge about the system and is a flexible and compact form of system representation (Khakzad, et al., 2011). References on the application of BNs to engineering safety, risk and reliability can be found in (Straub & Kiureghian, 2010) and (Lampis & Andrews, 2009). Only few examples of BN applied to railway systems can be found. (Marsh & Bearfield, 2007) use BN for the representation of a parameterized fault tree for SPAD; (Oukhellou, et al., 2008) develop a BN model for identifying and classifying rail defects based on sensor data.

In this paper, it is studied whether the use of BN provides significant advantages over the FT methodology for modeling safety risks in railway systems. The causes of train derailment due to SPAD are analyzed and the safety risk model train derailment due to SPAD is constructed using FT and then translated into a BN. The two methods are compared with respect to different modeling and analysis aspects that are relevant for railway systems.

2 SIGNAL PASSING AT DANGER (SPAD)

SPAD events occur when trains do not stop before a red light. SPAD can be caused by faulty brakes, high train speed, defective signals and train drivers wrongly reading and responding to cautionary signals (Whittingham, 2004). SPAD events can lead to train derailment, collision with infrastructure or collision with other trains. To prevent SPAD, modern railways have automatic signaling systems, which stop the trains whenever components of the system fail to perform their function. These signals ensure an adequate distance between the trains to avoid collisions. Train drivers follow these signals along the railway track in order to proceed further and switch railway lines. Additionally, trains are equipped with train protection and warning systems (TPWS) that further ensure safe train movement. This system prevents SPAD by automatically applying the brakes if the train speed is too high.

3 FAULT TREE MODELLING

The Fault Tree (FT) is a common technique used for logical representation of a technical system for the purpose of safety and reliability analysis. It provides a rational framework for modeling the possible scenarios leading to system failure. It is a deductive method in which an undesired event – called Top Event (TE) – is postulated and the scenarios leading to the TE are identified. These scenarios originate from so-called basic events, and are described by a series of logical operators and intermediate events leading to the TE. The system is analyzed in the context of its operational and safety requirements and environment to find all combinations of basic events that will lead to the occurrence of the TE (Stewart & Melchers, 1997). The basic assumptions of the standard FT methodology are

- the FT is based on events, it can thus only represent random variables with binary states;
- basic events are statistically independent;
- the relationship between events is represented by logical gates.

The basic constituents of the FT analysis used in this paper are shown in Figure 1 and explained below.

- *Basic event*: a triggering event for the TE, e.g. human error, failure of a system component.
- *Intermediate event*: events other than TE & basic events, defined through gates.
- *OR gate*: the output event occurs if one of the input events occur;
- *AND gate*: the output event occurs if all input events occur;
- *NOT gate*: the output event occurs if the input event does not occur;
- *Repeat bar*: the intermediate event (and the events leading to it) are repeated.

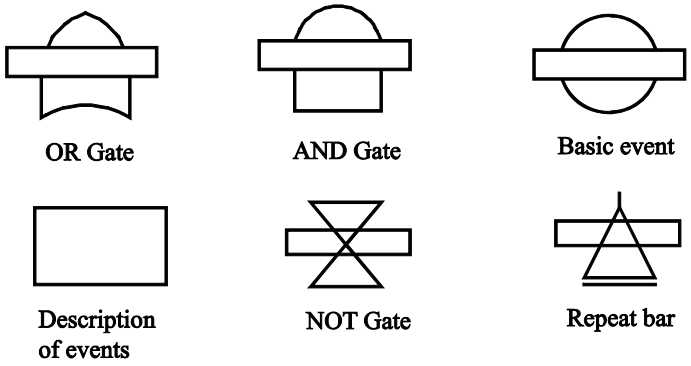

Figure 1. Graphical symbols for Fault Tree.

In the quantitative analysis of the FT, the probability of the TE is computed as a function of the probability of the basic events, by identifying (minimal) cut-sets. Algorithms for these computations are provided in (Bertsche, 2008) and (Aven, 2008). By using importance measures, the criticality of each basic event towards system failure can be determined (Borgonovo, et al., 2003). Here, the diagnostic importance factor $DIF_{(E)}$ from (Assaf & Dugan, 2004) is used, which for the basic event E is defined as the conditional probability of E given system failure F_S:

$$DIF_{(E)} = \Pr(E|F_S) = \frac{\Pr(F_S \cap E)}{\Pr(F_S)} \quad (1)$$

This importance measure has the disadvantage that it strongly depends on the marginal probability of the basic event E. (If the event has probability $\Pr(E) = 1$, the $DIF_{(E)}$ is always 1, independent of the logical relation between E and F_S.)

