Reliability Assessment on CTCS-3 Train Control System Using Faults Trees and Bayesian Networks

Hongsheng Su and Yulong Che

School of Automation and Electrical Engineering,
Lanzhou Jiaotong University, Lanzhou 730070, China

shsen@163.com, cylg717@163.com

Abstract

China Train Control System (CTCS-3) is a safety critical computer system that features large-scale, complex structure, and redundant configuration. CTCS-3 and as well as the equipment and technologies related to it can ensure the safety and reliability running of high-speed trains, and so the assessment on its reliability becomes very important. Generally, the two elements such as common cause factor (CCF) and failure mode polymorphism can not be ignored when assessing the reliability on a large complicated system. There are some limitations existing when applying the traditional fault tree analysis (FTA) is used to deal with the two factors mentioned above, and considering that Bayesian network (BN) possesses the abilities of bidirectional reasoning and the uncertain knowledge solving, and therefore BN is introduced to change the flaws. The method firstly establishes the FTA model of system from top to bottom, and then converts the FTA model into BN model from the lower to the upper, hierarchically. Eventually, the reliability indices are calculated using the BN with regard to the CCF and multi-state factors. Through integrating and evaluating sub-models using the approach with FTA combined with BN in the CTCS-3 system, some interesting results are acquired. The relative results show that the proposed approach is quite effective, and also provides a theoretical basis to improve the system reliability.

Keywords: *CTCS-3 Train Control System, Fault Tree, Bayesian Networks, Common Cause Failure, Multi-state, Reliability Evaluation*

1. Introduction

The reliability of high-speed train operation directly relates to the security of passenger lives and properties. There shall be very serious consequences when an accident occurs. Train control system is the core equipments and technologies to guarantee the safety, reliability and efficient operation of the high-speed train, and so its reliability and security assessment possesses very importance significance. China Train Control System (CTCS-3) is a safety-critical computer system in high speed train signaling system where a large number of complex electronic associated components and computer systems are applied [1, 2]. CTCS-3 possesses large complicated structure and redundancy configuration for the key equipments. Therefore, the requirements for reliability and security assessment on CTCS-3 is becoming higher and higher.

In CTCS-3, the correlation is the common feature of its failures. Common cause failure (CCF) is a kind of dependent failure, and also is an important factor causing system internal failure, dependently. It is apt to generate greater error if common cause failure is ignored [3]. Presently, the β factor model is often applied in CCF analysis. However it just is used in the 2-unit redundant system [4]. In traditional reliability analysis, it is always assumed that the

components or systems have only two states, such as work or failure, while it overlooks the system performance affected by dependent components and other failure states. There exists great difference between the established reliability analysis model and real situation [5]. Thus, Multi-state System (MSS) reliability analysis has received extensive attention. The reliability analysis on MMS with CCF based was reported in [6, 7]. However, the applications are lack in CTCS-3.

Fault Tree Analysis (FTA) is the common-used method in system reliability analysis, which has widely applied in railway reliability analysis [8, 9, 10]. By using figure deduction and establishing logical diagram, FTA can calculate the reliability of system and importance of component. FTA hypothetical event is two-value and independent, and so it can not solve the modeling problem of complicated system. As the number of bottom events and logical gates increasing, the calculation accuracy will be low, and the process time-consuming. With regard to the complicated system such as CTCS-3, the system failure process presents complicated dynamic characteristics as system complexity increasing in structures and functions. Meanwhile, there are some phenomena existing like CCF and system polymorphisms, and etc. Therefore, FTA has finite analytical abilities in train control reliability assessment.

Bayesian Network (BN) has continued to evolve and develop in the field of reliability that well remedy the limitation of traditional reliability method [11, 12, 13]. BN expresses the dependency between nodes in diagrams which is straightforward and prone to bidirectional reasoning. BN reduces not only contingent probability dimension of non-root node, but also greatly drops the computation complexity in reasoning process by utilizing conditional independence relations between variables. Hence, it is applied to express and analyze the uncertain knowledge. In the bidirectional reasoning mechanism and state description view, it has not merely FTA merits but also has the ability of disposing CCF, and system polymorphisms and uncertain logical relationships [14].

In this paper BN is combined by traditional FTA. It puts system internal logical relationship into reliability assessment to find out composite modes affecting train control system failures through BN bidirectional reasoning ability. And thus, it can find out weak links of system, and provide help to improve train control system reliability. The tool of HUGIN 7.7 simplifies the counting process, efficiently.

The paper is organized as follows: Section 1 presents the CTCS-3 introductions and its corresponding fault tree model; Section 2 discusses the architecture and property of BN and as well as the transformation from FTA to BN; Section 3 gives out the reliability modeling method applying BN based on CCF and multi-mode failure system; Section 4 synthesizes FTA and BN to perform reliability assessment of CTCS-3; Section 5 gives out some conclusions and hints for future work.

2. CTCS-3 train control system and fault tree model

2.1. CTCS-3 train control system

CTCS-3 Train Control System achieves train-ground information transmission based on Global System for Mobile communication-R (GSM-R) radio communication. Radio Block Center (RBC) grants the Movement Authority (MA). Track circuit achieves the train occupancy checking, and Balise systems achieve the dynamic orientating of trains. It satisfies the requirements of train operating with speed at 300～350km/h and minimal tracking intervals of 3min. It is equipped with train operational control system of CTCS-2 function. CTCS-2 Train Control System is the primary train control system for

200～250km/h trains, and the standby system of 300km/h and above high-speed trains [15].

Structure of CTCS-3 is shown in Figure 1, including ground subsystem and on-board subsystem. The on-board subsystem consists of Vital Computer (VC) [16], Track Circuit Information Receiver (TCR), Balise Transmission module (BTM) and BTM antenna, Specific Transmission Module (STM), Radio Transmission Unit (RTU), Driver Machine Interface (DMI), Train Interface Unit (TIU), Speed and Distance Unit (SDU) and Juridical Recorder Unit (JRU). Ground subsystem is constituted by RBC, Train Control Centre (TCC), track circuit, Balise system (including trackside electronic unit Lineside Electronic Unit (LEU)) and Temporary Speed Restriction (TSR).

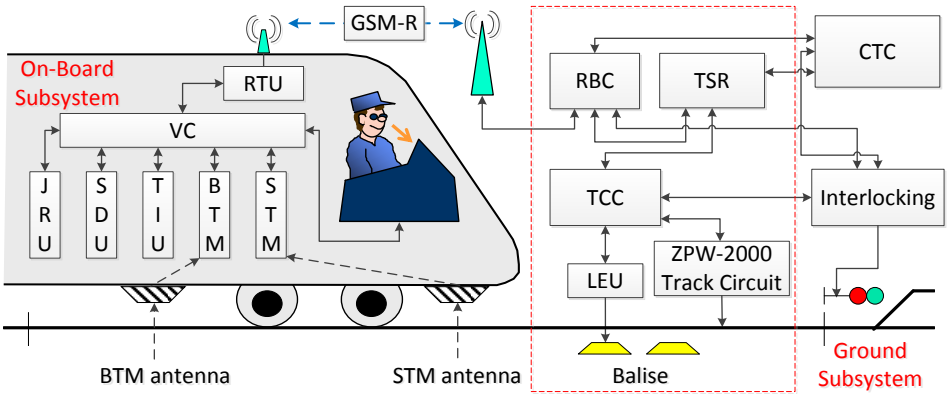


Figure 1. Structure diagram of CTCS-3

In order to improve the reliability and safety of the Train Control System, the entire train control system uses numerous redundancies cells, for instance, dual module hot spare, and double 2-vote-2, and 2-vote-3, and as well as the subsystem of train control system. The less reliable constituents should meet the system level RAM requirement of CTCS-3 as a safety critical computer system. The research on the safety part is not in the scope of this work, and thus we will consider only RAM specification alone. According to the system requirements specification of CTCS-3 Train Control System and the EN 50129 standard, Table 1 summarizes the most regardful indices that will be considered in the following sections.

