Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Availability evaluation of controller area networks under the influence of intermittent connection faults*

Longkai WANG[1], Leiming ZHANG[2], Yong LEI[‡1]

[1]*State Key Laboratory of Fluid Power and Mechatronic Systems, Zhejiang University, Hangzhou 310027, China*

[2]*The 14th Research Institute of China Electronics Technology Group Corporation, Nanjing 210039, China*

E-mail: lkwang@zju.edu.cn; smezlm2010@126.com; ylei@zju.edu.cn

Received Nov. 24, 2022; Revision accepted Aug. 6, 2023; Crosschecked Feb. 29, 2024

Abstract: Controller area networks (CANs), as one of the widely used fieldbuses in the industry, have been extended to the automation field with strict standards for safety and reliability. In practice, factors such as fatigue and insulation wear of the cables can cause intermittent connection (IC) faults to occur frequently in the CAN, which will affect the dynamic behavior and the safety of the system. Hence, quantitatively evaluating the performance of the CAN under the influence of IC faults is crucial to real-time health monitoring of the system. In this paper, a novel methodology is proposed for real-time quantitative evaluation of CAN availability when considering IC faults, with the system availability parameter being calculated based on the network state transition model. First, the causal relationship between IC fault and network error response is constructed, based on which the IC fault arrival rate is estimated. Second, the states of the network considering IC faults are analyzed, and the deterministic and stochastic Petri net (DSPN) model is applied to describe the transition relationship of the states. Then, the parameters of the DSPN model are determined and the availability of the system is calculated based on the probability distribution and physical meaning of markings in the DSPN model. A testbed is constructed and case studies are conducted to verify the proposed methodology under various experimental setups. Experimental results show that the estimation results obtained using the proposed method agree well with the actual values.

Key words: Controller area network; Intermittent connection fault; Arrival rate; Deterministic and stochastic Petri net; Availability evaluation

https://doi.org/10.1631/FITEE.2200592 **CLC number:** TP277

1 Introduction

The controller area network (CAN), as a fieldbus that effectively supports distributed and real-time control, is highly flexible and reliable with low cost. It has therefore been extended to fields with strict standards for safety performance and network reliability, such as aviation systems, agricultural machinery, medical instruments, and industrial automation control. As the communication carrier of critical data in these systems, CAN bus can significantly affect system efficiency and even operational safety due to network faults.

In practice, electromagnetic interference (EMI), component aging, and improper maintenance can cause short-time failures of the system and result in intermittent system faults. Intermittent faults are repetitive faults with random occurrence time and duration, which disappear automatically with the recovery of components or equipment functions without external intervention (Syed et al., 2013). As the deterioration of system performance increases, the frequency and severity of intermittent faults will also increase until intermittent faults develop into

‡ Corresponding author

* Project supported by the National Natural Science Foundation of China (No. 52072341)

ORCID: Longkai WANG, https://orcid.org/0000-0003-0865-0836; Yong LEI, https://orcid.org/0000-0003-0235-5203

permanent faults and system functions are damaged or lost. An intermittent connection (IC) fault is a cable connection type of intermittent fault that occurs frequently in CANs at the cable-to-cable or component-to-cable connectors and is hard to troubleshoot. The factors causing IC faults include fatigue fracture, insulation wear, aging loosening, and mechanical movement of cables and their connectors. IC problems often increase the transmission error counter (TEC) value embedded in a node because of the interruption in data transmission, and even turn the node to bus-off state when the value reaches 256 (Bosch, 1991). Although this error confinement mechanism indirectly reflects the degradation of network performance to some extent, the error counters are usually not accessible in practice. However, node disengagement from the production system bus usually leads to system-level shutdown for inspection and maintenance, which not only seriously reduces the production efficiency of the system, but also naturally increases the downtime cost. Therefore, to monitor the health status of the system in real time, improve the responsiveness of the system, and provide quantitative information for predictive maintenance of the system, the research of quantitatively evaluating the impact of IC faults on the availability of the CAN is of great importance.

The performance measurements of CANs under various scenarios have been studied in the literature. Mary et al. (2013) reviewed the reliability analysis methods of CAN-based automotive systems, which include reliability modeling with a deterministic error model, a fault-tolerant communication model, and a probabilistic error model. Herpel et al. (2009) proposed a deterministic evaluation method based on network calculus to determine the worst-case transmission times and the delay bounds of messages on all priority levels in the CAN. Zago and de Freitas (2018) presented a quantitative performance study regarding CAN, CAN with flexible data-rate (CAN FD) 8 B, and CAN FD 16 B from various perspectives including object pool transference, bus load usage, and message response time. Gujarati and Brandenburg (2015) proposed a method to derive the time rate failures of CAN-based distributed real-time systems, in which the probability of a correct and timely message transmission was analyzed considering the host and network failures. Hansson et al. (2002) calculated the probabilities of a communication failure considering intermittent interference sources and transient interference sources for distributed real-time systems. Sun et al. (2015) analyzed the message response time delay distribution for CANs that operate in polling communication mode. Wang et al. (2010) designed a CAN model with improved reliability based on a redundancy fault-tolerant technology that integrates the advantages of the hardware and analytical fault-tolerant redundancy technologies. Pohren et al. (2020) analyzed the performance of the CAN FD protocol using the electrical fast transient injection method. Dos Santos Roque et al. (2022) developed a runtime fault diagnostic mechanism to monitor performance degradation in the in-vehicle network using an early fault modeling approach. The above approaches investigate the performance evaluation of CANs under permanent faults as well as intermittent faults such as EMI and electrical fast transients (EFTs). However, they are not suitable for analyzing the impact of cable intermittent connection problems on CAN performance.

The literature related to the bus-off hitting time of nodes in CANs is extensive. Navet et al. (2000) and Navet and Song (2001) established an error model following a generalized Poisson process, computed the worst-case deadline failure probability for a CAN-based application, and modeled the evolution of TEC by a discrete-time Markov chain (DTMC) to calculate the bus-off time. On this basis, Chen et al. (2006) calculated the average bus-off hitting time of a CAN node. Gaujal and Navet (2005) modeled the TEC with a continuous-time Markov chain, and analyzed the bus-off and error-passive hitting time of the nodes in a CAN. Lei et al. (2010) established a DTMC to model the error confinement principle of a TEC, to predict the bus-off time of a node. However, all the above research is based on the difficult bit error rate (BER) measurement on the CAN bus and the premise that the current TEC value is zero, which limits the application of these methods in practice. Zhang et al. (2017b) described the stochastic characteristics of the errors and assessed the reliability of the nodes based on the renewal theory in the CAN. Zhang et al. (2015, 2017a) estimated the node TEC value based on segmented Markov chains, and predicted the time to reach the bus-off state of the nodes on the basis of the information of observable nodes. However, the above method had significant errors in the accuracy and precision of the prediction results in long-term monitoring situations. This method also did not consider the issue that observable node information interferes with bus message sending and occupies the bus bandwidth while being sent to the master controller.

As can be seen from the literature, although the research on CAN performance measurement and estimation established a statistical relationship between IC faults and system states, little analysis has been devoted to the degradation or deterioration of network availability as IC fault characteristics change with time in real industrial environments. The IC problem is distinct from general faults in the following two aspects: first, the IC phenomenon occurs randomly and disjointedly in the network with a momentary actuation duration, and cannot be repeated during the system offline diagnostics; second, it evolves dynamically (that is, its severity and frequency of occurrence grow with time). To the knowledge of the authors, few scholars designed Petri net to model the CAN states based on IC faults. Hence, existing performance measurement approaches for the CAN cannot handle a scenario in which IC faults with dynamic deterioration characteristics in real industrial environments occur in the network. Additionally, existing methods of calculating the bus-off hitting time cannot quantify the availability level of the whole CAN in real time, and suffer from poor long-range accuracy. Therefore, how to develop a real-time assessment method for CAN systems to evaluate the degree of IC fault effects on network availability, based on the IC fault characteristic parameters and the changes in network operation status, is essential.