3.1 *Modeling SPAD and subsequent train derailment using fault tree*

Figure 2 shows the FT for SPAD from (Marsh, et al., 2007). This FT represents a railway system with TPWS. The possible scenarios leading to SPAD are (a) the combined failure of TPWS and driver errors, and (b) a failure to break because of slip between the wheels and the rails, which is caused by high train speed and poor adhesion. The basic events of these two scenarios are summarized in Table 1.

Table 1. Basic events in the fault tree for SPAD.

Basic event	Description
Train approaching red signal	Train is running towards a red signal
Slip	Sliding of train due to poor adhesion
TPWS fails	TPWS fail while passing a signal
Driver errors in brake application	Driver fails to react to a signal in time

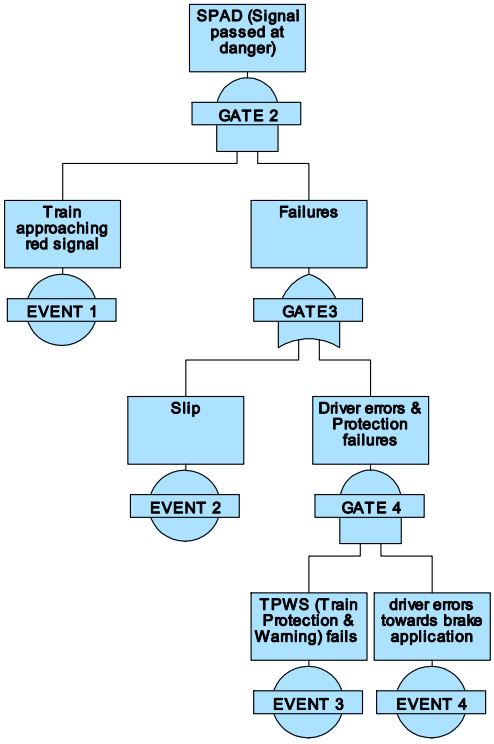

Figure 2. Fault tree for SPAD, after (Marsh, et al., 2007).

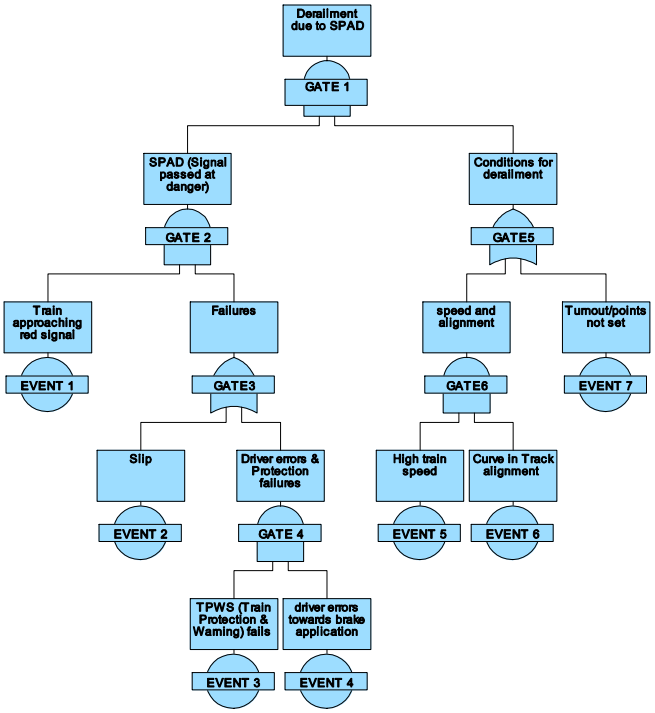

Figure 3. Fault Tree for train derailment due to SPAD.

SPAD events can lead to a number of possible consequences, including train derailment, head on collision with another train as well as collision with infrastructure. For illustrational purposes, only train derailment due to SPAD is considered hereafter.

