Application of Dynamic Bayesian network to reliability and availability evaluation of CTCS-3 onboard system

Highlights:

1. Using DBN-based approach to evaluate the reliability and availability, taking account of dynamic failure behavior, recovery mechanism, and temporal effect.
2. Combining some actual situation and analyzing the hierarchical architecture and field data of CTCS-3 onboard system.
3. Comparing the reliability and availability of three kinds of onboard system and analyzing the degraded state.

Findings:

1.The CDD, TMR and HDD onboard system possess high reliability and availability. Besides, the low occurrence probabilities of degraded state are almost the same.
2.The VDX, RLU, C3CPU, C2CPU, and Power should be given more attention in physical level.
3.The effects of failure rate on the onboard systems follow the order: WP > TD > KN > PB> LP, and KN> WP> TD > PB> LP for CDD and HDD system, respectively. However, the order is KN>TD>WP > PB> LP for TMR system.
4.The recovery mechanism should be paid more attention to improve the reliability and availability of CTCS-3 onboard system.
5.The results of availability are validated by the field data from one railway bureau.

Application of Dynamic Bayesian network to reliability and availability evaluation of CTCS-3 onboard system

Abstract

This paper presents a systemic approach to evaluate the reliability and availability of Chinese Train Control System Level 3 (CTCS-3) onboard system based on dynamic Bayesian network (DBN), aiming to solve the problems such as dynamic failure behavior, recovery mechanism, and temporal effect. Taking account of the actual operational situation, the hierarchical architecture and field data of the CTCS-3 onboard system is analyzed. Classified by the redundancy strategy of vital computer (VC), three kinds of train control systems corresponding to the triple modular redundancy VC (TMR), hot standby double dual VC (HDD), and cold standby double dual VC (CDD) are presented. By mapping the dynamic fault tree into DBN, the structure and parameter modeling are conducted in a case study. Adopting the forward inference, the results show that the reliability and availability of CDD onboard system are higher than HDD, while TMR is between them. And, the low occurrence probabilities of degraded state are almost the same. Through the backward analysis, the difference between posterior and prior probability shows the VDX, RLU, C3CPU, C2CPU, and Power should be paid more attention. The results of sensitivity analysis demonstrate that the effects of failure rate on the onboard systems follow the order: WP > TD > KN > PB> LP, and KN> WP> TD > PB> LP for CDD and HDD system, respectively. However, the order is KN>TD>WP > PB> LP for TMR system. The recovery mechanism should be paid more attention to improve the reliability and availability of CTCS-3 onboard system. The validation of the proposed approach is demonstrated by the field data from one railway bureau.

1.Introduction

With the rapid development of railway, Chinese train control system (CTCS) has been applied to all conventional and high-speed lines. CTCS level 3 (CTCS-3) is the highest application level in high-speed railway networks, featuring high complexity, dynamic, and interdependencies. CTCS-3 onboard system is the safety-critical system to avoid exceeding the limited speed or overrunning a signal. In case of any failure occurring in a CTCS-3 onboard system, it may result in big accidents, damaging passengers or assets. Therefore, the reliability and availability evaluation of CTCS-3 onboard system plays an extremely important role in guaranteeing safety and efficiency of infrastructure and trains.

In order to achieve high reliability and availability, redundancy technique is adopted in CTCS-3 onboard system. On the one hand, hot standby, cold standby, and triple modular redundancy (TMR) strategy are utilized to improve the reliability and availability. In the actual situation, there are mainly three types of train control onboard system classified by the redundancy strategy of vital computer (VC), corresponding to the TMR VC (TMR), hot standby double dual VC (HDD), and cold standby double dual VC (CDD) [1,2,3]. On the other hand, redundancy technique brings the dynamic

failure behaviors and recovery mechanism problems to the system. Thus, those problems must be considered in the systematic reliability and availability modeling.

Models and approaches involving the reliability and availability analysis of train control system were studied over the past decade. Flammini et al. combined the fault tree and Bayesian Network (BN) to evaluate the reliability of European train control system (ETCS) [1]. Di et al. utilized the Reliability Block Diagram (RBD) and Markov model to evaluate the reliability, availability, and maintainability of CTCS-3 onboard system [2]. Su and Che modeled CTCS-3 onboard system by mapping fault tree to BN and analyzed the multi-state situation [3]. Qiu et al. proposed a simulation approach to evaluate the availability of ETCS level 2 system in the presence of state uncertainty. This result reflects some parameters in the proposed model need more realistic values [4]. Bernardi et al. described a model-driven approach for the development of formal maintenance and reliability models for the availability evaluation of train control system [5]. However, the dynamic failure behaviors and recovery mechanism problems have been ignored in aforementioned papers. Moreover, to analysis the reliability and availability of CTCS-3 onboard system, some actual situations should be taken into account. For example, the onboard system cannot be repaired online in working time because it will largely influence the safety and efficiency of railway network. The onboard system can be repaired in the inspection and repair station. The transition between CTCS-3 and CTCS-2 is possible. Therefore, CTCS-2 is considered as the backup of CTCS-3 in presence of wireless communication failure.

Recently, BN has been proposed to model the complexity of industrial systems and is widely used in dependability, risk analysis and maintenance applications [6]. For instance, Boudali proposed a discrete-time BN reliability formalism for system reliability prediction and diagnosis [7]. Neil and Marquez utilized a hybrid BN framework to model the availability of renewable systems [8]. The result shows corrective repair time, logistics delay times and scheduled maintenance time distributions are modeled to derive system availability. However, the static BN represents a joint probability distribution at a fixed time slice. Instead, Dynamic Bayesian Network (DBN) can model the dynamic behavior of random variables by extending the static BN at different time slices. Liang et al. applied DBN modeling to evaluate the reliability of warship [9]. Cai et al. proposed a DBN to analyze the reliability and availability of subsea blowout preventer, taking account of imperfect repair and preventive maintenance [10]. Cai et al. proposed a framework for the reliability evaluation of grid-connected PV systems in presence of intermittent faults [11]. Barua et al. illustrated a risk assessment methodology for dynamic systems based on DBN and showed the method in capturing dynamic operational changes in the process due to the sequential dependency of components [12]. Wu et al. provided guidelines for dynamic safety analysis of the tunnel-induced road surface damage over time [13].

Therefore, this paper attempts to evaluate the reliability and availability of HDD, TMR，

and CDD onboard train control system by converting the DFT model to DBN, taking account of the dynamic failure behaviors, recovery mechanism, and temporal effects. Forward, sensitivity and backward analysis are conducted by the proposed approach. The results are validated by the field data from one railway bureau. The remainder of the paper is organized as follows: section 2 introduces the structure and operating principle of CTCS-3 onboard system. In section 3, the DBNs for reliability and availability evaluation are presented through structure, parameter modeling and model validation. In section 4, a case study of reliability and availability evaluation of CTCS-3 onboard system will be conducted. Lastly, conclusions occur in section 5.