In this paper, a novel availability evaluation methodology for the CAN is proposed which uses the IC fault arrival rate as a key parameter to derive network usability. The advantages of the proposed method are as follows:

1. An approach for real-time estimation of the IC fault arrival rate based on the error information in the data link layer is developed.

2. A novel deterministic and stochastic Petri net (DSPN) model for the communication states of the CAN under IC faults is constructed.

3. An online availability evaluation methodology for the CAN is developed.

The results of this work will help in understanding the relationship between system states and performance, and facilitate real-time production control and decision-making, which will ultimately improve the overall efficiency of the system and provide guidance for the design of the bus load and the message sending strategy.

2 Problem definition

In this work, network availability refers to the ability to successfully send messages, which is defined as the ratio of the available time that the bus can send messages successfully to the total system operation time. Using the error frame information collected from the data link layer to precisely evaluate CAN availability under the influence of IC faults in real time is a challenging problem, due to the inaccessibility of TEC values in nodes and the uncertainty of IC faults. Therefore, we divide the CAN availability assessment task with IC faults into the following issues to solve one by one:

1. How can a bridge between IC faults and the collected error records be built, and how can a model for estimating the arrival rate of IC faults be established?

2. How can the CAN states be illustrated when IC faults occur, and how can an appropriate model be established to describe the transfer conditions and relationship of each state?

3. How can a model be developed to predict the network availability level based on the probability distribution of network states derived from the state transition model?

Two assumptions are made: (1) the network configuration adopts the communication mode of master–slave polling and the bus-type topology commonly used in manufacturing systems, and (2) the interference is limited to the intermittent open-circuit fault.

3 Evaluation method

In this study, a novel DSPN model based system availability evaluation methodology for the CAN is proposed which uses the IC fault arrival rate as an important model parameter. The principal idea of this method is that establishing a discrete event model to describe the system state transition relationship under IC faults will allow the system availability, which characterizes the ability of a network to transmit messages normally, to be calculated based on the probability distribution of each state.

The overall procedure of the method is shown in Fig. 1. First, the relationship between the error frame (EF) and IC fault is established, and the IC fault arrival rate is estimated on the basis of the error information collected from the data link layer. Second, the CAN states and their transition relationship when synthesizing bus messages and IC faults are analyzed and defined. Third, the DSPN model is constructed to describe the state transition relationship, and the model parameters are determined based on the IC fault arrival rate, the messages sent on the bus, and the CAN protocol. Finally, the system availability is calculated based on the probability distribution of the markings in the DSPN model. Details of the proposed method are introduced in the following subsections.

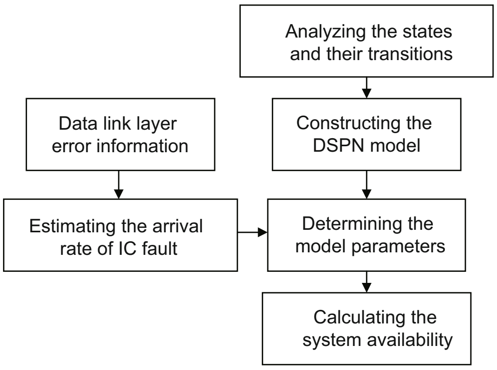
Analyzing the states and their transitions
Data link layer error information
Constructing the DSPN model
Estimating the arrival rate of IC fault
Determining the model parameters
Calculating the system availability

Fig. 1 Framework of the evaluation procedure

3.1 Estimating the IC fault arrival rate

Let $C(t)$ denote the total number of EFs on the bus in a time interval of t. Then the stochastic process $C(t)$ $(t \geq 0)$ is a compound process, and can be represented as

$$C(t) = \sum_{i=1}^{A(t)} L_i,\ t \geq 0, \tag{1}$$

where $\{A(t), t \geq 0\}$ is the IC fault arrival process, and the IC fault arrival events are independent of each other. L_i denotes the number of EFs caused by the i^{th} IC fault arrival event. The IC fault arrivals depend on the logic value transmitted on the bus, and the arrival of an IC fault can cause an EF on the bus only when the bus transmits the dominant bit. Thus, $\{L_i, i \geq 1\}$ is a family of independent and identically distributed random variables whose value is 0 or 1.

3.1.1 Distribution of L_i

Assuming that the message sequence transmitted in one cycle T_{cycle} on the bus is $\boldsymbol{U} = [U_1, U_2, \cdots, U_Q]$, then the distribution of L_i can be obtained as follows:

$$\begin{cases} \Pr\{L_i = 1\} = \sum_{q=1}^{Q} \frac{t_{U_q}}{T_{\text{cycle}}} \xi(U_q), \\ \Pr\{L_i = 0\} = 1 - \Pr\{L_i = 1\}, \end{cases} \tag{2}$$

where t_{U_q} is the transmitting time of message U_q, $t_{U_q} = B_{U_q} \tau_{\text{bit}}$, B_{U_q} is the number of bits in U_q, and τ_{bit} is the bit time. $\xi(U_q)$ denotes the probability that the IC fault arrival event can result in an EF during the transmission of U_q.

The standard message according to the CAN specification is shown in Fig. 2, which consists of the following seven fields: the start of frame (SOF) marks the beginning of the message, the arbitration field defines the message priority and resolves the bus access conflict of multiple messages, the control field indicates the number of bytes in the data field, the data field contains up to eight bytes of data, the cyclic redundancy check (CRC) field checks the transmission error, the acknowledge (ACK) field demonstrates the consistency between the messages received and transmitted, and the end of frame (EOF) delimits the message. The interframe space separates the messages from each other (Bosch, 1991).

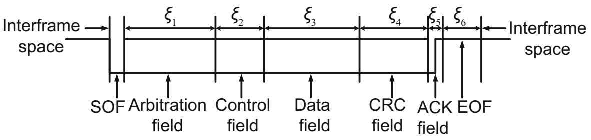

Fig. 2 Partition of the standard message

Based on the message format and the error handling mechanism, message U_q can be divided into six segments, as shown in Fig. 2, and $\xi_j(U_q)$ in the j^{th} segment denotes the probability that an IC fault arrival event will cause an EF when the j^{th} segment of U_q is being transmitted (Sun et al., 2015; Zhang et al., 2019):

$$\xi_j(U_q) = \frac{B_j^{(\text{D})}}{B_j} + \sum_{k \in \mathbb{B}(k,j)} \frac{B_k^{(\text{D})}}{B_k}, \tag{3}$$
$$j, k \in \{1, 2, \cdots, 6\},\ k < j,$$

where B_j represents the number of bits in the j^{th} segment, $B_j^{(\text{D})}$ represents the number of dominant bits in the j^{th} segment, and the set $\mathbb{B}(k,j)$ represents the scenario in which the EF caused by an IC fault occurring in the k^{th} segment is sent in the j^{th} segment. Then $\xi(U_q)$ can be calculated based on Eq. (3):

$$\xi(U_q)=\sum_{j=1}^{6}\frac{B_j}{B_{U_q}}\xi_j(U_q). \tag{4}$$

Moreover, based on the distribution of L_i in Eq. (2), the expectation and variance of L_i are obtained:

$$\begin{cases}E[L_i]=\Pr\{L_i=1\},\\ \operatorname{Var}(L_i)=\Pr\{L_i=1\}\left(1-\Pr\{L_i=1\}\right).\end{cases} \tag{5}$$