SPAD alone does not lead to train derailment; additional factors must be present. A train can derail when (1) the signal is followed by a turnout point that is not set or when (2) the signal is followed by a curve and train speed is high. The basic events describing these additional factors (causes of train derailment given SPAD) are summarized in Table 2 and are included in the FT in Figure 3, modeling train derailment due to SPAD.

Table 2. Causes (basic events) of train derailment given SPAD.

Event	Description
High train speed	Speed of the train passing a signal is greater than 60 miles/hour
Curve in Track alignment	Railway track is not straight after passing a signal. It has curves.
Turnout/point not set	There is a turnout/point in the following section with prevented route

3.2 *Advanced aspects of FT modeling applied to train derailment due to SPAD*

The FT for the modeling of train derailment due to SPAD shown in Figure 3 fails to address several types of dependences among basic events. These dependences, which should be included in an advanced FT model as described in (Xing & Amari, 2008), are summarized below.

3.2.1 *Advanced aspect 1: Common cause failures*

The FT in Figure 3 assumes that the basic events are statistically independent. This does not hold for the basic events „Slip'' and „High train speed''; they are dependent since a high train speed is required for the train to slip. Therefore, high train speed is a shared root cause, also called common cause failure (CCF). When CCFs are ignored, the safety risks will be (1) overestimated if the FT is dominated by series (OR gate) components and (2) underestimated if the FT has many components in parallel (AND gate).

3.2.2 *Advanced aspect 2: Disjoint events*

The basic events "Slip" and "Driver errors in brake application" in the FT of Figure 3 cannot occur jointly, because slip requires that brakes are applied. These events are therefore mutually exclusive (disjoint) events and are not statistically independent.

3.2.3 *Advanced aspect 3: Multistate components*

The events of FT in Figure 3 correspond to random variables with binary states (fail-success). The FT cannot directly model multistate components or mutually exclusive system states. However, such multistate modeling is often required for representing different conditions of a component or system. As an example, for the train derailment due to SPAD, two different system states (situations) must be distinguished:

Situation 1: SPAD occurs due to slip. This implies that brakes are applied when passing the red signal. In this situation, derailment will only occur if the distance between the signal and the turnout point (the overlap length) is sufficiently small. Otherwise the train will come to a stop before the turnout point.

Derailment due to a curvature in the track is negligible since the train speed is already limited due to the application of the brakes.

Situation 2: SPAD occurs because brakes are not applied, corresponding to occurrence of the intermediate event ,,Driver errors and protection failures''. In this situation, derailment can occur independently of the overlap length due to (1) a turnout in the following section with prevented route and (2) a curvature in the following section.

3.3 *Advanced fault tree for train derailment caused by SPAD*

The above discussed statistical dependences among the events in a FT can be included using advanced FT modeling techniques (Xing & Amari, 2008). However, in most cases these techniques lead to an exponential increase in the size of the FT structure with increaing dependences. As an example, Figure 4 shows the FT for train derailment due to SPAD where the above discussed dependences are included. Note that this FT contains several repeat bars, i.e. parts of the fault tree are repeated, and the advanced FT is thus significantly larger than the standard FT in Figure 3.

Because of the repetition of intermediate events in the advanced FT of Figure 4, a large number of basic events appear multiple times in the FT structure. These repeated basic events can be interpreted as common cause failures. In total, there are six CCFs ($E_1, E_3, E_4, E_5, E_7, E_8$). To account for these CCFs in the computation of the probability of system failure (here: the probability of train derailment due to SPAD), so called common cause events (CCE) are introduced. The CCEs are a set of mutually exclusive and collectively exhaustive events, defined as

$$\begin{aligned} CCE_1 &= \overline{E_1} \cap \overline{E_3} \cap \overline{E_4} \cap \overline{E_5} \cap \overline{E_7} \cap \overline{E_8} \\ CCE_2 &= E_1 \cap \overline{E_3} \cap \overline{E_4} \cap \overline{E_5} \cap \overline{E_7} \cap \overline{E_8} \\ &\vdots \\ CCE_{2^6} &= E_1 \cap E_3 \cap E_4 \cap E_5 \cap E_7 \cap E_8 \end{aligned} \quad (2)$$