2.System description

2.1 introduction of CTCS-3 onboard system

CTCS-3 consists of onboard and trackside subsystems and is based on the wireless communication system (GSM-R) to realize the bidirectional continuously information transmission between the trackside and onboard subsystem [14,15]. Through GSM-R, the train speed and location can transmit to the Radio Block Center (RBC), but also, the movement authorities, generated by RBC, can transmit to the onboard system. In this paper, we mainly focus on the hardware failure of CTCS-3 onboard system. Since the transition between CTCS-3 and CTCS-2 is possible, a CTCS-3 system also includes the equipment of CTCS-2 system. Figure 1 shows the hierarchical architecture of the CTCS-3 onboard system. To guarantee the safety and efficiency of the railway network, the functional layer can be divided into five parts: wireless communication processing (WP), lineside data processing (LP), train and driver interface (TD), kernel information processing (KN), and power and bus function (PB). Each function is realized by the corresponding equipment shown in the physical layer. A brief introduction to the equipment of CTCS-3 is given.

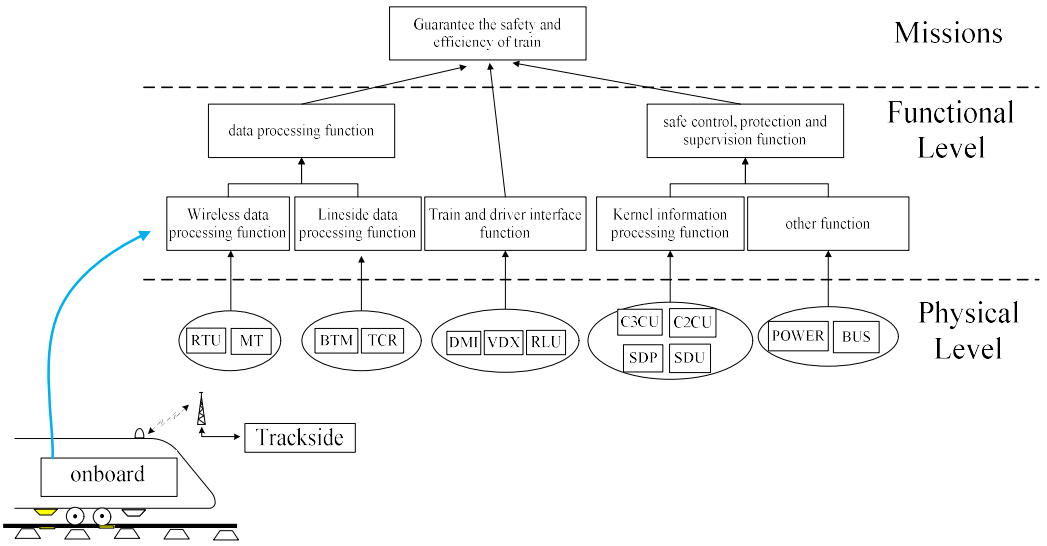


Figure 1. The architecture of the CTCS-3 onboard system

1. WP function is realized by Mobile Terminal (MT) and Radio Transmission Module (RTM). RTM is used for processing the messages, received or transmitted by MT.
2. LP function is conducted by Balise Transmission Module (BTM) and Track Circuit Reader (TCR). BTM is designed for processing the telegrams, received by BTM antenna. TCR receives the messages from TCR antenna and transmits the messages to C2-VC.
3. TD function is conducted by Driver-machine interface (DMI) and Train Interface Unit (TIU). TIU consists of Vital Digital input/output unit (VDX) and Relay Unit (RLU).
4. KN function accomplishes safe control, protection, and supervision of the train. CTCS-3 Vital Computer (C3-VC) and CTCS-2 Vital Computer (C2-VC) are the core computing system for preventing the train from overspeed or overrunning in CTCS-3 and CTCS-2, respectively. Speed and Distance Processing Unit(SDP) measures the speed and distance.
5. PB function provides the power and communication bus between equipment.

To proceed the reliability and availability evaluation of CTCS-3 onboard system, three assumptions should be made:
1. the basic events are mutually independent.
2. the failures of all components in the system follow the exponential distribution, meaning that basic event has a constant failure rate λ;
3. the CTCS-3 onboard system is considered "as good as new" after repair reaction.

2.2 problems statement
2.2.1 The actual working processing

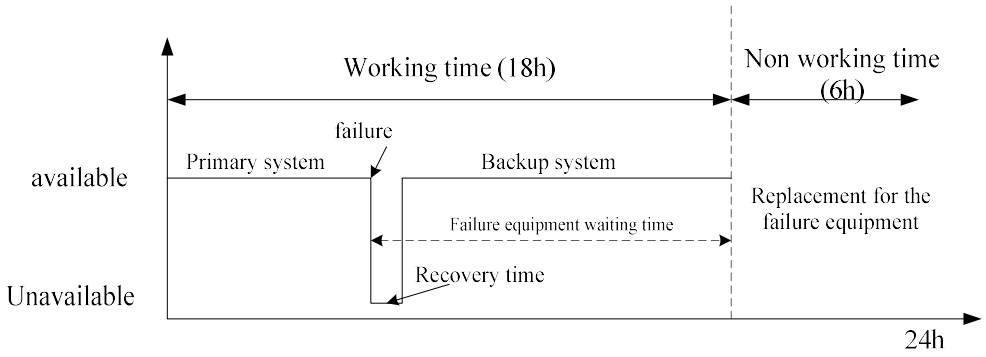


Figure 2. The working timetable of the CTCS-3 onboard system
Before evaluating the reliability and availability, the actual working processing of CTCS-3 onboard system should be explained first. Any fault in the five function parts can result in a failure of CTCS-3 onboard system. Due to the fail-safe principle in railway signaling system, the train usually stops and then the driver restarts the onboard system. The working timetable for onboard system in one day is shown in Figure 2. The average working time for a high-speed train is 18 hours in one day. For the rest 6 hours, the overhaul is required in the high-speed train inspection and repair station. The available state means the CTCS-3 onboard system is fully operative in the working 18

hours. However, the unavailable state represents the recovery time when the primary system suffers a failure. Particularly, the onboard system cannot be repaired online, that is to say, the onboard system only renews from the redundancy mechanism during the working 18 hours. Meanwhile, the onboard system can be fully repaired in the inspection and repair station during the 6 hours.

2.2.2 The use of field data

Considering the actual situation, the field data has been collected, which can be used for the failure rate calculation of the components and the partial validation of the results obtained. Failure mode/effect/cause and recovery time are analyzed by the field data from one railway bureau between 2015.5 to 2016.11, shown in Table 1. The recovery time is influenced by some dynamic factors, such as the recovery mechanism and the operational condition.

Table 1 The partial specification of field data.