3.1.2 Expectation and variance of $C(t)$

The expectation of $C(t)$ is

$$\begin{aligned}E[C(t)]&=E\left[\sum_{i=1}^{A(t)}L_i\right]=E\left[E\left[\sum_{i=1}^{A(t)}L_i\middle|A(t)\right]\right]\\&=E[A(t)E[L_i]]=E[A(t)]E[L_i].\end{aligned} \tag{6}$$

The variance of $C(t)$ is

$$\begin{aligned}&\operatorname{Var}(C(t))\\&=E[(C(t))^2]-(E[C(t)])^2\\&=\left\{E\left[E[(C(t))^2|A(t)]\right]-E\left[(E[C(t)|A(t)])^2\right]\right\}\\&\quad+\left\{E\left[(E[C(t)|A(t)])^2\right]-(E[E[C(t)|A(t)]])^2\right\}\\&=E\left[\operatorname{Var}(C(t)|A(t))\right]+\operatorname{Var}(E\left[C(t)|A(t)\right])\\&=E\left[A(t)\operatorname{Var}(L_i)\right]+\operatorname{Var}(A(t)E\left[L_i\right])\\&=E[A(t)]\operatorname{Var}(L_i)+\operatorname{Var}(A(t))(E[L_i])^2.\end{aligned} \tag{7}$$

3.1.3 Estimation of the IC fault arrival rate

The IC fault arrival rate $\lambda_{A(t)}$ can be estimated based on Eqs. (6) and (7), and is shown in Eq. (8):

$$\begin{aligned}\hat{\lambda}_{A(t)}\in\frac{1}{T_\text{e}}\Big[&E[A(T_\text{e})]-\sqrt{\operatorname{Var}(A(T_\text{e}))},\\&E[A(T_\text{e})]+\sqrt{\operatorname{Var}(A(T_\text{e}))}\Big],\end{aligned} \tag{8}$$

where T_e is the time interval of measuring the EFs on the bus. $E[A(T_\text{e})]$ and $\operatorname{Var}(A(T_\text{e}))$ can be calculated as

$$E[A(T_\text{e})]=\frac{E[C(T_\text{e})]}{E[L_i]}, \tag{9}$$

$$\operatorname{Var}(A(T_\text{e}))=\frac{\operatorname{Var}(C(T_\text{e}))E[L_i]-E[C(T_\text{e})]\operatorname{Var}(L_i)}{(E[L_i])^3}. \tag{10}$$

3.2 Analyzing the CAN states when IC faults occur

The state of a CAN bus changes according to the arrival of an IC fault and the logic value transmitted on the bus, and all the states are demonstrated below.

State 1: normal state. The normal state indicates that the bus is error-free and transmits the message correctly.

State 2: IC active state. The IC active state indicates that the bus is transmitting the dominant bit when an IC fault occurs. In this case, the IC fault will destroy this dominant bit and cause an EF ultimately.

State 3: IC inactive state. The IC inactive state indicates that the bus is transmitting the recessive bit when an IC fault occurs. In this case, the IC fault has no effect on the bus.

State 4: IC compound state. The IC compound state can be reached in two scenarios: (1) Because there is always a stochastic time interval between sending the EF and an IC fault disrupting a dominant bit, the bus can make a transition into the IC compound state from the IC active state if the bus is transmitting the recessive bit when the next IC fault event arrives; (2) The bus can make a transition into the IC compound state from the IC inactive state if the bus is transmitting the dominant bit when the next IC fault event arrives.

State 5: sending EF without IC. In the state of sending EF without IC, the bus is sending the EF without the IC fault arrival event.

State 6: sending EF with active IC. In the state of sending EF with active IC, the IC fault event arrives when the bus is sending a dominant bit of the EF.

State 7: sending EF with inactive IC. In the state of sending EF with inactive IC, the IC fault event arrives when the bus is sending a recessive bit of the EF.

The transition relationship among the above states is shown in Fig. 3. The bus can make a transition into the IC active state (IC inactive state) from the normal state if the IC fault event occurs when the bus is transmitting the dominant bit (the recessive

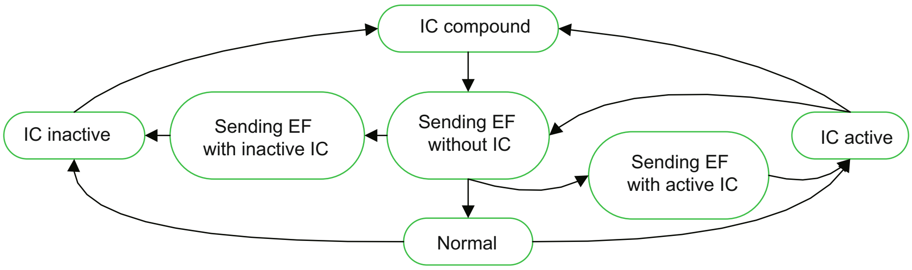

Fig. 3 Transition relationship among the controller area network states (EF: error frame; IC: intermittent connection)

bit). The bus can make a transition into the IC compound state from the IC inactive state if the next IC fault arrival event disrupts a dominant bit transmitted on the bus. In the IC active state, if the EF is sent before the next IC fault event that acts on a recessive bit transmitted on the bus arrives, then the bus will make a transition into the state of sending EF without IC. Otherwise, the bus will make a transition into the IC compound state.

In the IC compound state, since the dominant bit has been disrupted, the bus will ultimately make a transition into the state of sending EF without IC. In the state of sending EF without IC, if there is no IC fault event arriving during the EF sending process, then the bus will handle the error normally according to the CAN specification and make a transition into the normal state. If the IC fault event arrives and disrupts a dominant bit of the EF sent on the bus, then the bus will make a transition into the state of sending EF with active IC, in which the EF format is destroyed. In this case, the process of sending the EF is interrupted and the bus makes a transition into the IC active state. If the IC fault event arrives and acts on a recessive bit of the EF sent on the bus, then the bus will make a transition into the state of sending EF with inactive IC. In this case, the bus will make a transition into the IC inactive state after finishing the EF sending process.

3.3 Modeling the CAN state transition

According to the analysis above, the transition among the states is triggered by discrete events, such as the IC fault arrival event and the error handling process. There are either fixed or stochastic durations of these events, and thus the DSPN model can be applied to describe the transition relationship among the states.

A DSPN model can be represented by $(P, T; F, W, M_0, \lambda^{\mathrm{E}}, \tau^{\mathrm{D}})$, where $P = \{P_0, P_1, \cdots, P_m\}$ is the set of places, $T = T_{\mathrm{i}} \cup T_{\mathrm{e}} \cup T_{\mathrm{d}} = \{t_0, t_1, \cdots, t_n\}$ is the set of transitions, $T_{\mathrm{i}} = \{t_0, t_2, \cdots, t_k\}$ is the set of immediate transitions with zero firing time (i.e., the delay between enabling and firing of t), $T_{\mathrm{e}} = \{t_{k+1}, t_{k+2}, \cdots, t_l\}$ is the set of exponential transitions with exponentially distributed firing time, $T_{\mathrm{d}} = \{t_{l+1}, t_{l+2}, \cdots, t_n\}$ is the set of deterministic transitions with deterministic firing time (Choi et al., 1993), $F \subseteq (P \times T) \cup (T \times P)$ is the set of arcs, $W : F \to \{1, 2, 3, \cdots\}$ is the weight function, $M_0 : P \to \{0, 1, 2, \cdots\}$ is the initial marking, $\lambda^{\mathrm{E}} = \{\lambda_{k+1}, \lambda_{k+2}, \cdots, \lambda_l\}$ is the set of firing rates of exponential transitions, and $\tau^{\mathrm{D}} = \{\tau_{l+1}, \tau_{l+2}, \cdots, \tau_n\}$ is the set of delays of deterministic transitions. The state of a Petri net is defined by the number of tokens in places, and can be denoted as a vector $\boldsymbol{M} = [M(P_0), M(P_1), \cdots, M(P_n)]$, i.e., the marking of the Petri net, where $M(P_i)$ is the number of tokens in P_i. $\forall t \in T$, if $P_i \in {}^{\bullet}t$ and $M(P_i) \geq W(P_i, t)$, where ${}^{\bullet}t$ is the pre-set of t, then t is enabled, which can be denoted as $M[t >$. The firing of the enabled transition t will change the allocation of the tokens in the places and create a new marking M', which can be denoted as $M[t > M'$, and $\forall P_i \in P, M'(P_i) = M(P_i) - W(P_i, t) + W(t, P_i)$. If a transition sequence $t_1, t_2, \cdots, t_k$ satisfies the condition $M[t_1 > M_1[t_2 > \cdots > M_{k-1}[t_k > M_k$, then marking $\boldsymbol{M}_k$ is reachable from $\boldsymbol{M}$. The reachability graph can be established by connecting all the markings reachable from $\boldsymbol{M}$ with the directed arcs (Murata, 1989).