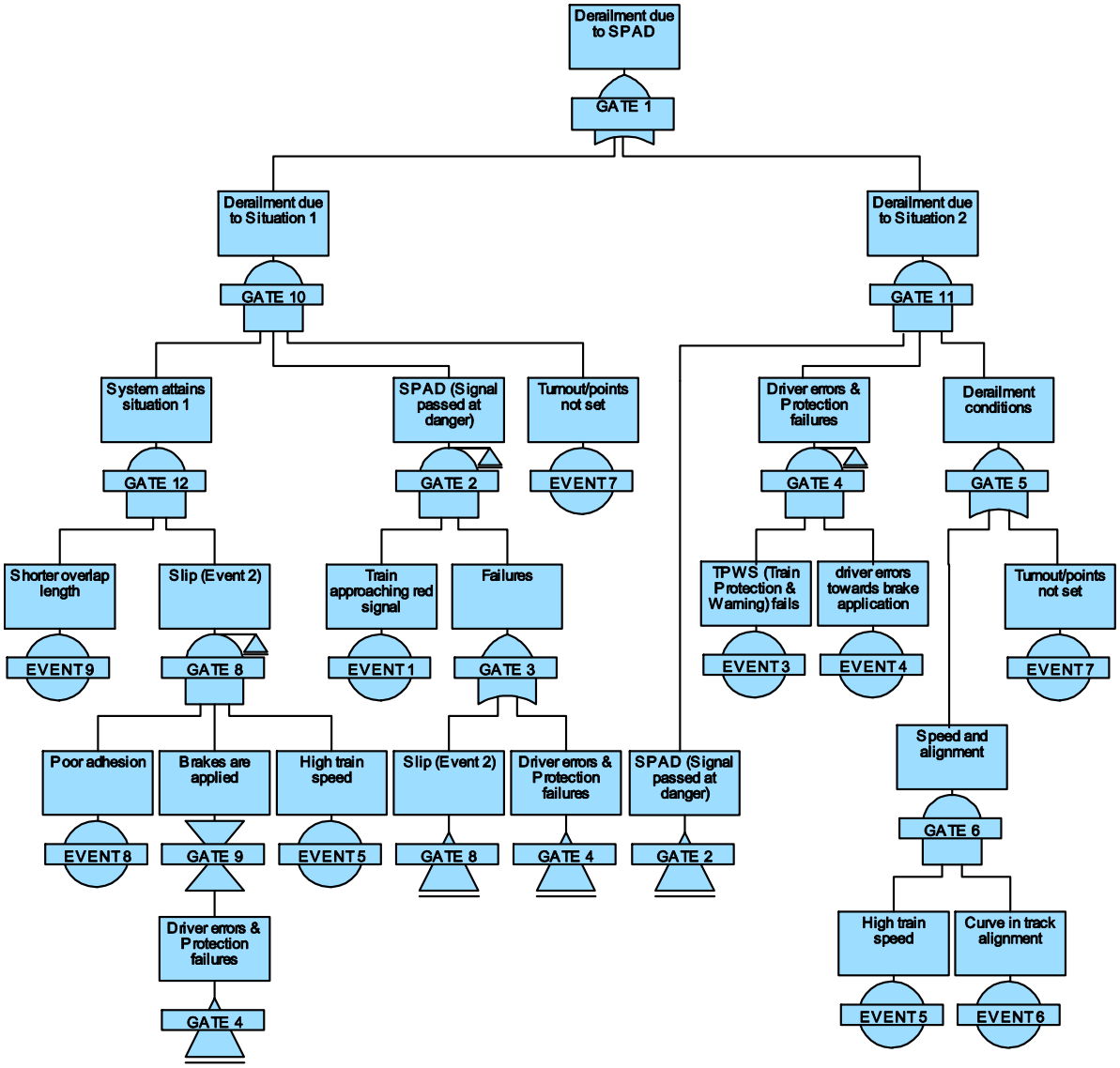

Figure 4. Advanced Fault Tree model for train derailment due to SPAD including dependences.

There are a total of 2^6 CCEs for the case of 6 CCFs. For each CCE, the conditional probability of the top event $\Pr(TE|CCE_i)$ is computed, which is achieved by setting the probabilities of the basic events corresponding to the CCFs to 0 or 1 respectively. The unconditional probability of the TE, $\Pr(TE)$ is then calculated by means of the total probability theorem as

$$\Pr(TE) = \sum_{i=1}^{2^6} \Pr(TE|CCE_i) \cdot \Pr(CCE_i) \qquad (3)$$

The dependence among the disjoint events "Slip" and "Driver errors in brake application" is modeled by introducing a NOT gate (gate 9 in Figure 4), which ensures that the slip event only occurs if the brake is applied. The multistate property of the system (situations) is modeled by copying parts of the FT and then combining these copies with OR gates.