Table 1. RAM indices of CTCS-3

Indices	Description	Value
MTBF	Mean time between failures	$\geqslant 10^5$h
A	Availability	$\geqslant$99.99%
MTTR	Mean time between repair	<10 h

The devices such as VC, BTM, TCR, RTM, DMI, TIU, and other key devices are adopted redundancy configuration. The VC contains CTCS-3 control unit and CTCS-2 control unit with separately setting and simultaneous running. CTCS-3 control unit takes charge of the core control function as CTCS-3 Train Control System works

normally, and CTCS-2 control unit takes charge of the core control unit of spare system, and the cells, such as DMI, TIU, SDU, and BTM, are shared by the two. Linking GSM-R unit, CTCS-3 control unit is responsible for the system bus management and uniform output. CTCS-2 control unit connects with TCR form which it obtains the MA [17].

The cells of RBC, TCC, track circuit, Balise system (including LEU), and TSR, and other key devices of ground adopt redundancy configuration. RBC provides MA, static speed profile, and temporary speed restriction order for trains. It also transmits data with CTC and stations interlocking systems which are peripherals of train control systems that can be not considered during the train control system reliability analysis process.

2.2. CTCS-3 train control system fault tree model

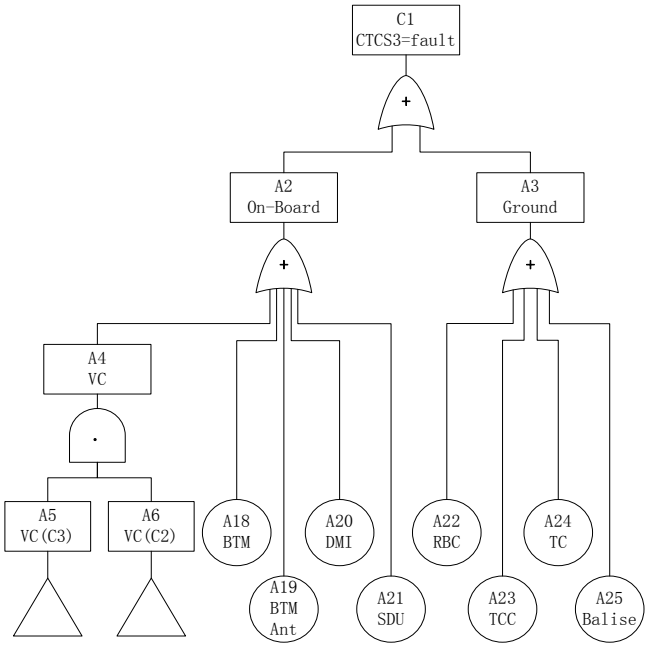
FTA is a deductive, structured reliability analysis method to determine the potential causes of an undesired event based on two-value states and static fault logical, and is widely used in reliability and safety analysis of complex systems. This paper did not present the FTA details since it has been widespread used and has mature technical specifications. Usually, the constructed FTA program is implemented as follows: (i) To select the top event; (ii) To establish fault tree downwards; (iii) To assess fault tree model qualitatively and quantitatively.

Seen from the function, the core function of CTCS-3 is to prevent the train outside the train control system under the safe speed and distance. Here, some executable indices, such as the train delays events and transmission errors, are not considered as they have nothing to do with the train safety, likewise, the harm caused by equipment error outside the train control system also is not considered. Assuming that there is no online maintenance during operation.

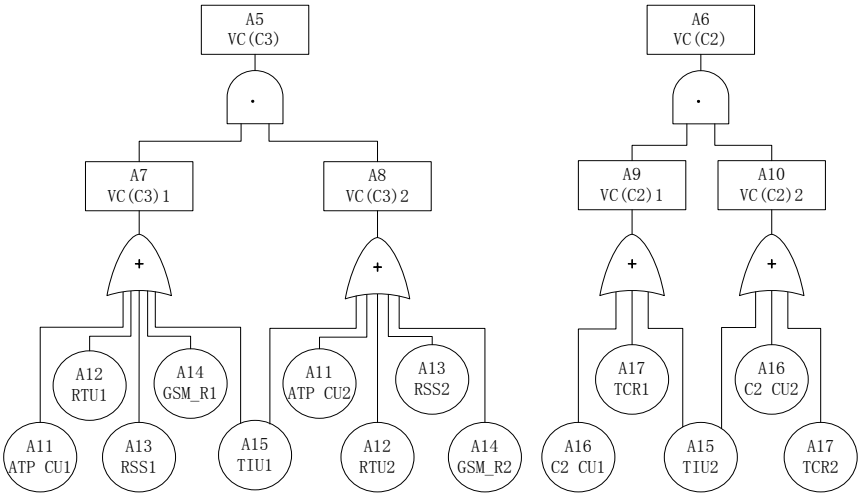
The fault tree structure of CTCS-3 is established from the perspective of safety function of CTCS-3. In accordance with the basic steps of the FTA model, the CTCS-3 failure is selected as the top event of fault tree (FT), firstly, and then the whole FT is created from top to bottom according to the functional logic relationship of each event as shown in Figure 2. It should be noted that the FT is actually a concept FT of the function structure of CTCS-3, where the cells A18, A19, …, A25 are the bottom events, all such cells have redundancy configurations, containing a lot of devices that be handled as a whole during the process of establishing FT. In here we only present FT structures of CTCS-3 control unit (event A5, as shown in Figure 2-b) and CTCS-2 control unit (event A6, as shown in Figure 2-c) as the representatives of redundancy configuration structures.

The created FT contains ten logic gates, fifteen root events, and ten intermediate events. The logical expression of the top event can be viewed as a function of minimal cut sets as shown in (1).

$$C1=A5A6+A18+A19+A20+A21+A22+A23+A24+A25 \quad (1)$$



(a) Notional FT of CTCS-3



(b) FT of event A5 (c) FT of event A6

Figure 2. FT of CTCS-3

Supposed that the end of the event is independent of each other in the FT, and the events in the entire system exist only in both working and non-working two states. The system components follow the exponential distribution. Table 2 shows the list of the event, codes, names, and their prior probabilities in CTCS-3 FT, the data come from the references [18, 19, 20], where 365 days as a year, and 24 hours as a day.