The established DSPN model of the CAN bus when considering IC faults is shown in Fig. 4, where $P = \{P_0, P_1, P_2, P_3, P_4, P_5\}$, $T = T_{\mathrm{e}} \cup T_{\mathrm{d}}$, $T_{\mathrm{e}} = \{t_0, t_1, t_2, t_3\}$, and $T_{\mathrm{d}} = \{t_4, t_5, t_6\}$. F includes both the conditional arcs and the inhibitor arcs, and the arc weights are 1. Initially, P_0 and P_5 are each marked with one token, and thus the initial marking is $\boldsymbol{M}_0 = [100001]$. The physical meaning of the places and transitions is shown in Table 1.

The reachability set of the DSPN model is $\{\boldsymbol{M}_0, \boldsymbol{M}_1, \boldsymbol{M}_2, \boldsymbol{M}_3, \boldsymbol{M}_4, \boldsymbol{M}_5, \boldsymbol{M}_6\}$, which is shown in Table 2, and the corresponding reachability graph is shown in Fig. 5. Obviously, the transition relationship of the markings in the reachability graph is consistent with that of the network states shown in Fig. 3, and hence the established DSPN model can correctly describe the transition relationship among the CAN states.

3.4 Calculating DSPN model parameters

Transitions t_0, t_1, t_2, and t_3 have exponentially distributed firing rates, which are r_0, r_1, r_2, and r_3, respectively. Transitions t_4, t_5, and t_6 have deterministic firing delays, which are τ_4, τ_5, and τ_6, respectively.

3.4.1 Calculating r_0 and r_1

Parameters r_0 and r_1 depend on the message sequence transmitted on the bus and the IC fault arrival rate, and can be calculated as

$$r_0 = \Pr\{L_i = 1\}\hat{\lambda}_{A(t)}, \tag{11}$$

$$r_1 = \Pr\{L_i = 0\}\hat{\lambda}_{A(t)}. \tag{12}$$

3.4.2 Calculating r_2 and r_3

Parameter r_2 depends on the IC fault arrival rate and the probability that an IC fault arrives with

Table 2 Reachable markings and their meaning in the DSPN model

$\boldsymbol{M}$	P_0	P_1	P_2	P_3	P_4	P_5	Meaning
$\boldsymbol{M}_0$	1	0	0	0	0	1	State 1
$\boldsymbol{M}_1$	0	1	0	0	0	1	State 2
$\boldsymbol{M}_2$	0	0	1	0	0	1	State 3
$\boldsymbol{M}_3$	0	0	0	1	0	1	State 4
$\boldsymbol{M}_4$	1	0	0	0	1	0	State 5
$\boldsymbol{M}_5$	0	1	0	0	1	0	State 6
$\boldsymbol{M}_6$	0	0	1	0	1	0	State 7

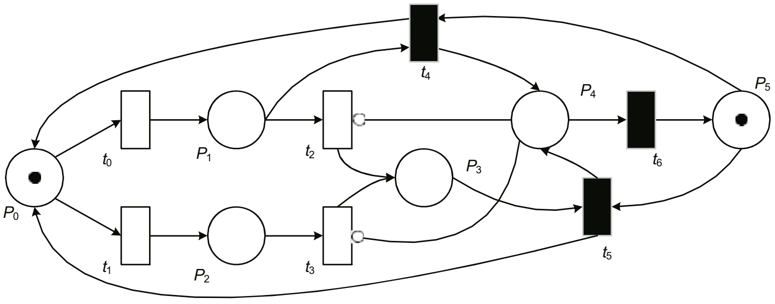

Fig. 4 DSPN model of the CAN bus when considering IC faults

Table 1 Physical meaning of the places and transitions in the DSPN model

Place	Physical meaning
P_0	Normal state
P_1	IC active state
P_2	IC inactive state
P_3	IC compound state
P_4	Initialization of error handling
P_5	Error detection mechanism
Transition	**Physical meaning**
t_0	The IC fault event arrives at a dominant bit
t_1	The IC fault event arrives at a recessive bit
t_2	The bus is transferred from the IC active state to the IC compound state
t_3	The bus is transferred from the IC inactive state to the IC compound state
t_4	The IC active state causes an error interruption
t_5	The IC compound state causes an error interruption
t_6	An EF is sent

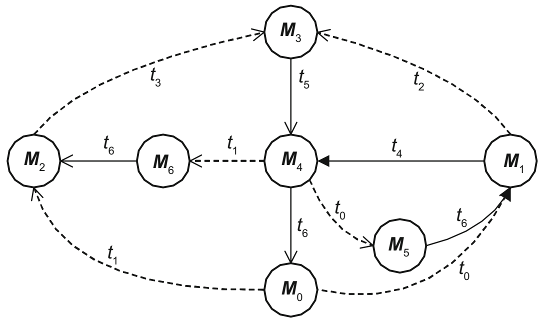

Fig. 5 Reachability graph of the DSPN model
The dashed arcs represent the firing of exponential transitions, and the solid arcs represent the firing of deterministic transitions

the bus sending the dominant bit and the next IC fault arrives with the bus sending the recessive bit:

$$r_2 = \hat{\lambda}_{A(t)} \frac{\sum\limits_{i=1}^{T_{\text{cycle}}/\tau_{\text{bit}}} \delta_i^{r_2}}{T_{\text{cycle}}/\tau_{\text{bit}} - 1}. \tag{13}$$

$\delta_i^{r_2}$ is subject to

$$\delta_i^{r_2} = \begin{cases} 1, \ \text{BL}[i] = 0 \wedge \text{BL}\left[i + \frac{1}{\hat{\lambda}_{A(t)}\tau_{\text{bit}}}\right] = 1, \\ 0, \ \text{otherwise}, \end{cases} \tag{14}$$

where 0 and 1 denote the dominant bit and the recessive bit transmitted on the bus, respectively. $\text{BL}[i]$ and $\text{BL}\left[i + \frac{1}{\hat{\lambda}_{A(t)}\tau_{\text{bit}}}\right]$ denote the i^{th} and $\left(i + \frac{1}{\hat{\lambda}_{A(t)}\tau_{\text{bit}}}\right)^{\text{th}}$ logic values transmitted on the bus, respectively.