4 BAYESIAN NETWORKS

Bayesian Networks (BNs) are graphical probabilistic models of a set of dependent random variables. The nodes in network are random variables and the directed links between them represent their dependence structure. The resulting graph must be acyclic. If X_1 has a link pointing to X_2, then X_1 is called a *parent* of X_2 and X_2 is called a *child* of X_1. Each random variable X_i is defined conditional on its parents $pa(X_i)$. Here only BNs with discrete random variables are considered and each random variable X_i is thus described by a table of conditional probability mass functions (PMF) $p[x_i|pa(x_i)]$.

Consider a Bayesian network with random variables $\mathbf{X} = [X_1, \ldots, X_n]$. The joint probability mass function of $\mathbf{X}$ is the product of the conditional PMFs:

$$p(\mathbf{x}) = p(x_1, x_2, \ldots, x_n) = \prod_{i=1}^{n} p[x_i|pa(x_i)] \qquad (4)$$

For a general introduction to BN and the modeling of statistical dependence in BNs, the reader is referred to (Jensen, et al., 2007).

4.1 *Bayesian Networks representation of advance aspects of Fault Tree*

Any FT can be translated into a BN, as shown in (Bobbio, et al., 2001). The FT of Figure 4 is mapped into an equivalent BN, shown in Figure 5. To this end, all basic and intermediate events are represented by corresponding random variables (nodes); the dependences among these are included through corresponding directed links and associated conditional probabilities. As an example, Table 3 shows the modeling of an AND gate.

Table 3. AND gate for TPWS & driver errors (T&DE).

TPWS failure	Yes		No	
Driver errors	Yes	No	Yes	No
Pr(T&DE = Yes)	1	0	0	0
Pr(T&DE = No)	0	1	1	1

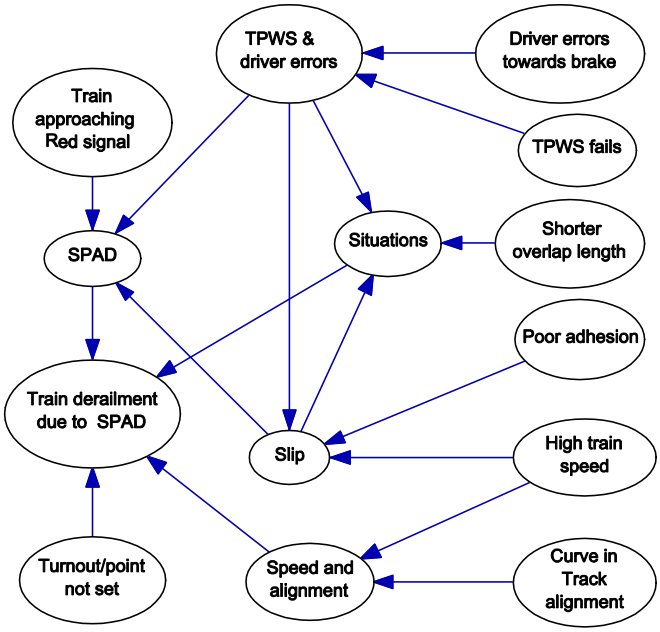

Figure 5. Bayesian Network for train derailment due to SPAD.

In the following it is outlined how the advanced FT modeling aspects introduced in Section 3.2 can be efficiently represented in the BN.

4.1.1 *Advanced aspect 1: Common cause failures*

In the advanced FT of Figure 4 a large number of CCFs is introduced to model dependences. In the BN, the dependencies can be directly introduced by adding corresponding links. The CCF „high train speed'' is accounted for by introducing the link from „High train speed'' to „Slip'' and "Speed and alignment".