Failure time	Failure mode	Failure effect	Recovery time (minutes)	Failure cause
12/05/2015	Invalid BTM port	Stopped the train	10	BTM1 failure
09/05/2015	Wireless communication timeout	Degraded to CTCS-2	26	MT1 failure
07/05/2015	Error on driver interface	Stopped the train	10	DMI failure
02/05/2015	Error on train interface	Stopped the train	18	VDX2 failure

2.2.3 Dynamic problem

The dynamic problem of CTCS-3 onboard system mainly includes dynamic failure behaviors and recovery mechanism. Recovery mechanism explained that a single component failure in a redundant system entails a complete system failure. Meanwhile, recovery mechanism can influence the recovery time of the CTCS-3 onboard system. The dynamic failure behaviors problem refers to time sequence of redundancy strategy. According to HDD, TMR，and CDD onboard system, both active redundancy and standby redundancy (hot standby and cold standby) are utilized. For instance, the SDU, POWER, and DMI adopt the parallel structure, hot standby, and cold standby, respectively. Nevertheless, the C3CU and C2CU of TMR control system are the 2oo3 voting architecture. The DBN-based reliability and availability modeling can handle with those problems, which is described in next section.

3. DBN-based reliability and availability modeling

3.1 Introduction on BN and DBN

A Bayesian network consists of two parts, corresponding a directed acyclic graph (DAG) and a joint probability distribution. Precisely, a Bayesian network is a triplet $< (V, E), P >$, where (V, E) are the variables (nodes) and edges (arcs) of a DAG and P is the probability distribution for every V [16]. The DAG realizes the qualitative analysis of dependence V (structure modeling). Meanwhile, the Conditional Probabilistic Table (CPT) over V accomplishes the quantitative analysis (parameter modeling). For discrete

random variables $V = \{X_1, X_2, \cdots X_N\}$, the joint probability distribution can be given by:

$$P(V) = P(X_1, X_2, \cdots X_N) = \prod_{X_i \in V} P(X_i \left| \mathrm{Pa}(X_i)\right.) \qquad (1)$$

where N is the number of random variables in the graph, and $\mathrm{Pa}(X_i)$ is the parent of X_i.

DBNs can model the dynamic behavior of random variables by extending the static BN with the temporal dependencies at different time slices. Intra-slice arcs at the same time slice and temporal arcs in different time slices are two types of conditional dependencies between nodes. Generally, two-time slices temporal Bayesian networks (2TBN) are considered in modeling the temporal evolution, assuming that temporal arcs between the consecutive time *t-1* and *t* satisfy the first order Markov process. The 2TBN defines $P(X_t|X_{t-1})$ by means of a DAG as follows: [17]

$$P(X_i \left| X_{i-1}\right.) = \prod_{i=1}^{N} P(X_t^i \left| \mathrm{Pa}\,(X_t^i)\right.) \qquad (2)$$

Where X_t^i is the *i*th node in time slice *t*, and $\mathrm{Pa}(X_t^i)$ indicates the parent of X_t^i which can only stand in slices *t-1* and *t*.

Note that the nodes in the first time slice do not associate any parameters, while each node from the second time slice has an associated CPT.

Thereby, the joint distribution can be defined by "unrolling" the 2TBN with T time slices as follows:

$$P(X_{1:T}) = \prod_{t=1}^{T} \prod_{i=1}^{N} P(X_t^i \left| \mathrm{Pa}(X_t^i)\right.) \qquad (3)$$

3.2 DBN structure modeling

The structure modeling presents the mapping rules from DFT into DBN. Here, we briefly model the AND gate, OR gate, 2oo3 voting gate, and spare gate as they will be later used in the case study. For those static logic gates (the AND gate, OR gate and 2oo3 voting gate), mapping rules are described in the study [18]. As indicated in OR gate shown in Figure 3(b), the relationship between C1, C2, and S is linked by intra-slice arcs. Then, DBN extends the BN by incorporating temporal dependencies at different time slices. For instance, the node C1 (t) is extended to C1 ($t+\Delta t$) with a temporal arc. Similarly, the DBN of AND gate and 2oo3 voting gate is shown in Figure 3(a) and Figure 3(c), respectively.

Dynamic logic gates are designed to express the time sequence and failure behaviors of the systems. The priority AND (PAND) gate, the functional dependency (FDEP) gate and the spare gate are commonly used in DFT modeling. Based on the previous study [19, 20], the mapping rules of spare gate is described. Generally, a SP gate consists of two types of elements: the primary modules and one or multiple redundant modules. As an example, a simple situation is considered that the spare gate includes one primary P and one spare S. From Figure 3(d), it is observed that the DBN structure is similar to

Figure 3(a). Moreover, it demonstrates that component states S at $t+\Delta t$ time slice is dependent on the states P at t time slice. Assuming the primary P is active at the t time slice with failure rate λ, and one spare S is dominant with failure rate $\alpha\lambda$, where α is the dominant factor. Hot and cold standby can be modeled by setting α equal to 1 and 0, respectively. Whenever the P fails, a replacement is initiated and the S will be powered up to keep the system functional.

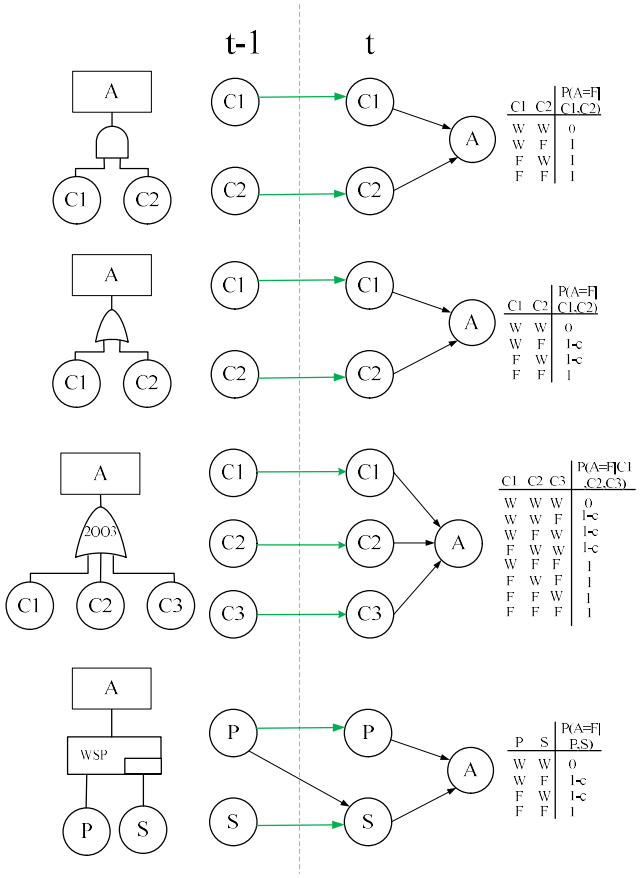


Figure 3 Mapping the AND gate (a), OR gate (b), 2oo3 voting gate (c) and spare gate (d) to DBNs

3.3 DBN parameter modeling

After DBN structure modeling, the quantitative part should be conducted. DBN parameter modeling involves two parts: the prior probabilities of root nodes and the CPT of intermediate nodes and leaf nodes. Each node involves two states denoted by Working (W) or Failed (F). The node C1 in Figure 3(b) is demonstrated as an example. Assuming the failure rate is λ, it can be obtained by:

$$P\left\{C1(t+\Delta t)=F \middle| C1(t)=W\right\}=1-e^{-\lambda t}$$

Considering the repair action, the availability of C1 can also be obtained. If the repair rate of C1 is μ, it can be get:

$$P\left\{C1(t+\Delta t)=W \middle| C1(t)=F\right\}=1-e^{-\mu t}$$

The CPT for C1 at t+Δt time slice given C1 at t time slice is provided in Table 2 and Table 3.