Table 2. The event, codes, names, and their prior probabilities in FT of CTCS-3

Event Number	Event Code	Event Name	Failure Rate(/h)
1	C1(CTCS3fault)	CTCS3 fault	—*
2	A2(On-Board)	On-Board Subsystem fault	—
3	A3(Ground)	Ground Subsystem fault	—
4	A4(VC)	VC fault	—
5	A5(VC(C3))	VC level 3 fault	—
6	A6(VC(C2))	VC level 2 fault	—
7	A7(VC(C3)1)	Master VC level 3 fault	—
8	A8(VC(C3)2)	Spare VC level 3 fault	—
9	A9(C(C2)1)	Master VC level 2 fault	—
10	A10(VC(C2)2)	Spare VC level 2 fault	—
11	A11(ATP CU)	ATP CU fault	1.49×10^{-5}
12	A12(RTU)	RTU fault	1.80×10^{-5}
13	A13(RSS)	RSS fault	1.20×10^{-5}
14	A14(GSM-R)	GSM-R fault	1.45×10^{-8}
15	A15(TIU)	TIU fault	2.10×10^{-5}
16	A16(C2 CU)	C2 CU fault	1.20×10^{-5}
17	A17(TCR)	TCR fault	2.30×10^{-6}
18	A18(BTM)	BTM fault	2.00×10^{-6}
19	A19(BTM Ant)	BTM Ant fault	7.00×10^{-8}
20	A20(DMI)	DMI fault	5.00×10^{-6}
21	A21(SDU)	SDU fault	2.50×10^{-9}
22	A22(RBC)	RBC fault	5.00×10^{-8}
23	A23(TCC)	TCC fault	2.50×10^{-8}
24	A24(TC)	Track Circuit fault	3.50×10^{-7}
25	A25(Balise)	Balise System fault	2.90×10^{-6}

*Note: * represents the intermediate event*

3. Theory of Bayesian Networks

3.1. Architecture of Bayesian Networks

BN, known as belief nets, causal networks, probabilistic and dependence graphs, and etc, are a directed acyclic graph (DAG) which is made up of the nodes and the edges. One BN with N nodes consists of two parts: one is mode structure, namely, the N-node DAG; the other part is relevant parameters. From another perspective, similar to FTs, BNs consist of both qualitative and quantitative parts. The nodes represent variables that can be abstraction of any things, such as the events, equipment state observation value, and *etc*. Arcs signify direct causal relationships between the linked nodes. The relevant parameters denote the marginal probability of root node, and conditional probability between nodes. The conditional probability tables (CPT) assigned to the nodes specify how strongly the linked nodes influence each other. For the directed edges (V_i, V_j), V_i is called the child node of V_j, and V_j is called the parents of V_i. The local conditions dependency of BN model can be conveyed by the annotation of

conditional probability distribution (CPD) and the uncertain knowledge expressed by graphical methods [21].

Let the nodes set $V=\{X_1, X_2,\cdots, X_n\}$ represents n random variables on U, BN(BS, BP) stands for a BN on U, where BS=(V, E) is a DAG Γ defined on variables set V. Discrete variables V and the edges E are assigned to the node-set and the causal probabilistic relationship among the nodes of Γ, respectively. BP is the probability distribution of nodes.

$$BP = \{P(X_i \mid \pi X_i)[0,1] \mid X_i \in V\} \tag{2}$$

where πX_i represent the directly parent nodes of X_i in BN.

The simple quantitative analysis is based on the conditional independence assumption. Given three random variables X, Y, Z, X is said to be conditionally independent from Y given Z if $P(X,Y \mid Z) = P(X \mid Z)P(Y \mid Z)$. With the independence of BN, it can greatly reduce the number of parameters required to calculate the joint probability distribution. Due to these assumptions, the quantitative part is completely specified by considering the probability of each value of variables conditioned by any possible instantiation of its parents.

BN takes advantage of the conditional independence and the chain rule to perform quantitative analysis. And BNs indicate the joint probability distribution $P(V)$ of variables $V=\{X_1, X_2,\cdots, X_n\}$ included in the network as

$$P(V) = \prod_{i=1}^{n} P(X_i \mid \pi X_i) \tag{3}$$

The foundation of BN is Bayes theory, and Bayesian formula is defined as follows.

Let B_1, B_2, …, B_n be mutual exclusive variable on simple spatial S, that is,

$$\begin{cases} P(\bigcup_{i=1}^{\infty} B_i) = 1 \\ B_i \cap B_j = \varnothing, i \neq j \\ P(B_i) > 0 \end{cases} \tag{4}$$

Let A be a variable on S, $P(A)>0$, for each k, we have

$$P(B_k \mid A) = \frac{P(A|B_k)\ P(B_k)}{\sum_{i=1}^{\infty} P(A|B_k)\ P(B_k)} \tag{5}$$

The initial probability $P(B_k)$ and amendment probability $P(B_k|A)$ are named prior distribution and posteriori distribution, respectively, and $P(A|B_k)$ is a likelihood function.The prior distribution is a probability density function of the parameters estimated before observing data. The prior distribution does not have to hold an objective foundation, and it can be partially or completely based on subjective belief. The Likelihood function responds the sample information, and it is equivalent to a given probability distribution of sample data for estimating the parameters under the conditions.

3.2. BN nature in reliability

BN is a kind method to be applied to express the knowledge based on the probabilistic reasoning structure, which has a solid probability theory foundation. A BN

is founded on the basis of prior information and existing data, and then it can combine the data from various sources and draw inferences about these data, synthetically. The probabilistic reasoning is a process of calculating the other variables information by the given variables information. The certainty state of a variable intitules evidence, expressed by E, and the evidence E can update the BN belief. The chief task of BN is to calculate the posterior probability when the evidence E is entered: $P(X_i)$ expresses the probability distribution of $X_i \in X$ when there is no evidence. $P(X_i)$ is the prior probability distribution of X_i, and then $P(X_i|E)$ is the posterior probability distribution after X accepts the evidence E.

$$P(X_i|E) = \sum_{X \setminus X_i} P(X) \times \varepsilon_E \tag{6}$$

where ε_E means the probability of the evidence E.

BN owns two inference that is forward inference and backward inference. The purpose of BN inference is to calculate the probability of a certain event occurrence by joint probability distribution formula with the known evidence under given the BN structure. The forward reasoning of BN, also known as causal inference, it can compute the conditional probability of network working or malfunction under the evidence of any one or more variable nodes provided. The backward reasoning can calculate the conditional probability of any one or more variable nodes and diagnose the weak links of networks when the network is broken-down.

3.3. Mapping fault trees to Bayesian Networks

FT is a logical reasoning using the graphical interpretation in case of certain condition of event fault. The FT analysis conducted by a logical diagram (fault tree) comes into being the cause of a system failure (hardware, software, human factors, environment, and *etc*.). Thereby the cause and the probability of system failure occurrence can be defined. The basic assumptions of the standard FTA methodology are recalled as: (i) events are binary events (working or non-working); (ii) events are statistically independent.

Assuming that the set K_1, K_2, $\cdots$, K_n is the minimal cut sets of the FT already obtained, and it is known the occurrence probability of the basic events x_1, x_2, $\cdots$, x_n, and then the minimal cut sets of structure functions is

$$\phi(K_1, K_2, \cdots, K_n) = \prod_{i=1}^{n} x_i \tag{7}$$

The probability of the top event T is,

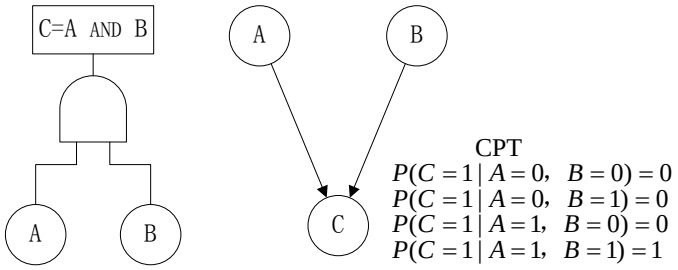
$$P\{T\} = P\left\{\bigcup_{i=1}^{n} K_i\right\} \tag{8}$$