Similarly, r_3 depends on the IC fault arrival rate and the probability that an IC fault arrives with the bus sending the recessive bit and the next IC fault arrives with the bus sending the dominant bit:

$$r_3 = \hat{\lambda}_{A(t)} \frac{\sum\limits_{i=1}^{T_{\text{cycle}}/\tau_{\text{bit}}} \delta_i^{r_3}}{T_{\text{cycle}}/\tau_{\text{bit}} - 1}. \tag{15}$$

$\delta_i^{r_3}$ is subject to

$$\delta_i^{r_3} = \begin{cases} 1, \quad \text{BL}[i] = 1 \wedge \text{BL}\left[i + \frac{1}{\hat{\lambda}_{A(t)}\tau_{\text{bit}}}\right] = 0, \\ 0, \quad \text{otherwise}. \end{cases} \tag{16}$$

3.4.3 Calculating τ_4 and τ_5

Parameters τ_4 and τ_5 denote the time interval between the time when a dominant bit is disrupted by an IC fault and the time when the EF starts to be sent. There are five types of error that can be detected in the CAN: bit error, stuff error, CRC error, form error, and ACK error. Any node detecting a bit error, a stuff error, a form error, or an ACK error flags this error by transmitting an EF at the next bit, and transmits an EF at the bit following the ACK delimiter when detecting a CRC error. Thus, τ_4 and τ_5 depend on the position of the disrupted dominant bit and the number of bits of the message, and can be calculated as

$$\tau_4 = \tau_5 = \frac{\sum_{q=1}^{Q} B_{U_q}}{2Q} \tau_{\text{bit}}. \tag{17}$$

3.4.4 Calculating τ_6

Parameter τ_6 denotes the time interval between the start time of sending an EF and the time of bus recovery. According to the CAN standard, $\tau_6 = 20\tau_{\text{bit}}$ (Bosch, 1991).

3.5 Evaluating CAN availability

The marking process $\{D(t), t \geq 0\}$ of the DSPN model is a Markov regenerative process (Choi et al., 1993, 1994), and its state space is $\Omega = \{\boldsymbol{M}_0, \boldsymbol{M}_1, \boldsymbol{M}_2, \boldsymbol{M}_3, \boldsymbol{M}_4, \boldsymbol{M}_5, \boldsymbol{M}_6\}$. $\forall i \in \Omega$, let $\varepsilon(i)$ denote the set of exponential transitions and $\psi(i)$ denote the set of deterministic transitions enabled in marking i. There are two different cases according to the cardinal number of $\psi(i)$, which are as follows:

1. $\psi(i) = \varnothing$. Then the rate of leaving marking i is $\Lambda_i = \sum_{j\in\Omega} \lambda(i,j)$, where $\lambda(i,j)$ is the transition rate from marking i to j.

2. $\psi(i) = \{t_{\text{d}}\}$. Then the generator matrix $\boldsymbol{Q}(i)$ of the subordinated continuous-time Markov chain can be formed as follows: $\forall j \in \Omega(i)$, the rate from j to $k \in \Omega$ is $\lambda(j,k)$, and the rate of leaving j is zero if $j \notin \Omega(i)$, where $\Omega(i)$ is the set of all states reached from i.

Let $\Omega_\varepsilon(i)$ denote the set of states reachable from i by firing a competitive exponential transition, and $\Omega_\psi(i)$ denote the set of states reachable from i by firing the deterministic transition t_{d}. Moreover, the branching-probability matrix can be defined as $\boldsymbol{B} = [B(j,k)], j \in \Omega(i), k \notin \Omega(i)$, and $B(j,k) = \Pr\{\text{next marking is } k | \text{current marking is } j \ \& \ t_{\text{d}} \text{ fires}\}$.

The behavior of the marking process between two transition epochs of $\{D(t), t \geq 0\}$ can be described by $\boldsymbol{E}(t)$, where $\boldsymbol{E}(t) = [E_{ij}(t)]$ $(i, j \in \Omega)$, which is calculated as follows:

1. If $\psi(i)=\varnothing$, then $E_{ij}(t)=\delta_{ij}\mathrm{e}^{-\varLambda_i t}$, where

$$\delta_{ij}=\begin{cases}1, & \text{if } i=j,\\ 0, & \text{otherwise.}\end{cases} \tag{18}$$

2. If $\psi(i)=\{t_\mathrm{d}\}$, and the delay time of t_d is τ, then for $j\in\varOmega(i)$, we have

$$E_{ij}(t)=\begin{cases}[\mathrm{e}^{\boldsymbol{Q}(i)t}]_{ij}, & t<\tau,\\ 0, & t\geq\tau,\end{cases} \tag{19}$$

and for $j\notin\varOmega(i)$, $E_{ij}(t)=0$.

The steady-state probability $\boldsymbol{V}=[V_i]$ $(i\in\varOmega)$ of the embedded Markov chain for $\{D(t),t\geq 0\}$ can be obtained by

$$\begin{cases}\boldsymbol{V}=\boldsymbol{V}\boldsymbol{T},\\ \sum_{i\in\varOmega}V_i=1,\end{cases} \tag{20}$$

where $\boldsymbol{T}=[T_{ij}]$ $(i,j\in\varOmega)$ is the one-step transition probability matrix, and can be calculated as follows:

1. If $\psi(i)=\varnothing$, then

$$T_{ij}=\begin{cases}0, & \varLambda_i=0,\\ \frac{\lambda(i,j)}{\varLambda_i}, & \varLambda_i>0.\end{cases} \tag{21}$$

2. If $\psi(i)=\{t_\mathrm{d}\}$, and the delay time of t_d is τ, then if $j\in\varOmega_\varepsilon(i)$ and $j\notin\varOmega_\psi(i)$, $T_{ij}=[\mathrm{e}^{\boldsymbol{Q}(i)\tau}]_{ij}$; if $j\notin\varOmega_\varepsilon(i)$ and $j\in\varOmega_\psi(i)$, $T_{ij}=\sum_{k\in\varOmega(i)}[\mathrm{e}^{\boldsymbol{Q}(i)\tau}]_{ik}B(k,j)$; if $j\in\varOmega_\varepsilon(i)$ and $j\in\varOmega_\psi(i)$, $T_{ij}=[\mathrm{e}^{\boldsymbol{Q}(i)\tau}]_{ij}+\sum_{k\in\varOmega(i)}[\mathrm{e}^{\boldsymbol{Q}(i)\tau}]_{ik}B(k,j)$; if $j\notin\varOmega_\varepsilon(i)$ and $j\notin\varOmega_\psi(i)$, $T_{ij}(t)=0$.

The limiting probability distribution $\boldsymbol{P}=[P_j]$ $(j\in\varOmega)$ of $\{D(t),t\geq 0\}$ is given by

$$P_j=\sum_{i\in\varOmega}\beta_i\frac{\alpha_{ij}}{\mu_i}, \tag{22}$$

where $\alpha_{ij}=\int_0^\infty E_{ij}(t)\mathrm{d}t$, $\beta_i=\frac{V_i\mu_i}{\sum_{k\in\varOmega}V_k\mu_k}$, and

$$\mu_i=\begin{cases}\frac{1}{\varLambda_i}, & \psi(i)=\varnothing,\\ \sum_{j\in\varOmega(i)}\int_0^\tau[\mathrm{e}^{\boldsymbol{Q}(i)t}]_{ij}\mathrm{d}t, & \psi(i)=\{t_\mathrm{d}\}.\end{cases} \tag{23}$$

During system operations, the bus can send the message successfully only when it is in the normal state or the IC inactive state. Thus, based on the real-time estimation of the IC fault arrival rate and the solution of the DSPN model, the availability of the system when considering IC faults can be defined as

$$\mathcal{A}=P_{\boldsymbol{M}_0}+P_{\boldsymbol{M}_2}, \tag{24}$$

where $P_{\boldsymbol{M}_0}$ and $P_{\boldsymbol{M}_2}$ denote the probabilities of the DSPN model being in the markings $\boldsymbol{M}_0$ and $\boldsymbol{M}_2$, respectively.

4 Case studies

In this section, the method proposed in this study is illustrated in detail and its effectiveness is verified. First, the testbed is set up, and then the method of estimating the IC fault arrival rate is demonstrated. Finally, the method of evaluating CAN availability is verified under different cases.