Table 2 CPT of C1 at t+Δt time slice without repair

C1 at t	C1 at t+Δt	
	W	F
W	$e^{-\lambda_i t}$	1- $e^{-\lambda_i t}$
F	0	1

Table 3 CPT of C1 at t+Δt time slice with repair

C1 at t	C1 at t+Δt	
	W	F
W	$e^{-\lambda t}$	1- $e^{-\lambda t}$
F	1- $e^{-\mu t}$	$e^{-\mu t}$

For spare gate shown in Figure 3(d), the CPT of node S without and with repair are given in Table 4 and Table 5, where α is the dominant factor.

Table 4 CPT of equipment without repair

P at t	S at t	S at t+Δt	
		W	F
W	W	$e^{-\alpha\lambda t}$	1- $e^{-\alpha\lambda t}$
W	F	0	1
F	W	$e^{-\lambda t}$	1- $e^{-\lambda t}$
F	F	0	1

Table 5 CPT of equipment with repair

P at t	S at t	S at t+Δt	
		W	F
W	W	$e^{-\alpha\lambda t}$	1- $e^{-\alpha\lambda t}$
W	F	1- $e^{-\mu t}$	$e^{-\mu t}$
F	W	$e^{-\lambda t}$	1- $e^{-\lambda t}$
F	F	1- $e^{-\mu t}$	$e^{-\mu t}$

An important parameter in a redundant system is the coverage factor. The coverage factor is defined as the ability of the system to automatically recover from the occurrence of a fault during normal system operation [21]. Due to the inaccurate recovery mechanism, the fact is rational that a single component failure in a redundant system entails a complete system failure. Therefore, it should be considered in both active and standby redundant system. The coverage factor *c* is modeled in the CPT shown in Figure 3(a), (b), (c), (d).

3.4 reliability and availability evaluation

Through the method above, the DBN of CTCS-3 onboard system can be obtained. The reliability and availability can be evaluated by the forward analysis of DBN and the comparisons for the three kinds of control system are conducted. Meanwhile, the

posterior probabilities of each node are generated by the backward analysis after an evidence is entered. A sensitivity analysis is carried out with the assumption that the prior probabilities of five categories are subject to an uncertainty of +10%. Moreover, the effects of coverage factor on reliability and availability are calculated.

3.5 DBN validation

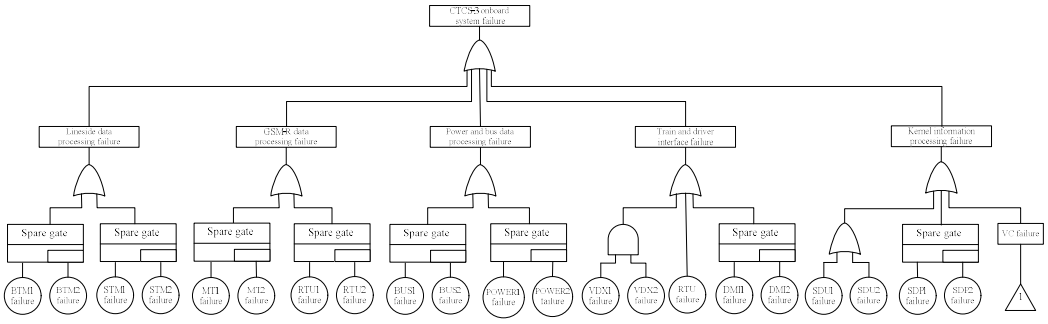
The validation of the proposed model is a significant procedure to prove that it is reasonable for the reliability and availability evaluation of the actual system. Verification should be performed by the model usability and the results obtained. In this paper, the validation is accomplished by two ways:
A partial validation of the model usability should satisfy three axioms proposed by Jones at al [22].
The results, such as the availability, are validated by analyzing the field data of one railway bureau. The field data is based on the corrective maintenance between 2015.5 to 2016.11.

4. case study

A case study on reliability and availability of CTCS-3 onboard system is conducted and the results for three types of control system are compared in this section.

4.1 The DFT of CTCS-3 onboard system

The construction of DFT is based on the system structure and the expert experience. The CTCS-3 onboard system failure is considered as the top event. There are five intermediate events, i.e. Lineside data processing failure, Wireless communication failure, Power and bus failure, Kernel information processing failure, and the Train and driver interface failure. The relationship between events is connected by AND gate, OR gate, 2oo3 voting gate, and Spare gate, shown in Figure 4. The spare gate is either cold or hot spare gate. Specifically, VDX1 and VDX2 are connected by a AND gate because they collect the output signaling mutually. In case of any fault in the VDX1 and VDX2, the train will execute emergency braking unconditionally.