So, the reliability of the system is obtained by

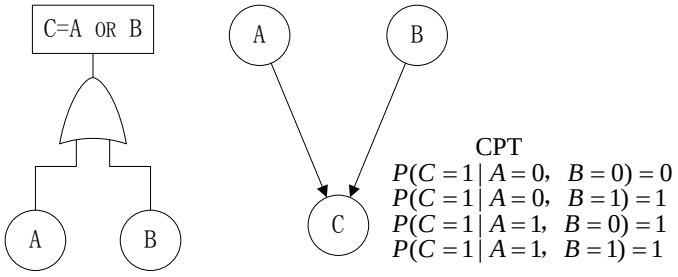
$$R_s = 1 - P\{T\} \tag{9}$$

There is a limit when FTA is employed in large complex and dynamic system, due to the assuming constraints. BN has been widely used in the field of reliability at home and abroad because of the conditional independence of BN nodes and bidirectional reasoning mechanism. Meanwhile, it has formed a complete set of methods for mapping

FT to BN [22, 23]. Figure 3 shows the way how the logical AND and OR gates in fault tree is converted to the equivalent nodes in BN. Assume that C=1 indicates the event C occurs, C=0 indicates the event C works normally. Readily seen, the logical relationship of the fault tree can be expressed in BN corresponding to the CPT of the nodes simply. According to the conversion rules for the basic gates, it is easy to implement an FT mapping into a binary BN. A root node is created in BN correspondence with each leaf node of the FT. The information of root nodes and intermediate nodes of the FT are corresponding to marginal distribution and CPT in BN, respectively.



(a) Fault Tree- AND Gate Bayesian Networks-AND Node



(b) Fault Tree- OR Gate Bayesian Networks-OR Node

Figure 3. FT logic gate to the transformation of the Bayesian Networks

Mapping FT to BN is a reaction that the logic gate relationship of FT is expressed by nodes and CPT in BN equivalently. View from the description of the system state and reasoning process, mapping FT to BN can be divided into two parts, graphics mapping and value mapping. Corresponding to two principles: (i) events in the FT and nodes in BN is one to one correspondence; (ii) the CPT of BN is the reaction of the relationship among logical gates of FT.

4. Reliability modeling methods on CCF and MSS in BN

4.1. Reliability model of common cause failure in BN

CCF is more than one part, unit or system failure caused by the same kind of external event. To apply BN to establish CCF model, the key is to separate the common cause components of system into the independent failure components and the CCF

components. Two sub-components are in series, in which the failure rate of common cause components can be divided into common cause failure rate and independent failure rate. After the two sub-components are connected, we will consider the logical relationship between other non-common cause components and the two sub-components.

Take parallel system for example to explain the process of establishing CCF model by BN. Supposing two states exist in system X and component D_1, D_2. State 0 means the system or component works normally. State 1 means failure of the system or component.

Without regard to common cause failure, the reliability of system is showed as follows:

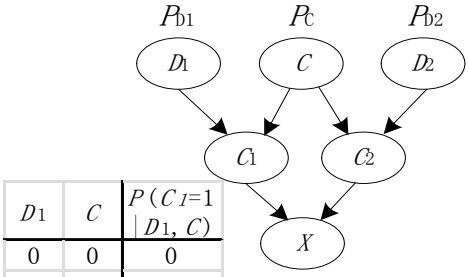
$$R_s(t) = 1-(1-R_1(t))(1-R_2(t)) \tag{10}$$

If the component life distribution obeys the exponential distribution,

$$R_i(t) = e^{\int_0^t \lambda_i(t)dt}, \quad i=1,2 \tag{11}$$

$R_i(t)$, $\lambda_i(t)$ express the degree of reliability and failure rate of component i, respectively. $R_s(t)$ express the reliability degree of system.

Regard to common cause failure, parallel system CCF model established by BN is showed as Figure 4. D_1, D_2 and C are root nodes. D_1, D_2 express independent failure factors. P_{D1} and P_{D2} mean independent failure rates. C presents common failure component. P_C indicates common cause failure rate. Node C_1 shows the state that independent failure component D_1 of common cause failure component 1 and common cause failure component C are in series. Node C_2 denotes the state that independent failure component $D2$ of common cause failure component 2 and common cause failure component C are in series. Node X expresses the state which C_1 and C_2 are in parallel.



D_1	C	$P(C_1=1 \mid D_1, C)$
0	0	0
0	1	1
1	0	1
1	1	1

C_1	C_2	$P(X=1 \mid C_1, C_2)$
0	0	0
0	1	0
1	0	0
1	1	1

Figure 4. BN model for parallel system with CCF

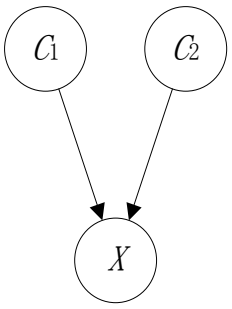
Set the independent failure rate of D_1 and D_2 equal. That is $P_{D1}=P_{D2}=P$. The reliability degree of system is:

$$\begin{aligned} p(X=0) &= \sum_{D_1,D_2,C,C_1,C_2,X} p(D_1,D_2,C,C_1,C_2,X) \\ &= \sum_{C_1,C_2} \{p(X=0\mid C_1,C_2) \\ &\quad \cdot \sum_{D_1,C} [p(C_1=0\mid D_1,C)p(D_1)p(C)] \\ &\quad \cdot \sum_{D_2,C} [p(D_2=0\mid D_2,C)p(D_2)p(C)]\} \\ &= 2p(D_1=0)p(\mathrm{C}=0) - p^2(D_1=0)p(\mathrm{C}=0) \\ &= 2P\cdot P_c - P^2\cdot P_c \end{aligned} \tag{12}$$

4.2. Reliability model of multi-state system in BN

A component or system features multiple failure modes constantly and actually. For example, besides working normally, diodes have two other failure states—short-circuit and open circuit. Modeling for reliability of multimode system, we should ensure the states of nodes of BN and components of system and provide the failure rate of each state. Then the relationship among the states of components is described by probability distribution to express the state of relevant nodes.

Take the parallel system of two tri-states components for example to describe BN model of multimode system reliability, as shown in Figure 5. Taking 0, 1, 2 represent the three states of the system and components respectively—open circuit, short circuit and normal. P (•) represents the state probability of system or component. In Figure3, node C_1 and node C_2 express two components states. X represents system state. The initial probability of three states of C_1 and C_2 should be given. The state of system node X is analyzed by CPT (Condition the different states of C_1 and C_2). Then the hard expressed relationship of multimode components can be easily and clearly described.



C_1	C_2	X	$P(X=1\mid C_1, C_2)$	$P(X=2\mid C_1, C_2)$
0	0	0	0	0
0	1	1	1	0
0	2	2	0	1
1	0	1	1	0
1	1	1	1	0
1	2	1	1	0
2	0	2	0	1
2	1	1	1	0
2	2	2	0	1

Figure 5. Reliability model of parallel system in BN with two three-state components

Clearly, as C_1=1 or C_2=1, then X=1.

as C_1=0 and C_2=0, then X=0.

as $C_1 \neq 1$, C_2=2 or C_1=2, $C_2 \neq 1$, then X=2.

According to Figure 5, the probability of parallel multi-state system is solved as follows:

$$\begin{aligned} P(X) &= \sum_{C_1,C_2} P(C_1,C_2,X) \\ &= \sum_{C_1,C_2} P(C_1)P(C_2)P(X \mid C_1,C_2) \\ &= \sum_{C_1} P(C_1) \sum_{C_2} P(C_2)P(X \mid C_1,C_2) \end{aligned} \tag{13}$$

According to the prior probabilities and the conditional probability table, we can easily calculate the probability of the parallel system.