4.1 Testbed setup

The schematic layout of the testbed is shown in Fig. 6, which contains three parts: the CAN communication system, the IC fault injection implementation, and the CAN analyzer. Moreover, the constructed testbed is shown in Fig. 7.

The CAN communication system is constructed using DeviceNet devices and contains five nodes, which are the node PLC and nodes N_6–N_9. The PLC is developed using the AB CompactLogix 1769-L35E controller module and the 1769-SDN DeviceNet scanner module. The communication mode of the system is set to polling with a cycle time of 10 ms, and its communication rate is 500 Kb/s. Thus, $\tau_\text{bit}=2$ μs. A high-speed analog switch is added on the drop line of node N_8, and the IC fault is emulated by randomly and transiently disconnecting the switch. The arrivals of IC faults are controlled by the host program running on the computer and the NI Compact-RIO embedded device. The Kvaser Leaf Professional HS CAN analyzer is used to record the identifier, the data field, the transmitting time of the messages, and the EFs on the bus.

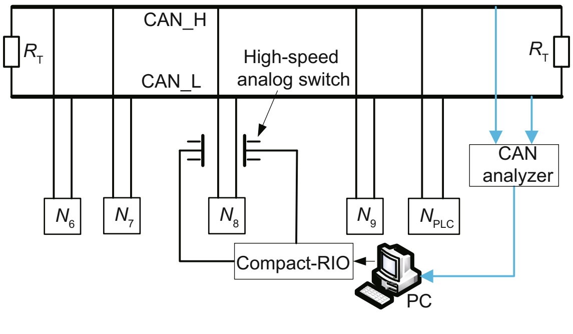

Fig. 6 Schematic layout of the testbed

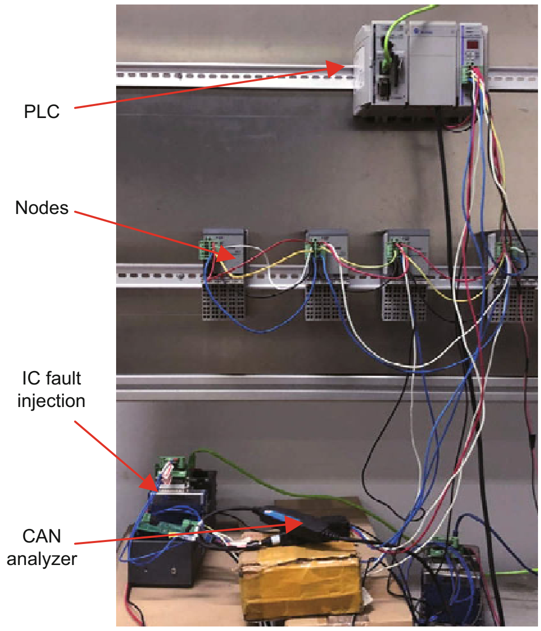

Fig. 7 Experimental testbed for case studies

4.2 Verifying the calculation of $C(t)$

There are eight messages on the CAN bus shown in Fig. 6, and $\xi(U_q)$ of these messages can be calculated based on logical bits of the messages, as shown in Table 3, where U_1 is the remote message sent from the PLC to N_6, U_2 is the remote message sent from the PLC to N_7, U_3 is the message sent from N_6, U_4 is the remote message sent from the PLC to N_8, U_5 is the message sent from N_7, U_6 is the remote message sent from the PLC to N_9, U_7 is the message sent from N_8, and U_8 is the message sent from N_9.

When $A(t)$ is a homogeneous Poisson process, $E[A(t)] = \mathrm{Var}(A(t)) = \lambda_{A(t)}t$, $E[C(t)] = \lambda_{A(t)}t\Pr\{L_i = 1\}$, and $\mathrm{Var}(C(t)) = \lambda_{A(t)}t\Pr\{L_i = 1\}$. Based on these equations, the expectation and variance of $C(t)$ can be estimated with a given $\lambda_{A(t)}$. Fig. 8 shows the results under the condition of $\lambda_{A(t)} = 1000$ faults/s, where the actual value of $C(t)$ is obtained based on the data collected by the CAN analyzer, and the upper and lower bounds of the error bars are the positive and negative standard deviations of the estimated value of $C(t)$, respectively.

Table 3 Number of bits and $\xi(U_q)$ of messages

U_q	B_{U_q}	$\xi(U_q)$	U_q	B_{U_q}	$\xi(U_q)$
U_1	46	0.090	U_5	64	0.139
U_2	45	0.093	U_6	45	0.082
U_3	64	0.120	U_7	65	0.121
U_4	45	0.087	U_8	65	0.162

It shows that the estimated values of $C(t)$ agree well with the actual values, which verifies the effectiveness of the method of calculating the number of EFs on the bus.

4.3 Estimating the arrival rate of IC fault

After verifying the effectiveness of the EF counting process model, the IC fault arrival rate can be estimated based on this model and the actual value of $C(t)$ recorded by the CAN analyzer. Two fault cases are set up: the first case is that $A(t)$ is a homogeneous Poisson process with $\lambda_{A(t)} = 500$ faults/s; the second case is that $A(t)$ is a nonhomogeneous Poisson process, whose arrival rate is $\lambda_{A(t)} = 500$ faults/s initially and changes to $\lambda_{A(t)} = 1000$ faults/s at a random time point in the process of system operation. The actual value of $C(t)$ obtained by the CAN analyzer is shown in Fig. 9.

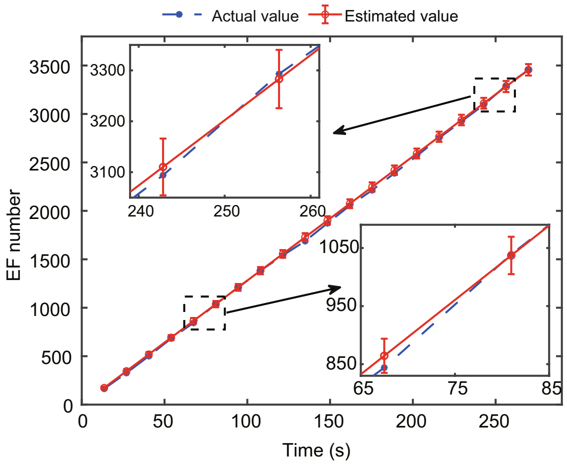

Fig. 8 Comparison between the estimated and actual values of $C(t)$ when $\lambda_{A(t)} = 1000$ faults/s

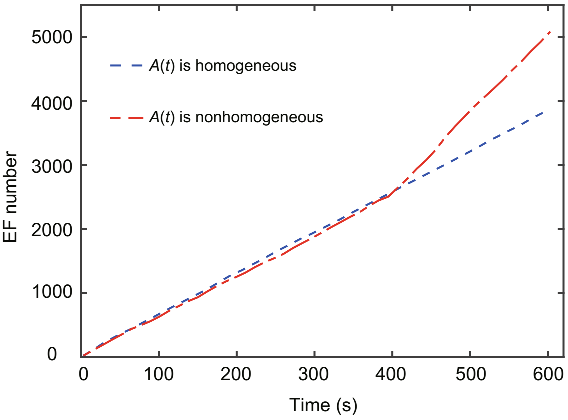

Fig. 9 Actual value of $C(t)$ for estimating the IC fault arrival rate

When $A(t)$ is a homogeneous Poisson process, based on the actual value of $C(t)$ in a different time interval T_{e}, the estimation intervals of the IC fault arrival rate $\hat{\lambda}_{A(t)}$ can be calculated by Eq. (8). As shown in Table 4, the actual IC fault arrival rate is always within the estimation intervals of $\hat{\lambda}_{A(t)}$ under various values of T_{e}, and the variance of the interval decreases with an increase of T_{e}. Moreover, the mean values of different estimation intervals corresponding to different values of T_{e} agree well with the actual IC fault arrival rate. In the following analysis, T_{e} is set to 100 s based on the tradeoff between the estimation variance and computational complexity.