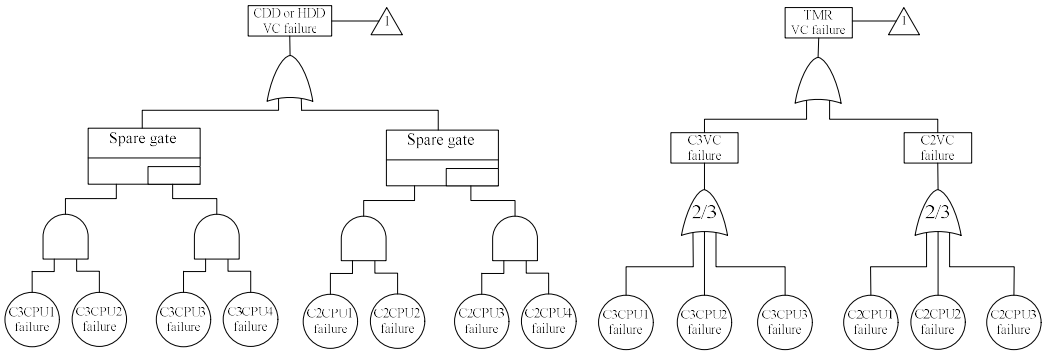


Figure 4. The DFT of CTCS-3 onboard system

Table 6 The failure rates, prior, and posterior probabilities of components

			CDD		HDD		TMR	
NO.	component	failure rate λ (/h)	Prior probabilities	Posterior probabilities	Prior probabilities	Posterior probabilities	Prior probabilities	Posterior probabilities
1	C3CPU1	7.45E-06	8.56E-02	1.54E-01	8.56E-02	1.61E-01	8.56E-02	1.82E-01
2	C3CPU2		7.71E-03	6.14E-02	8.56E-02	1.61E-01		
3	C2CPU1	6.00E-06	7.02E-02	1.21E-01	7.02E-02	1.25E-01	7.02E-02	1.39E-01
4	C2CPU2		5.12E-03	4.08E-02	7.02E-02	1.25E-01		
5	SDP1	5.00E-07	6.27E-03	8.63E-03	6.27E-03	8.09E-03	6.27E-03	8.30E-03
6	SDP2		2.93E-05	2.33E-04	6.27E-03	8.09E-03	6.27E-03	8.30E-03
7	SDU1	2.50E-07	3.14E-03	4.31E-03	3.14E-03	4.04E-03	3.14E-03	4.15E-03
8	SDU2		1.46E-05	1.17E-04	3.14E-03	4.04E-03	3.14E-03	4.15E-03
9	RTU1	1.80E-06	2.24E-02	2.24E-02	2.24E-02	2.24E-02	2.24E-02	2.24E-02
10	RTU2		2.51E-04	2.51E-04	2.24E-02	2.24E-02	2.51E-04	2.51E-04
11	MT1	6.00E-06	7.28E-02	7.28E-02	7.28E-02	7.28E-02	7.28E-02	7.28E-02
12	MT2		7.28E-02	7.28E-02	7.28E-02	7.28E-02	7.28E-02	7.28E-02
13	BTM1	2.07E-06	2.57E-02	3.66E-02	2.57E-02	3.49E-02	2.57E-02	3.60E-02
14	BTM2		3.31E-04	2.64E-03	2.57E-02	3.49E-02	3.31E-04	2.60E-03
15	TCR1	2.30E-06	2.86E-02	4.09E-02	2.86E-02	3.91E-02	2.86E-02	4.03E-02
16	TCR2		4.08E-04	3.25E-03	2.86E-02	3.91E-02	2.86E-02	4.03E-02
17	Power1	6.00E-06	7.28E-02	1.28E-01	7.28E-02	1.12E-01	7.28E-02	1.17E-01
18	Power2		7.28E-02	1.28E-01	7.28E-02	1.12E-01	7.28E-02	1.17E-01
19	Bus1	4.00E-06	4.92E-02	7.32E-02	4.92E-02	7.13E-02	4.92E-02	7.39E-02
20	Bus2		1.22E-03	9.68E-03	4.92E-02	7.13E-02	4.92E-02	7.39E-02
21	DMI1	5.00E-06	6.11E-02	9.29E-02	6.11E-02	9.14E-02	6.11E-02	9.49E-02
22	DMI2		1.88E-03	1.50E-02	1.88E-03	1.36E-02	1.88E-03	1.66E-02
23	VDX1	2.00E-06	2.49E-02	1.98E-01	2.49E-02	1.49E-01	2.49E-02	1.64E-01
24	VDX2		2.49E-02	1.98E-01	2.49E-02	1.49E-01	2.49E-02	1.64E-01
25	RLU	1.50E-06	1.87E-02	1.49E-01	1.87E-02	1.12E-01	1.87E-02	1.23E-01

4.2 Mapping the DFT to DBN

In this paper, the DBNs for CDD, TMR and HDD control system are analyzed using GeNIe 2.1 academic software (http://genie.sis.pitt.edu/) developed at the University of Pittsburgh [23]. To establish the DBNs, the mapping rules introduced in section 3.2 is utilized. The DFTs of "CTCS-3 system failure" are translated into the corresponding DBNs with two-time slices as shown in Figure 5. For instance, the top event is translated into the corresponding child node (CTCS-3 onboard), whereas the basic events are translated into the corresponding parent nodes in DBNs. Considering the actual situation that the degradation from CTCS-3 to CTCS-2 level is possible, the child node (CTCS-3 onboard) has three states corresponding to Working (W), Degraded (D) and Failed (F), whereas the other nodes only have two states (W, F).

In the case study, the Δt is set to be one week, i.e. 126 hours. Since the failures of components follow the exponential distribution, the initial states are in the perfect functioning in 0th week, and the failure probabilities of those nodes are assigned to 0. According to the DBN parameter modeling described in section 3.3, the CPT of the nodes in other time slices can be calculated, which is shown in from Table 2 to Table5. The failure rates of the components are based on both field data and expert experience, shown in Table 6. It should be mentioned that, the degraded state of the node (CTCS-3 onboard) occurs if and only if the wireless communication failure happens, and the CPT of this child node is shown in Table 7.

Table 7. The CPT of the node (CTCS-3 onboard).

LP		WP		PB		KN		TD		P(system | LP, WP, PB, KN, TD)		
W	F	W	F	W	F	W	F	W	F	W	D	F
1	0	1	0	1	0	1	0	1	0	1	0	0
1	0	0	1	1	0	1	0	1	0	0	1	0
0	1	1	0	1	0	1	0	1	0	0	0	1
……												
0	1	0	1	0	1	0	1	0	1	0	0	1

Since the component is considered "as good as new" after repair action, the availability A_o is equal to MUT/(MUT+MDT), where the MUT is the average working time, and the MDT is the average down time. Considering the operational situation of CTCS-3 onboard system shown in Figure 2, the MDT mainly depends on the mean waiting time of the component in 18 hours after it failed. Therefore, the mean waiting time for both primary and spare component in hot spare and 2oo3 redundancy system is 9 hours, whereas the values are 9 and 4.5 hours in cold spare redundancy system.