5. Reliability modeling of CTCS-3 train control system based on BN

Introducing the Bayesian network technology, and starting from the end of event in fault tree, the hierarchical establishment of CTCS-3 Train Control System Bayesian network reliability assessment model is conducted from the lower to the upper on the basis of the conceptual fault tree of CTCS-3 associated the actual operation of the train control system.

5.1. Reliability calculation of the root node considering CCF

The bottom events of FT are mapped to the root node in BN. According to the description of Section 1.2, in addition to the DMI and BTM unit that they are dual cold standby structure and can be seen as monophyletic, the remaining parts are hot standby redundant structure among the end of events in conceptual fault tree. Being the momentous failure source of redundant systems, CCF advances the joint failure probability of each failure modes of systems and then results to the reduction of the redundant system reliability.

In this paper, β-factor model has been used to analyze the CCF of the redundant equipment. Described in Section 3.1, the total probability of failure for each component can be expanded into an independent and a dependent contribution. The select principle of CCF probability is in accordance with β-factor in the range of 0.1% to 10% for hardware failure reflected by experts opinions [24].

Considering the CCF, the reliability parameters of root nodes in BN reliability model of CTCS-3 are calculated as instance the dual-redundant configuration of radio transmission unit (RTU). From Table 1, the failure rate of one RTU component is $\lambda_1=1.80\times10^{-5}$ /h, and the common cause failure rate is set as $\lambda_2=1.80\times10^{-6}$ /h when two RTU components are faulty simultaneously. Figure 6 is the parallel reliability block diagram of a dual RTU.

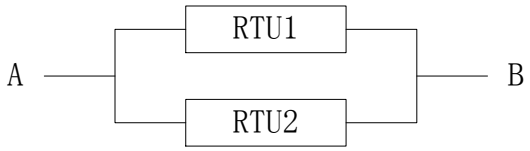


Figure 6. Parallel reliability block diagram of a dual RTU

The BN reliability model considering CCF of dual RTU is same to the CCF BN reliability model of parallel system as shown in Figure 4. The node D_1, D_2 indicate

independent failure factor of RTU1 and RTU2, respectively, and the node C represents the CCF. The value taking 1 or 0 signifies the variable's state on behalf of the event to be invalid or work properly, respectively. The node C_1 expresses the state that the relationship is in series between the independently lapse factor D_1 of RTU1 and the CCF C, similarly, the node C_2 expresses the state that the relationship is in series between the independently lapse factor D_2 of RTU2 and the CCF C . The node X means the state C_1 and C_2 are in parallels. The probability of $P(X=1|C_1, C_2)$ is the failure rate of the dual RTU system considering the CCF.

Let t =2×10^4 h. Without regard to the CCF, the reliability of one component is

$$P = P_1 = P_2 = \exp[-(\lambda_1 + \lambda_2)t] = 0.6730$$

The reliability of the dual RTU system is

$$R_s(2\times10^4) = 2\exp(-\lambda_1 t) - \exp(-2\lambda_1 t) = 0.9086$$

With regard to the CCF, the reliability of one component is

$$P_s = P_{s1} = P_{s_2} = \exp(-\lambda_1 t) = 0.6977$$

$$P_c = \exp(-\lambda_2 t) = 0.9646$$

The reliability of the dual RTU system is obtained from the Eq. (12),

$$R_c(2\times10^4) = 2P_s \cdot P_c - P_s^2 \cdot P_c = 0.8765$$

Assumed that the task time t =2×10^5 h, the Figure 7 shows the system reliability contrast curves varied with time between the BN reliability model considering CCF and the reliability model on assumption of independent units without CCF. Judging from the single-point reliability calculations and continuous-time reliability contrast curve, we can see $R_c(t) < R_s(t)$ in the parallel case, while it is opposite in the series case.

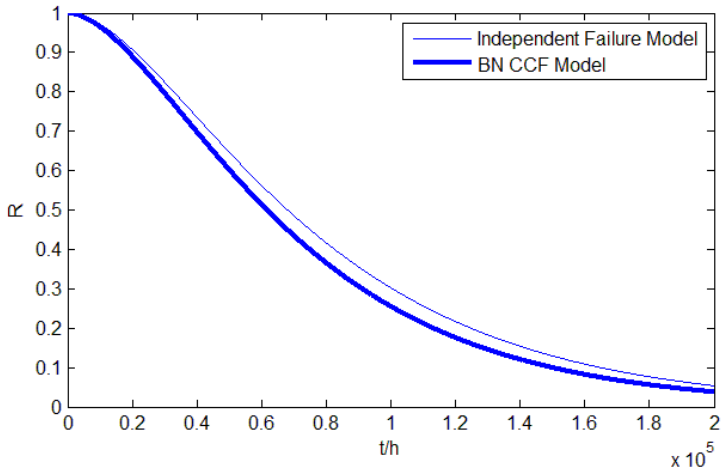


Figure 7. The reliability correlation curve of dual RTU

Similarly, t=2×10^{4}h, the reliability of other dual redundant configuration component can be obtained on the condition with regard to CCF or without regard to CCF, as shown in Table 3.

Table 3. Reliability of root node whether considering CCF

Component	λ_1 (/h)	λ_2 (/h)	$R_s(t)$	$R_c(t)$
ATP CU	1.49×10^{-5}	1.49×10^{-6}	0.9336	0.9062
RTU	1.80×10^{-5}	1.80×10^{-6}	0.9086	0.8765
RSS	1.20×10^{-5}	1.20×10^{-6}	0.9545	0.9318
GSM-R	1.45×10^{-8}	1.45×10^{-9}	1.0000	1.0000
TIU	2.10×10^{-5}	2.10×10^{-6}	0.8824	0.8461
C2 CU	1.20×10^{-5}	1.20×10^{-6}	0.9545	0.9318
TCR	2.30×10^{-6}	2.30×10^{-7}	0.9980	0.9934

where, λ_1, λ_2, $R_s(t)$, $R_c(t)$ indicate independent failure rate, CCF failure rate, reliability without considering CCF, reliability with considering CCF, respectively.

5.2. Reliability Assessment of intermediate node by example of the VC subsystem

An intermediate event in FT is mapped to an intermediate node in BN. Section 4.1 describes the reliability parameters calculation of root nodes considering the CCF. In this section, the BN reliability of intermediate nodes is assessed by the example of CTCS-3 control unit (VC (C3)) in On-board vital computer (VC). VC consists of CTCS-3 Train Control System control unit (VC (C3)) and CTCS-2 Train Control System control unit (VC (C2)), VC (C3) is the core security computer in normal operation of CTCS-3 line, and VC (C2) is the core of the backup system control functions. VC (C3) and its component units are hot standby redundant structure.

Firstly, in accordance with CCF reliability model with the previous consideration, the reliability parameters of each compositional unit in VC (C3) are computed, as shown in Table 3. The BN reliability model of VC (C3) (corresponding to Figure 2b, the fault tree of event A5) is established according to the front approach for mapping FT into BN, as shown in Figure 8. The node A7 and A8 are OR gate node, and A5 is AND gate node. The top event probability P=2.1×10^{-5}.