When $A(t)$ is a nonhomogeneous Poisson process, the IC fault arrival rate is estimated by using a sliding time window with both window time and sliding time of 100 s. As shown in Fig. 10, the mean values of estimation intervals corresponding to different arrival rate settings agree well with the actual rates. Based on the above analysis, the method of estimating the IC fault arrival rate is verified under both the homogeneous and nonhomogeneous IC fault arrival processes.

Table 4 $\hat{\lambda}_{A(t)}$ corresponding to different T_{e}'s

T_{e} (s)	$\hat{\lambda}_{A(t)}$ interval (fault/s)
20	[430.2, 580.3]
40	[454.2, 555.2]
60	[462.0, 545.9]
80	[466.3, 541.8]
100	[473.6, 534.0]

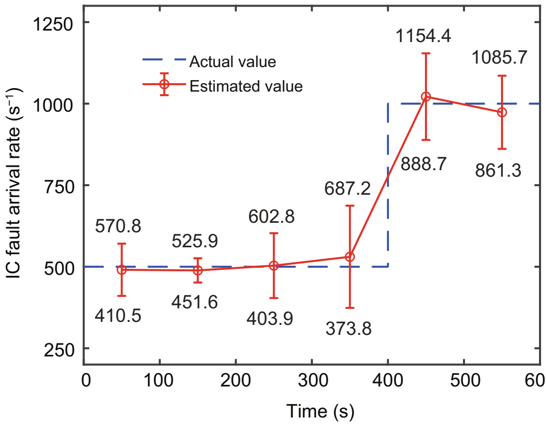

Fig. 10 Comparison between the estimated and actual values of $\lambda_{A(t)}$

4.4 Calculating the availability of the CAN network

4.4.1 CAN network with five nodes

Based on the estimation of the IC fault arrival rate and the logical bit in a polling cycle, the DSPN model parameters under different $\lambda_{A(t)}$'s can be calculated and are shown in Table 5, where for the estimation of the IC fault arrival rate under conditions of $\lambda_{A(t)} = 500$ faults/s and $\lambda_{A(t)} = 1000$ faults/s, the results of time windows (100, 200) and (500, 600) are used in Fig. 10, respectively.

The availability of system $\mathcal{A}$ can be estimated after solving the DSPN model, and the actual values of $\mathcal{A}$ at different times can be obtained based on the CAN analyzer recorded transmitting time of messages and EFs. The comparison between the estimated and actual values of $\mathcal{A}$ when $\lambda_{A(t)}$=1000 faults/s is shown in Fig. 11.

As shown in Fig. 11, the actual value of $\mathcal{A}$ fluctuates over time, which is caused by transient faults and environmental disturbances during the practical operation. The estimated value of $\mathcal{A}$ is 0.9967 and the mean actual value of $\mathcal{A}$ is 0.9945, so the error between the estimated value and the actual value is 0.22%.

Following the procedures above, the comparison between the estimated and actual values of $\mathcal{A}$ when $\lambda_{A(t)} = 500$ faults/s is shown in Fig. 12. The estimated value of $\mathcal{A}$ is 0.9982 and the mean actual value of $\mathcal{A}$ is 0.9971, so the error between the estimated value and the actual value is 0.11%.

4.4.2 CAN network with nine nodes

As the number of nodes in a CAN increases, the contention and interaction between messages sent on the bus during a polling cycle are more frequent, which will affect the network availability. To address this issue, in this subsection, the number of nodes in the CAN is increased to nine on the basis of the network shown in Fig. 6.

The DSPN model parameters under different $\lambda_{A(t)}$ can be calculated and are shown in Table 5. The comparison between the estimated and actual values of $\mathcal{A}$ when $\lambda_{A(t)} = 1000$ faults/s is shown in Fig. 13. The estimated value of $\mathcal{A}$ is 0.9949 and the mean actual value of $\mathcal{A}$ is 0.9904, so the error between the estimated and actual values is 0.45%.

The comparison between the estimated and actual values of $\mathcal{A}$ when $\lambda_{A(t)}$ = 500 faults/s is shown in Fig. 14. The estimated value of $\mathcal{A}$ is 0.9974 and the mean actual value of $\mathcal{A}$ is 0.9951, so the error between the estimated value and the actual value is 0.23%.

4.4.3 Analyzing the experimental results

The summary and comparison of the above case studies are shown in Table 6 and Fig. 15, where A represents the five-node network with $\lambda_{A(t)}$= 1000 faults/s, B represents the nine-node network with $\lambda_{A(t)}$ = 1000 faults/s, C represents the five-node network with $\lambda_{A(t)}$ = 500 faults/s, and D represents the nine-node network with $\lambda_{A(t)}$= 500 faults/s.

As shown in Table 6, the estimated availability values agree well with the actual values under different network setups and IC fault arrival rates, and the errors between the estimated value and the actual value are within 0.5%. Thus, the effectiveness of the method that conducts the availability evaluation of the CAN based on the DSPN model is verified. Moreover, in each experimental setup, the

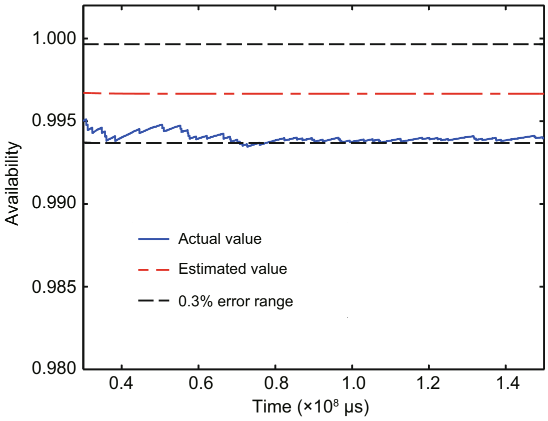

Fig. 11 Comparing the estimated and actual values of $\mathcal{A}$ in a five-node network when $\lambda_{A(t)}$ = 1000 faults/s

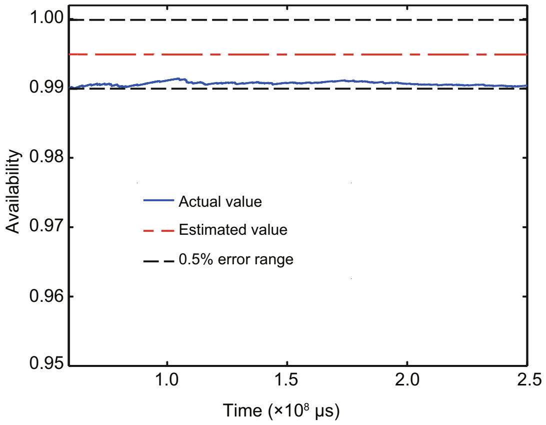

Fig. 13 Comparing the estimated and actual values of $\mathcal{A}$ in a nine-node network when $\lambda_{A(t)}$ = 1000 faults/s

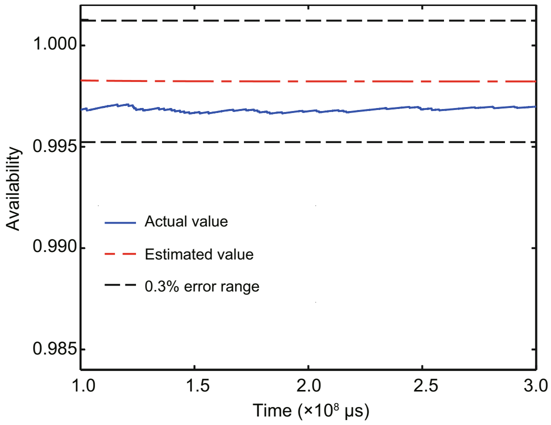

Fig. 12 Comparing the estimated and actual values of $\mathcal{A}$ in a five-node network when $\lambda_{A(t)}$ = 500 faults/s