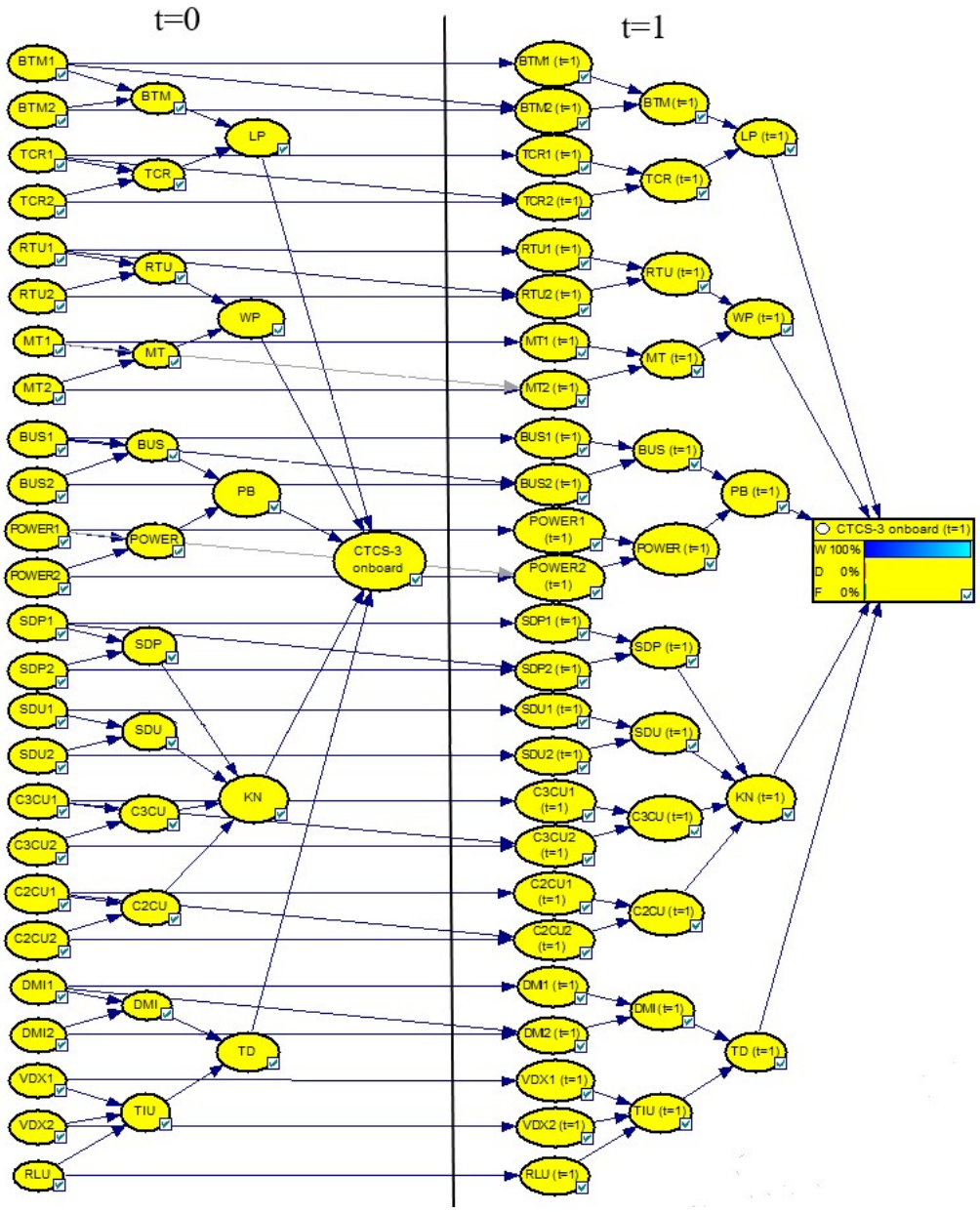


Figure 5. The DBN of CTCS-3 onboard system (HDD or CDD)

4.3 results and discussion

4.3.1 Reliability and availability evaluation.

The reliability and availability of CTCS-3 onboard system within 100 weeks are evaluated by the forward analysis of DBN as shown in Figure 6. The coverage factors for the redundancy system are assigned to 0.95. As indicated in Figure 6(a), the reliabilities of the three kinds of control systems decrease with the increasing of weeks. The reliability of CDD system is higher than HDD system, whereas the TMR system is

between them. Moreover, the reliabilities of CDD, TMR, and HDD system at 100th week are 0.81, 0.785, and 0.771, respectively. As indicated in Figure 6(b), the occurrence probabilities of degraded state for the CDD, TMR, and HDD system increase to 0.065, 0.064, and 0.063 at 100th week, respectively. Obviously, the degraded states are almost the same for the three systems at different time slice.

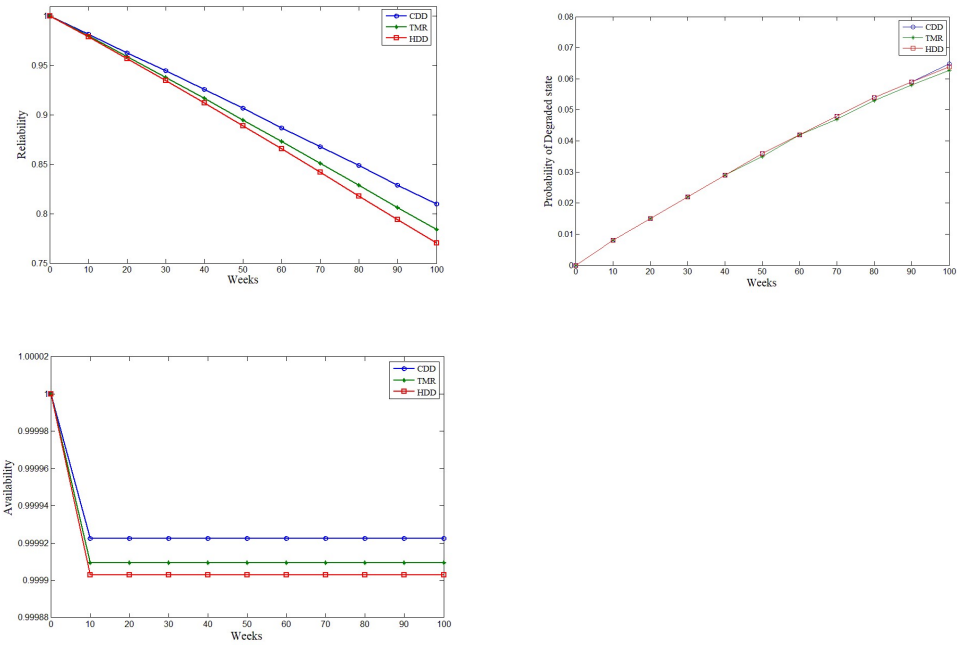


Figure 6. The reliability and availability evaluation of CTCS-3 onboard system

As shown in Figure 6(c), the Availability of CDD, TMR, and HDD system is 0.999923, 0.999909, and 0.999902, respectively. All the three systems reached their steady-state availability in 10 weeks and are much higher than the reliability. Obviously, the availabilities accord with design specification that the availability should be greater than 0.9999.

By setting the failure probability of CTCS-3 onboard node to 1, the posterior probabilities of the component are conducted by backward analysis. The prior probability and posterior probability for three control system at 100th week are listed in the 4th-9th columns of Table 6. The difference between posterior probability and prior probability are shown in Figure 7. It can be seen that the values of VDX, RLU, C3CPU, C2CPU and Power are much higher than other components, meaning that the five components should be given more attention to improving the reliability of CTCS-3 onboard system. Besides, the wireless communication failure only leads the system to degraded state so that the values of MT and RTU are 0.