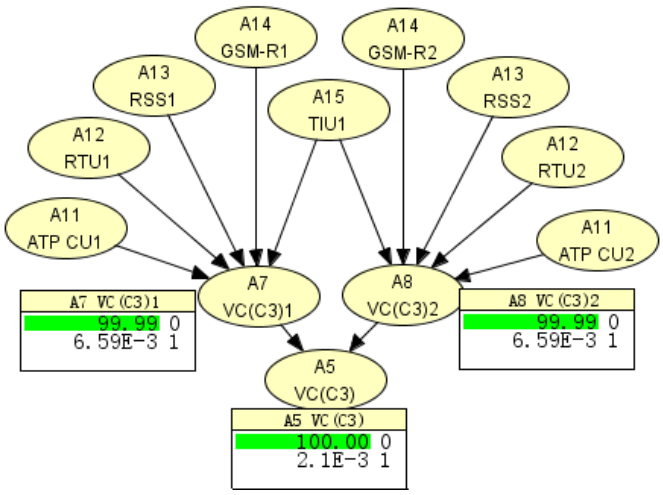


Figure 8. Bayesian Network diagram for VC redundant structure

For diagnostic reasoning, it is assumed that the subsystem (corresponding to the node A5) is broken-down, so the conditional probability of each component failure is calculated as shown in Table 4. This shows that the conditional probability of element A15 when the system is fault is 0.999904 that is maximum, because the equipment A15 is a share part of two sets of redundant subsystems (A7 and A8), so we can diagnose the element A15 is a vulnerable spot once a lineage of redundant subsystem is faulty.

Table 4. Component failure probability as system fails (diagnosis)

Node	A11	A12	A13	A14	A15
Failure Rate	4.68E-5	5.65E-5	3.77E-5	4.55E-5	0.999904

For cause and effect reasoning, the probability of subsystem failure is computed under the assumption that the components of master device VC (V3) 1 (A7 node) in VC (C3) (A5 nodes) is broken-down, as shown in Table 5. The dual module hot spare system will still be able to work properly as long as a lineage of redundant subsystem works, although the system is in a degraded state. As the member function logic relationship of the components of one lineage (such as VC (V3) 1, A7 node) in VC (C3) (A5 nodes) is OR, the conditional probability of A7 node is 1 when any one of component in VC (V3) 1 is broken-down.

Table 5. System failure probability as component fails (cause and effect)

	A11	A12	A13	A14	A15
A5	6.59E-5	6.59E-5	6.59E-5	6.59E-5	1
A7	1	1	1	1	1
A8	6.59E-5	6.59E-5	6.59E-5	6.59E-5	1

5.3. Reliability Assessment of CTCS-3 Train Control System

The reliability assessment of the entire CTCS-3 Train Control System is presented in this section. The degraded state of CTCS-3 Train Control System can be defined as the working status and can also be defined as the failure status, as there is no unified conclusion so far. Firstly, we consider the two-state system reliability assessment, namely the downgrade status seen as a failed state. Then we consider three state system reliability assessment, that is the upcoming degraded state looked upon another working state. The comprehensive reliability assessment proceeds under the consideration of the common cause failure and multi-state system.

5.3.1. Reliability Assessment of two-state CTCS-3 Train Control System: The BN modeling for reliability evaluation of CTCS-3 Train Control System is established from the FT of CTCS-3 using the algorithm of mapping FT to BN, as shown in Figure 9. C_1, A_2, and A_3 are an OR logic gate, and A_4 is an AND one.

The probability of occurrence of the top event using HUGIN 7.7 is $P_{two\text{-}state}= 1.04 \times 10^{-5}$. Compared with FTA, according to the minimal cut sets of FT (as shown in Eq.(1)), the probability of occurrence of the top event is $P_{FTA}=1.0398\times10^{-5}$ using the Eq.(8). It can be seen that the reliability of system obtained by BN is same to the one using FTA in two-state CTCS-3. Well, according to the Eq.(9), the reliability of the system: $R_{two\text{-}state}=1-P_{two\text{-}state} =1-1.04\times10^{-5}= 99.9989\%$. And it meets the reliability indices of CTCS-3 as shown in Table 1.

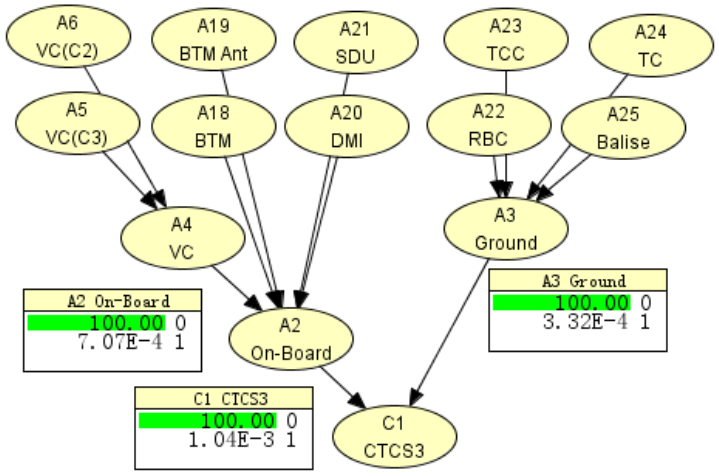


Figure 9. BN model of two-state CTCS-3

On the assumption that the top event (C_1 node) is a failure, the failure probability of each root node is calculated according to BN diagnostic reasoning, *i.e.*, Eq.(5), as shown in Figure10. Due to the failure rate of the equipment DMI A20 is 5×10^{-6}/h that is maximum, the conditional probability of failure of device A20 is 0.4879 that is also the largest one when the CTCS-3 system (C_1 node) is broken-down, so the equipment A20 is the weak link in the system.

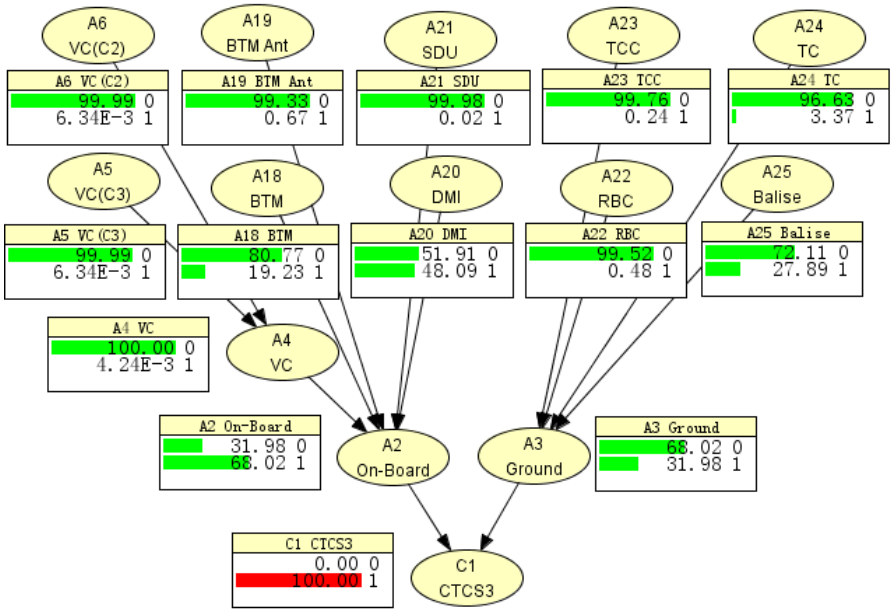


Figure 10. Model evaluation by means of the system failure (diagnosis)

The system failure probability is obtained using BN causal reasoning (*i.e.*, Eq. (6)) when each of the root node failure occurs, as shown in Table 6. Apparently, $P(C_1 \mid \overline{A_j}) = 1$,

(j=18,19,20,21,22,23,24,25), this shows that the CTCS-3 (C_1) will be broken-down in case any one of A_j (j=18,19,20,21,22,23,24,25) are faulty. The other value 1 also can be understood the meaning of expression.