4.1.2 *Advanced aspect 2: Disjoint events*

Modeling of disjoint events is straightforward in the BN. A link is added between the corresponding two random variables and the conditional probability table of the child node is defined accordingly. An example is given in Table 4. The event "TPWS failure and driver errors" and the event "slip" are mutually exclusive, as discussed previously. A link is added from the node "TPWS failure and driver errors" and the probability of slip given "TPWS failure and driver errors" is set to zero (compare column 2 and column 6 in the conditional probability table of Table 4).

Table 4. Conditional probability table for node "Slip"

High train speed	High				Controlled			
Poor adhesion	Yes		No		Yes		No	
TPWS & driver errors	Yes	No	Yes	No	Yes	No	Yes	No
Slip	0	1	0	0	0	0	0	0
No slip	1	0	1	1	1	1	1	1

4.1.3 *Advanced aspect 3: Multistate components*

The system states (situations) presented in section 3.2.3 can be represented directly by introducing a corresponding node in the BN. This node has three states, corresponding to the two situations described previously as well as a third state corresponding to no-derailment conditions. The corresponding conditional probability table is shown in Table 5.

Table 5. Conditional probability table for node „Situations''.

Overlap length	Shorter				Greater			
TPWS fails & driver errors	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
No-derailment conditions	-	0	0	1	-	0	1	1

The random variable „Train derailment due to SPAD'', corresponding to the TE of the FT, is modeled by introducing the links from four random variables as shown in Figure 5. The train will derail if SPAD and either situation 1 or situation 2 occur together in the presence of derailment conditions. The dependences among theses random variables are shown in Table 6.

5 RESULTS

The random variables in the BN are assigned the same probabilities as the basic events in the FT. Hence, the two models result in the same probability of train derailment due to SPAD. The computation of the diagnostic importance factor DIF of the various basic events, as defined in Eq. (1), is straightforward with the BN model. The posterior probability of every random variable given the TE is directly obtained when applying standard BN inference algorithms (Jensen & Nielsen, 2007). With the FT model, the DIF can be obtained from application of Bayes' rule. Table 7 presents the DIF values computed with the two methods.

Table 7. Diagnostic importance factor of the basic events, as computed with FT and BN.

Event	DIF
Train approaching red signal	100%
Turnout/point not set	99.7%
TPWS & driver errors	82.4%
High train speed	18.7%
Shorter overlap length	18.0%
Poor adhesion	20.0%
Curve in track alignment	4.3%

6 DISCUSSION

Both BN and FT are capable to handle the various dependences arising in the safety analysis of railway systems, including common cause failures, multistate components and disjoint events. Both the network structure of the FT and the conditional probability tables of the BN grow exponentially with increasing dependence among the basic events.

The FT has the advantage that it graphically shows the logical relations between the basic events and the top event. It is a well-known methodology that can be applied relatively easily by non-experts. However, as illustrated by the example provided in this paper, the resulting FT becomes non-intuitive and difficult to handle when dependences are present.

The application of BN to railway safety is not common practice in the industry. It requires some additional expertise and understanding in comparison with FT analysis. BN has the disadvantage that the logic relations between components of the system (e.g. AND, OR) cannot be directly observed from the graphical representation. However, the BN has strong advantages when modeling dependences in

Table 6. Conditional probability table for node "Train derailment due to SPAD".

SPAD	Yes												No											
Situations	Situation 1				Situation 2				No-derailment conditions				Situation 1				Situation 2				No-derailment conditions			
Turnout/point	Not set		Set		Not set		Set		Not set		Set		Not set		Set		Not set		Set		Not set		Set	
Speed & alignment	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No
Yes	1	1	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
No	0	0	1	1	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

the system. Because it was developed to efficiently represent complex probabilistic dependence among random variables, the resulting graphical model is concise even for systems with complex dependences. Because it is a general-purpose modeling tool, the BN has the advantage of flexibility. Any BN model can easily be extended. As an example, consider the case where experts are uncertain or disagree on the probability of basic events. This can be directly included by adding a node “Expert” in the BN and defining the probabilities of the basic events conditional on the state of this node.

7 CONCLUSIONS

The use of Fault Tree (FT) and Bayesian Networks (BN) for modeling safety risks in railway systems was illustrated for the case of train derailment caused by SPAD events. Various types of dependences among the basic events leading to the failure are discussed and implemented in the FT and BN models. It is observed that the BN is more suitable to handle these dependences.