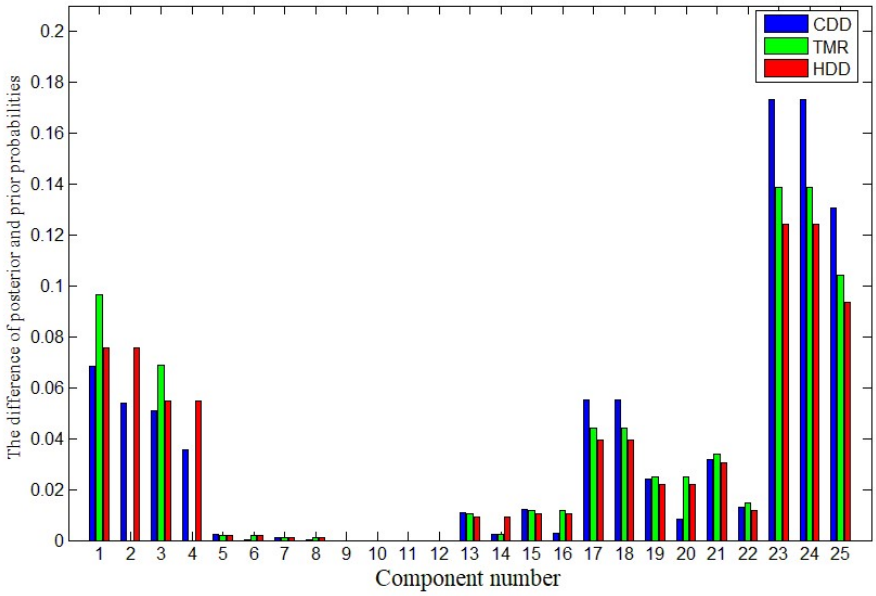
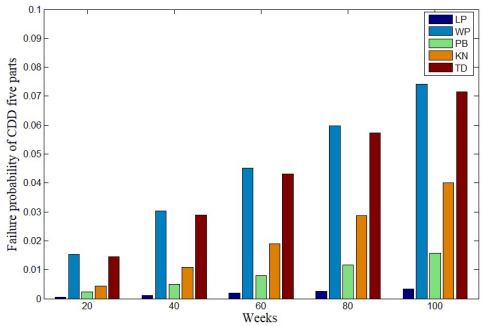


Figure 7. The difference between posterior probability and prior probability

4.3.2 the failure probability for five parts in different time slices

As indicated in Figure 8, the failure probabilities of the three kinds of CTCS-3 onboard system increase with the increasing of weeks. Obviously, WP, KN, and TD have higher failure probabilities than LP and PB. Besides, LP has a negligible effect on system failure. Specifically, WP is mainly responsible for the degraded state of CTCS-3 onboard system, meaning that the higher probability of WP brings the less efficient of the system. It can be concluded that KN and TD are more critical than LP and PB as their failure probabilities are much higher. It should be noted that the failure probability of KN is higher than TD at 100th week for HDD system, whereas the failure probability is lower in CDD and TMR system.



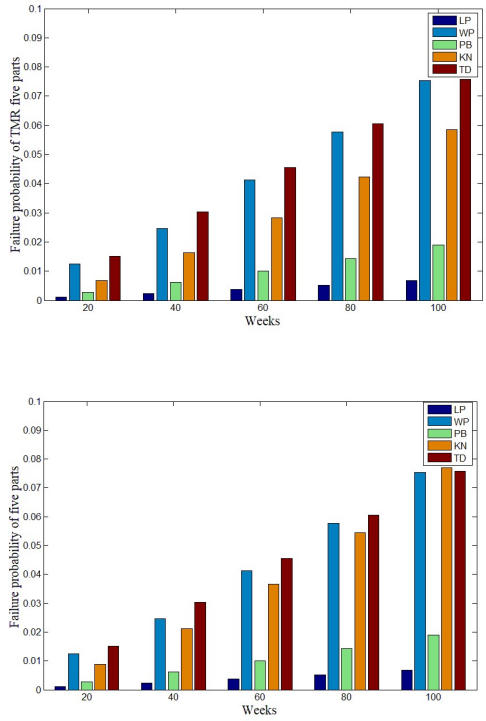


Figure 8. The failure probability for five parts in different time slices

4.3.3 Sensitivity analysis.

The variables of failure probabilities for each control system at 100th week are calculated with the assumption that the failure rates of each function module increase 10%. Effects of changes in each function part are shown in Figure 9. It can be concluded that the order of effects on the systems failure are: WP > TD > KN > PB> LP, and KN> WP> TD > PB> LP for CDD and HDD system, respectively. However, the order is KN>TD>WP > PB> LP for TMR system. Moreover, it shows that the KN has the large fluctuation for the three kinds of CTCS-3 onboard system, whereas others have little fluctuation.

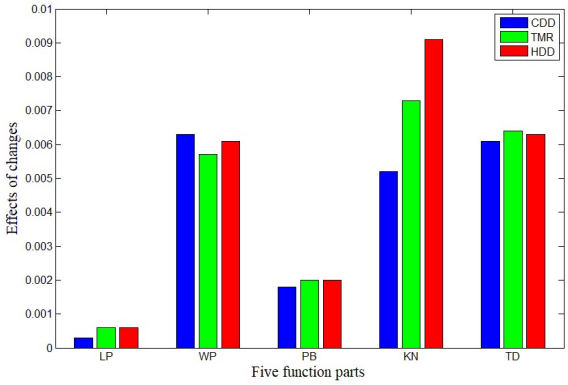


Figure 9 the effects of changes in each function module

4.3.4 Effects of coverage factor to reliability and availability

From the above analysis, the value of coverage factor is 0.95. To analyze the effects of coverage factor, the values are assigned to 0.9, 0.925, 0.95, 0.975, and 1 to calculate the reliability and availability of three kinds of CTCS-3 onboard system at 100th week, as shown in Figure 10. It can be seen that the reliability and availability increase with the increasing coverage factor, meaning that the recovery mechanism is significant for the three kinds of CTCS-3 onboard system. Furthermore, the effects on HDD system is more important than CDD system, whereas the TMR system is between them. The difference of reliability and availability shrinks with the increasing coverage factor. Specifically, the availabilities of the three kinds of control systems reach the same value, i.e. 0.999949. To achieve high reliability and availability, the recovery mechanism should be paid more attention.

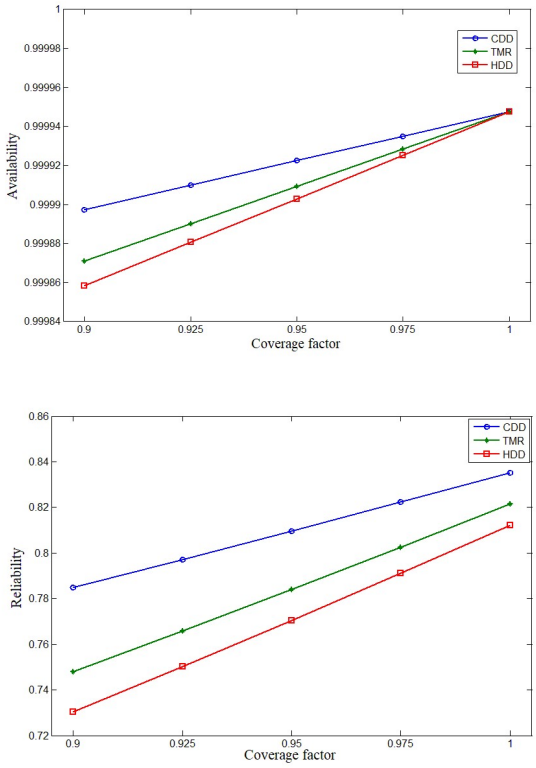


Figure 10. The effects of coverage factor to reliability and availability

4.4 Validation of the model

4.4.1 The model usability validation

To validate the model usability, the DBNs of HDD system is taken as an example. When the parent node “BTM1” is set to 50% from 0%, the reliability of system decreases to 0.743 from 0.771. When both the change plus the parent node “BTM2” is set to 50%, the reliability decreases to 0.55. With the addition of parent node “TCR1”

and “TCR2” are set to 50%, the reliability decreases to 0.392. Besides, the sensitivity analysis in section 4.3.3 is also a validation of the model usability. Therefore, the exercise of increasing the influencing node give a partial validation to the proposed model.