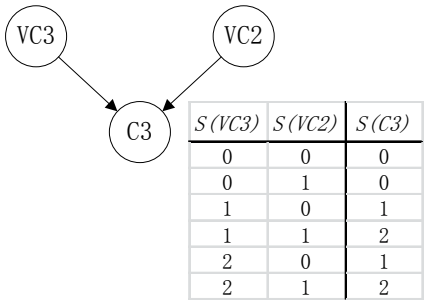
Table 6. Failure probability of system as subsystem fails (cause and effect)

	A5	A6	A18	A19	A20
C1	3.14E-5	3.14E-5	1	1	1
A2	2.81E-5	2.81E-5	1	1	1
A3	3.32E-6	3.32E-6	3.32E-6	3.32E-6	3.32E-6
A4	2.10E-6	2.10E-6	4.41E-10	4.41E-10	4.41E-10
	A21	A22	A23	A24	A25
C1	1	1	1	1	1
A2	1	7.07E-6	7.07E-6	7.07E-6	7.07E-6
A3	3.32E-6	1	1	1	1
A4	4.41E-10	4.41E-10	4.41E-10	4.41E-10	4.41E-10

From Figure 10 and Table 6, the conclusion can be further seen that different devices on the CTCS-3 Train Control System have different contributions, so the status of components is not in the same position. And thus this provides a reliable basis in order to further improve the reliability of the system. Improve the weak links that affect the system safety to increase the system security level.

5.3.2. Reliability Assessment of three-state CTCS-3 Train Control System: The degrade state that CTCS-3 level downgrades switch to CTCS-2 level in CTCS-3 Train Control system operational status is the most common situation in addition to the normal and fault condition. The degrade switch can be divided into the normal switching and the failure switching. Here, the degrade situation refers to the scenario of failure downgrade from CTCS-3 to CTCS-2 when the ground equipment or vehicle equipment are broken-down. Before CTCS-2 switches to CTCS-3, namely during VC (C2) controls the train, VC (C3) withdraws the function of controlling train, but VC (C3) and VC (C2) maintain communications with each other.

The VC (C3) has three kinds of states, state 0 and 1 indicates normal operation and fault itself, respectively, state 2 means VC (C3) exits controlling the train when ground equipment or vehicle equipment are faulty. VC (C2) has two states, state 0 represents the normal operation; state 1 represents fault itself. CTCS-3 Train Control system has three states, state 0 means C3-level train control system working properly, that is the train is controlled by VC (C3), and VC (C2) is in standby mode; state 1 means degraded operation, namely the train is controlled by VC (C2), and VC (C3) exits the function of controlling train; state 2 represents C3-level train control system is faulty, i.e., VC (C3) and VC (C2) are all broken-down. The reliability model of CTCS-3 train control system based on Bayesian network is established, as shown in Figure 11.



S(VC3)	S(VC2)	S(C3)
0	0	0
0	1	0
1	0	1
1	1	2
2	0	1
2	1	2

Figure 11. Three-state simplified BN model of CTCS-3

Among the rest, C3, VC3 and VC2 represents CTCS-3 train control system, VC (C3) and VC (C2), respectively. *S* (•) represents the state of the system or unit. Given the prior probability of VC3 and VC2 unit with different states, the node C3 state can be analyzed by the conditional probability table. Using the Eq.(13), the state probability of system can be calculated.

5.3.3. Reliability Assessment of CTCS-3 with regard to the CCF and multi-state: Consider the system with regard to the common cause failure and multi-state variables, known to the state 2 of the VC (C3) is caused by ground equipment or vehicle equipment failure. Here, it is assumed that the state 2 of the VC (C3) is caused by the RBC fault, GSM-R fault or On-board equipment failure, the relation of these three factors is OR logical. So it can be estimated that the probability of occurrence of VC (C3) status 2 for $P_{VC\ (C3)}$ =7.07×10^{-6}+1.45×10^{-8}+5.00×10^{-8}=7.13×10^{-6}. The BN model of a 3 status CTCS3 Train Control System is built according to the conceptual fault tree model (as shown in Figure2) of CTCS-3 combined with the actual operation of CTCS-3, as shown in Figure 12.

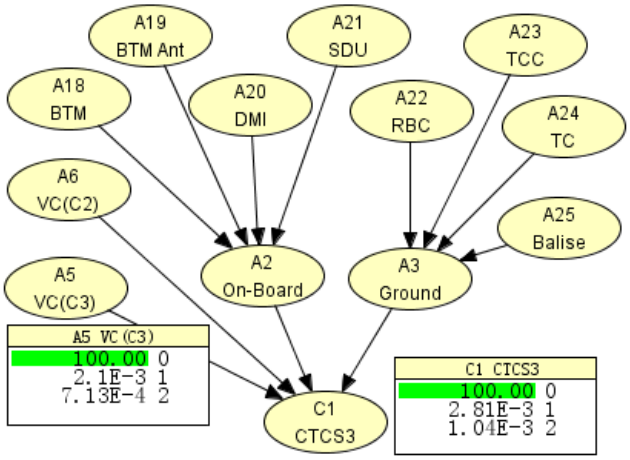


Figure 12. BN model evaluation of three-state CTCS-3

The calculating results are as follows: the probability of CTCS-3 train control system under degraded state is $P(C_1=1)=2.81\times10^{-5}$, and the probability of CTCS-3 train control system under failure state is $P(C_1=2)=P_{three\text{-}state}$ =1.04×10^{-5}. So the reliability of CTCS-3 is P (C_1=0)= $R_{three\text{-}state}$=1-2.81×10^{-5}-1.04×10^{-5} =99.9962%. Compared with the literature [17], the reliability of two-state CTCS-3 fulfills the system level requirement ($R_{two\text{-}}$

$_{state}$=99.9989% > 99.9985%), however the reliability of three-state CTCS-3 does not meet the system level requirement ($R_{three\text{-}state}$=99.9962% < 99.9985%).

It is thus clear that, $P_{two\text{-}state}=P_{three\text{-}state}$ and $R_{two\text{-}state} > R_{three\text{-}state}$, the failure probability of two state CTCS-3 taken the degraded state as failure status (as shown in Figure 9) is identical with the failure probability of three state CTCS-3 taken the degraded state as another working status (as shown in Figure 12). However, the reliability of two-state CTCS-3 is greater than the one of three-state CTCS-3.

It is known that the reliability of monophyletic unit system is obviously inferior to the reliability of dual unit system. Simultaneously, the degraded operation of three state CTCS-3 can be regarded as another working condition (correspond to the monophyletic unit system), and the normal operation of three state CTCS-3 can be seen as dual unit system. Ultimately, we can make a conclusion that the reliability of system degradation is less than the reliability of system normally. This can also be confirmed from the calculated results that the probability of system degradation is bigger than the probability of system failure ($P\ (C_1=1) > P(C_1=2)$). For the reason that, if the causes which lead to the CTCS-3 system degrade are prevented intensively, the occurring probability of switch from CTCS-3 level to CTCS-2 level can be reduced, and thereby the reliability of CTCS-3 Train Control System in runtime can be improved.

6. Conclusion

In this paper we have shown the compositional approach and the combination of Fault Tree Analysis and Bayesian Networks in order to evaluate system reliability aspects of CTCS-3 Train Control System. BN reliability assessment model of CTCS-3 with regard to common cause failure and multi-state is established according the fault tree of CTCS-3 combined with the actual operation of CTCS-3. This approach not only has the function of the traditional method of FTA, but also is superior to the traditional FTA in data calculation and reasoning. CTCS-3 acts as safety-critical computer system where the CCF and failure mode polymorphism cannot be ignored, while BN shows a clear advantage in dealing with these two aspects than FTA.