8 ACKNOWLEDGEMENTS

Financial support of the Higher Education Commission (HEC) Pakistan, Pakistan Railways and the German Academic Exchange Service (DAAD) is acknowledged.

9 BIBLIOGRAPHY

Assaf, T., & Dugan, J. (2004). Diagnostic expert systems from dynamic fault trees. *Reliability and Maintainability, Annual Symposium - RAMS , vol., no., 26-29 Jan.* (pp. 444- 450,). doi: 10.1109/RAMS. 2004.1285489.

Aven, T. (2008). *Risk analysis.* West Sussex: John Wiley & Sons.

Bertsche, B. (2008). Fault Tree Analysis, FTA. In B. Bertsche, *Reliability in Automotive and Mechanical Engineering* (pp. 160-190). Berlin Heidelberg: Springer.

Bobbio, A., Portinale, L., Minichino, M., & Ciancamerla, E. (2001). Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. *Reliability Engineering and Systen Safety 71* , 249-260.

Borgonovo, E., Apostolakis, G. E., Tarantola, S., & Saltelli, A. (2003). Comparison of global sensitivity analysis techniques and importance measures in PSA. *Reliability Engineering & System Safety,79(2)* , 175-185.

Chen, S., Ho, T., & Mao, B. (2007). Reliability evaluations of railway power supplies by fault-tree analysis. *Electric Power Applications,, IET , vol.1, no (2),* (pp. 161-172). doi: 10.1049/iet-epa:20060244.

Dhillon, B. (2007). *Human Reliability and Error in Transportation Systems.* London: Springer.

Duffey, R. B., & Saull, J. W. (2003). *Learning from Errors and Accidents: Safety and Risk in Today's Technology* . Boston: Butterworth-Heinemann.

Esveld, C. (2001). *MODERN RAILWAY TRACK.* Zaltbommel: MRT-Productions.

Evans, A. (2011). Fatal Train Accidents On Europe`s Railways: 1980-2009. *Accident Analysis and Prevention; 43(1) , 43* (1(391-401)), 391-401.

Heilmann, R., Rothbauer, S., & Sutor, A. (2007). Component Fault Tree Analysis Resolves Complexity: Dependability Confirmation for a Railway Brake System. In *Computer Safety, Reliability, and Security: Lecture Notes in Computer Science* (Vols. 4680/2007, 100-105). DOI: 10.1007/978-3-540-75101-4_11: Springer.

Jensen, F. V., & Nielsen, T. D. (2007). *Bayesian Networks and Decision Graphs.* Berlin: Springer.

Khakzad, N., Khan, F., & Amyotte, P. (2011). Safety Analysis in Process Facilities: Comparison of Fault Tree and Bayesian Network Approaches. *Reliability Engineering and System Safety* , doi:10.1016/j.ress.2011.03.012.

Lampis, M., & Andrews, J. D. (2009). Bayesian Belief Networks for System Fault Diagnostics. *Quality and Reliability Engineering International* , 409-426.

Limnios, N. (2007). *Fault Trees.* London: ISTE Ltd.

Marsh, W., & Bearfield, G. (2007). Representing Parametrized Fault Trees Using Bayesian Networks. *SAFECOMP* (pp. 120-1333). Heidelberg: Springer.

NASA. (2002). *Fult Tree Handbook with Aerospace Applications.* Washington, DC: NASA Office of Safety and Mission Assurance.

Oukhellou, L., Côme, E., Bouillaut, L., & Aknin, P. (2008). Combined use of sensor data and structural knowledge processed by Bayesian network: Application to a railway diagnosis aid scheme. *Transportation Research Part C: Emerging Technologies,Volume 16, Issue 6* , 755-767 .

Stewart, M. G., & Melchers, R. E. (1997). *Probabilistic Risk Assessment of Engineering Systems.* London: Champan & Hall.

Straub, D., & Kiureghian, A. D. (2010). Bayesian Networks Enhanced with Structural Reliability Methods. Part A: Theory. *Journal of Engineering Mechanics*, Trans. ASCE, **136**(10), pp. 1248-1258.

Whittingham, R. (2004). *The Blame Machine:Why Human Error Causes Accidents.* Oxford: Elsevier.

Xing, L., & Amari, S. V. (2008). Fault Tree Analysis. In K. B. Misra, *Handbook of Performability Engineering* (pp. 595-620). London: Springer.