4.4.2 The results validation

The availabilities obtained can be validated by the field data from one railway bureau. Through the description of system, the corrective maintenance data has been analyzed between 2015.5 and 2016.11. The CTCS-3 onboard adopted the CDD system. The total number of EMU is 63. And the total recovery time is 2683 minutes. Therefore, the availability of the system is 0.999928, which gives a partial validation to the availability the model calculated.

5. Conclusions

The reliability and availability of train control system are extremely significant for the performance of railway network. According to the CTCS-3 onboard system architecture and field data analysis, a DFT is constructed. Then, a DBN-based approach to evaluate the reliability and availability of CTCS-3 onboard system is proposed to handle the dynamic failure behaviors and recovery mechanism problems. The case study for three kinds of train control systems, corresponding to CDD, TMR, and HDD, is presented. The validation and feasibility of the proposed approach are demonstrated by the results. The main achievements can be summarized as follow:

(1) The DBN-based approach provides a powerful solution for the dynamic and complex CTCS-3 onboard system. The CDD, TMR and HDD onboard system possess high reliability and availability. Besides, the low occurrence probabilities of degraded state are almost the same.
(2) Through the backward analysis of DBN, the VDX, RLU, C3CPU, C2CPU, and Power should be given more attention in physical level. According to the failure probability for five parts in different time slices, the KN and TD are more critical than LP and PB in function level.
(3) Based on sensitivity analysis, the effects of failure rate on the onboard systems follow the order: WP > TD > KN > PB> LP, and KN> WP> TD > PB> LP for CDD and HDD system, respectively. However, the order is KN>TD>WP > PB> LP for TMR system.
(4) The recovery mechanism should be paid more attention to improve the reliability and availability of CTCS-3 onboard system. Moreover, the effect of recovery mechanism on HDD system is more important than CDD system, whereas the TMR system is between them.
(5) The model usability Validation is conducted by the sensitivity analysis. And, the results of availability are validated by the field data from one railway bureau.

Based on the DBN approach, future work would focus on the reliability and availability

evaluation of the whole CTCS-3 system in order to handle the interdependencies and dynamic problems between onboard and trackside system.

Reference

1. Flammini F, Marrone S, Mazzocca N, at al. Modeling system reliability aspects of ERTMS/ETCS by fault trees and Bayesian Network. In: Soares G and Zio (eds) Safety and Reliability for Managing Risk. London: Taylor & Francis Group, 2006, pp.2675-2683.
2. Di, L.Q. Yuan, X. Wang, Y.N. 2010. Research on the Evalua-tion Method for the RAM goals of CTCS-3. China Railway Science 31(6): 92-97.
3. CTCS3-300T onboard system maintenance specification. National Railway Research and Design Institute of Signal and Communication, Beijing, China, 2010.
3. Su, H.S. and Che, Y.L. 2014. Dependability Assessment of CTCS-3 On-Board Subsystem Based on Bayesian Network. China Railway Science 35(5): 96-104.
4. S. Qiu, M. Sallak, W. Schön, Z. Cherfi-Boulanger, at al. Availability assessment of railway signalling systems with uncertainty analysis using Statecharts. Simulation Modelling Practice and Theory 2014; 47: 1-18.
5. S. Bernardi, F. Flammini, S. Marrone, at al. Model-Driven Availability Evaluation of Railway Control Systems. In: International Conference on Computer Safety, Reliability, and Security, 2011, pp.15-28.
6. P. Weber, G. Medina-Oliva, C. Simon, B. Iung. Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. Engineering Applications of Artificial Intelligence 2012; 25: 671-682.
7. H. Langseth and L. Portinale. Bayesian networks in reliability. Reliability Engineering and System Safety. 2007; 92: 92-108.

7. H. Boudali, J.B. Dugan. A discrete-time Bayesian network reliability modeling and analysis framework. Reliability Engineering and System Safety 2005; 87: 337-349.
8. M. Neil, D. Marquez. Availability modelling of repairable systems using Bayesian networks. Engineering Applications of Artificial Intelligence 2012; 25: 698-704.
9. X.F. Liang, H.D. Wang, H. Yi, D. Li. Warship reliability evaluation based on dynamic bayesian networks and numerical simulation. Ocean Engineering 2017; 136: 129-140.
10. B.p. Cai, Y.h. Liu, Y.W. Zhang, Q. Fan, S.L. Yu. Dynamic Bayesian networks based performance evaluation of subsea blowout preventers in presence of imperfect repair. Expert Systems with Applications 2013; 40: 7544-7554.
11. B.P. Cai, Y.H. Liu, Y.P. Ma, L. Huang, Z.K. Liu. A framework for the reliability evaluation of grid-connected photovoltaic systems in the presence of intermittent faults. Energy 2015; 93: 1308-1320.
12. S. Barua, X.D. Gao, H. Pasman, M. Mannan. Bayesian network based dynamic operational risk assessment. J Loss Prev Process Ind 2016; 41: 399-410.
13. X.G. Wu, H.T Liu, L.M. Zhang, at al. A dynamic Bayesian network based approach to safety decision support in tunnel construction. Reliability Engineering and System Safety 2015; 134: 157-168.
14. CTCS-3 system requirements specification. Ministry of Railways, Science and Technology Division, Beijing, China, 2008.

15. CTCS-3 function requirements specification. Ministry of Railways, Science and Technology Division, Beijing, China, 2008.
16. A.G. Wilsona and A.V. Huzurbazar. Bayesian networks for multilevel system reliability, Reliability Engineering & System Safety, 2007, pp.1413-1420.
17. K.P. Murphy. Dynamic Bayesian Networks: Representation, Inference and Learning. University of California, Berkeley, 2002.
18.A. Bobbio, L. Portinale, M. Minichino and E. Ciancamerla, Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. Reliability Engineering and System Safety. 2001, pp.249-260
19. L. Portinale, D.C. Raiteri, S. Montani. Supporting reliability engineers in exploiting the power of Dynamic Bayesian Networks. International Journal of Approximate Reasoning. 2010; 51: 179-195.
20. S. Montani, L. Portinale, A. Bobbio, D.C. Raiteri. RADYBAN: A tool for reliability analysis of dynamic fault trees through conversion into dynamic Bayesian networks. Reliability Engineering and System Safety 2008; 93: 922-932.
21. J.B Dugan and K.S Trivedi. Coverage Modeling for Dependability Analysis of Fault-Tolerant Systems. IEEE Transaction on reliability 1989; 38: 775-787.
22. B. Jones, I. Jenkinson, Z. Yang, J. Wang. The use of Bayesian network modelling for maintenance planning in a manufactoring industy. Reliability Engineering and System Safety 2010; 95: 267-277.
23. University of Pittsburgh, GeNIe and SMILE-Home, (n.d.), ⟨https://dslpitt.org/genie/⟩.