The reliability analysis and assessment on CTCS-3 allows us obtain several interesting results. Firstly, the reliability of system with regard to CCF is less than the one without regard to CCF, as the failure rate of components are higher, the result gets more and more obvious. Secondly, the reliability of system obtained by BN is same to the one using FTA in two-state CTCS-3. Last but not least, the reliability of two-state CTCS-3 that fulfills the system level requirements is greater than the reliability of three-state CTCS-3 does not meet the system level requirement, so the downgrade needs to be handled prudentially and objectively.

Bayesian Networks have the ability of uncertainty bidirectional inference, and bond the cause and consequence analysis of a failure effectively. It can also analyze the impact any one or more components' failure affecting the system failure, as well as compute the component failure probability under the condition of system failure. Thus the calculation of the minimal cut sets and important degree in FTA can be abstained. What is more, it is convenient to find the vulnerability of the system, and the efficiency of the system reliability analysis is greatly improved. The BN model also makes the reliability analysis of system more flexible and intuitive. It is very feasible that the reliability assessment method based on BN is introduced in the Train Control System, as well as other complex and dynamic railway signal systems. At the same time, as more integration of impact reliability factors and more accumulation of failure data, the

model realization will be greatly enhanced, and the proposed result of reliability assessment will be more objective.

Acknowledgements

This project is supported by Railways Ministry Technology Research and Development Program (2012X003-B).

References

[1] CENELEC 2003, "EN 50129 Railway Applications: safety related electronic systems for signalling", **(2003)**.
[2] F. Yan, "Safety assurance and assessment method research for train control system", China Safety Science Journal, vol. 20, no. 12, **(2010)**, pp. 98-104.
[3] J. Borcsok, S. Schaefer and E. Ugljesa, "Estimation and evaluation of common cause failures", Proceeding of Second International Conference on Systems, ICONS'07, **(2007)**, pp. 41-41, IEEE.
[4] X. W. Yin, W. X. Qian and L. Y. Xie, "Common cause failure model of system reliability based on Bayesian networks", China Mechanical Engineering, vol. 20, no. 1, **(2009)**, pp. 90-94.
[5] G. Levitin, "A universal generating function approach for the analysis of multi-state systems with dependent elements", Reliability Engineering and System Safety, vol. 84, no. 3, **(2004)**, pp. 285-292.
[6] G. Levitin, "Incorporating common-cause failures into non-repairable multistate series-parallel system analysis", IEEE Transactions on Reliability, vol. 50, no. 4, **(2001)**, pp. 380-388.
[7] C. Y. Li, X. Chen and X. S. Yi, "Reliability optimization of multi-state system in presence of common cause failures", China Mechanical Engineering, vol. 21, no. 2, **(2010)**, pp. 155-159,.
[8] Y. Zhang, C. Y. Liu, Q. H. Li, X. L. Hou, H. J. Yuan and M. Jiang, "Quantitative safety assessment method based on risk in railway system block center and countermeasures", China Railway Science, vol. 31, no. 4, **(2010)**, pp. 112-117.
[9] J. H. Liu, X. C. Dai, Z. Guo and Y. Wang, "Quantitative safety assessment method based on risk in railway system", China Railway Science, vol. 30, no. 5, **(2009)**, pp.123-128.
[10] Y. D. Zhang, J. Guo, X. C. Dai and G. Z. Bai, "Quantitative safety assessment method based on risk in railway system block center and countermeasures", China Safety Science Journal, vol. 22, no. 9, **(2012)**, pp. 37-42.
[11] Y. W. Yin, W. X. Qian and L. Y. Xie, "A method for system reliability assessment based on Bayesian networks", Acta Aeronautica et Astronautica Sinica, vol. 29, no. 6, **(2008)**, pp. 1482-89.
[12] H. Langseth and L. Portinale, "Bayesian networks in reliability", Reliability Engineering System Safety, vol. 92, no. 1, **(2006)**, pp. 92-108.
[13] B. P. Cai, Y. H. Liu, Q. Fan and Y. W. Zhang, "Application of Bayesian networks to reliability evaluation of software system for subsea blowout preventers", International Journal of Control and Automation, vol. 6, no. 1, **(2013)**, pp. 47–60.
[14] O. Doguc and J. E. Ramirez-Marquez, "A generic method for estimating system reliability using Bayesian networks", Reliability Engineering and System Safety, vol. 94, no. 2, **(2009)**, pp. 542-550.
[15] S. G. Zhang, "Overall technical program for CTCS-3 Train Control System", China Railway Publishing House, Beijing **(2008)**.
[16] Y. Furukawa, T. Yamauchi and H. Taniguchi, "Implementation and evaluation for sophisticated periodic execution control in embedded systems", International Journal of Control and Automation, vol. 4, no. 3, **(2011)**, pp. 87-106.
[17] Y. Y. Lin, L. Tan, X. Y. T and Y. Wei, Editors, "High-speed railway signaling technology", China Railway Publishing House, Beijing **(2012)**.
[18] L. Q. Li, X. G. Yuan and Y. N. Wang, "Research on the evaluation method for the RAM goals of CTCS-3", China Railway Science, vol. 31, no. 6, **(2010)**, pp. 92-97.
[19] F. Flammini, S. Marrone, N. Mazzocca and V. Vittorini, "Modelling system reliability aspects of ERTMS/ ETCS by fault trees and Bayesian networks", In: Safety and reliability for managing risk: Proceedings of the 15th European Safety and Reliability Conference (ESREL 2006), **(2006)**, pp. 2675–83, Estoril, Portugal.
[20] UNISIG SUBSET 088, ETCS Application Levels 1 & 2 — Safety Analysis, Version 2.3.0, http://www.era.europa. eu/Document-Register/ Pages/ UNISIGSUBSET-088.aspx
[21] G. Weidl, A. L. Madsen and S. Israelson, "Applications of object-oriented Bayesian networks for condition monitoring root cause analysis and decision support on operation of complex continuous processes", Computers and Chemical Engineering, vol. 29, no. 9, **(2005)**, pp. 1996-2009.

[22] 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, vol. 71, no. 3, **(2001)**, pp. 249-260.
[23] A. Bobbio, L. Portinale, M. Minichino and E. Ciancamerla, "Comparing fault trees and Bayesian networks for dependability analysis", Proceedings of the 18th International Conference on Computer Safety, reliability and Security, **(1999)**, pp. 310-322, Toulouse, France.
[24] W. M. Goble, "Control systems safety evaluation and reliability", Research Triangle Park, New York, **(1998)**.

Authors

Hongsheng Su obtained his Master in Traffic Information Engineering and Control, Lanzhou Jiaotong University in 2001. He acquired his PhD in Power Systems and Its Automation, Southwest Jiaotong University. Now he is serving as a full-time professor at school of Automation and Electrical Engineering, Lanzhou Jiaotong University. His research interest includes System Security and Reliability, Intelligent Control, Power Systems and Its Automation, and etc.

Yulong Che

He was born in Gansu, China, in 1988. He received his B. S. degree in Electrical Engineering and Automation from Shijiazhuang Tiedao University in 2011. Currently, he is a Master candidate in Power Electronics and Power Drives in Lanzhou Jiaotong University, China. His recent research interest is reliability and safety analysis of Chinese train control system of level 3 system.