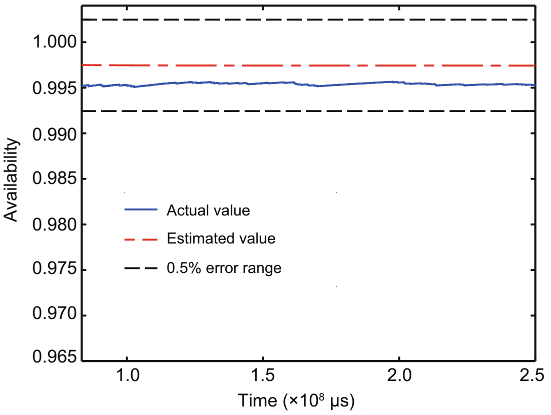

Fig. 14 Comparing the estimated and actual values of $\mathcal{A}$ in a nine-node network when $\lambda_{A(t)}$ = 500 faults/s

Table 5 DSPN model parameters of four case studies

Network load	$\lambda_{A(t)}$ (fault/s)	r_0 (s^{-1})	r_1 (s^{-1})	r_2 (s^{-1})	r_3 (s^{-1})	τ_4 (μs)	τ_5 (μs)	τ_6 (μs)
Five nodes	1000	7.28	992.72	36.08	36.08	54.875	54.875	40
	500	3.52	496.48	19.27	19.27	54.875	54.875	40
Nine nodes	1000	16.75	983.25	55.40	55.40	55.000	55.000	40
	500	7.97	492.03	28.05	28.05	55.000	55.000	40

Table 6 Summary of the four case studies

Network load	Estimated $\mathcal{A}$		Actual $\mathcal{A}$		Error (%)	
	$\lambda_{A(t)}$ = 1000 faults/s	500 faults/s	1000 faults/s	500 faults/s	1000 faults/s	500 faults/s
Five nodes	0.9967	0.9982	0.9945	0.9971	0.22	0.11
Nine nodes	0.9949	0.9974	0.9904	0.9951	0.45	0.23

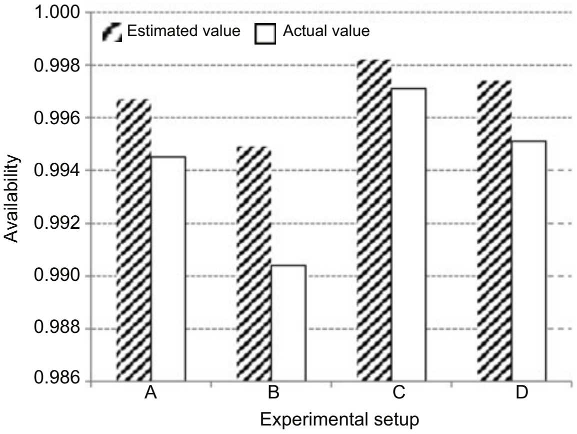

Fig. 15 Comparison of the four case studies

estimated availability value is greater than the actual value within the allowable error range. This is due to the underestimation of the IC fault arrival rate, which is caused by the scenario where multiple IC faults cause only one EF. Under the same network load, the error in the estimated availability increases as the IC fault arrival rate increases. This is because the higher the IC fault arrival rate, the greater the possibility that multiple IC faults will cause only one EF, and thus the greater the estimation errors in the number of EFs and the IC fault arrival rate, the greater the error in network availability.

By comparing cases A with C, and cases B with D in Fig. 15, we can conclude that the availability of the CAN decreases as the IC fault arrival rate increases under the same network load. By comparing cases A with B, and cases C with D in Fig. 15, we can conclude that the availability of the CAN decreases as the network load increases under the same IC fault arrival rate. These two comparisons indicate that, on one hand, the larger the network load, the larger the ratio of message transmitting time to cycle, and the more frequently IC faults affecting the bus message transmission process, which results in more severe deterioration of network availability. On the other hand, the higher the IC fault injection rate, the greater the possibility of IC faults on the bus within unit time, and thus the greater the possibility of destroying the normal transmission of bus messages, the lower the network availability level.

5 Conclusions

In this paper, we propose a DSPN model based methodology for real-time high-accuracy estimation of CAN availability under the influence of IC faults using the estimated IC fault arrival rate without occupying the bus load. First, the IC fault arrival rate is estimated based on a stochastic model for counting the number of EFs under IC faults. Then, the transition relationship among the states of the CAN network when considering IC faults is described using a DSPN model, and the model parameters are calculated based on the IC fault arrival rate. Finally, the probability distributions of the system states are obtained by solving the Markov regenerative process, based on which the availability of the system is defined and calculated. The testbed is constructed and case studies with different network loads and fault configurations are analyzed. Experimental results show that the IC fault arrival rates estimated by the proposed approach agree well with the actual values in both time-invariant and time-varying IC fault arrival rates. The results also show that the network availabilities calculated by the proposed method match the actual values under various network loads and IC fault arrival rates within a 0.5% estimation error, which demonstrates the effectiveness of the proposed evaluation methodology. Future work will include applying the methodology proposed in this paper to the CAN with a complex topology and evaluating the system performance when considering other kinds of faults.

Contributors

All the authors designed the research. Longkai WANG and Leiming ZHANG processed the data. Leiming ZHANG drafted the paper. Yong LEI and Longkai WANG helped organize the paper. Longkai WANG revised and finalized the paper.

Conflict of interest

All the authors declare that they have no conflict of interest.

Data availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

Bosch R, 1991. CAN Specification Version 2.0. Technical Report. Robert Bousch GmbH, Postfach, Gerlingen, Germany.

Chen JX, Luo F, Sun ZC, 2006. Reliability analysis of CAN nodes under electromagnetic interference. IEEE Int Conf on Vehicular Electronics and Safety, p.367-371. https://doi.org/10.1109/ICVES.2006.371617

Choi H, Kulkarni VG, Trivedi KS, 1993. Transient analysis of deterministic and stochastic Petri nets. Proc 14th Int Conf on Application and Theory of Petri Nets, p.166-185. https://doi.org/10.1007/3-540-56863-8_46

Choi H, Kulkarni VG, Trivedi KS, 1994. Markov regenerative stochastic Petri nets. *Perform Eval*, 20(1-3):337-357. https://doi.org/10.1016/0166-5316(94)90021-3

Dos Santos Roque A, Jazdi N, De Freitas EP, et al., 2022. A fault modeling based runtime diagnostic mechanism for vehicular distributed control systems. *IEEE Trans Intell Transp Syst*, 23(7):7220-7232. https://doi.org/10.1109/TITS.2021.3067552

Gaujal B, Navet N, 2005. Fault confinement mechanisms on CAN: analysis and improvements. *IEEE Trans Veh Technol*, 54(3):1103-1113. https://doi.org/10.1109/TVT.2005.844652

Gujarati A, Brandenburg BB, 2015. When is CAN the weakest link? A bound on failures-in-time in CAN-based real-time systems. IEEE Real-Time Systems Symp, p.249-260. https://doi.org/10.1109/RTSS.2015.31

Hansson HA, Nolte T, Norstrom C, et al., 2002. Integrating reliability and timing analysis of CAN-based systems. *IEEE Trans Ind Electron*, 49(6):1240-1250. https://doi.org/10.1109/TIE.2002.804970

Herpel T, Hielscher KS, Klehmet U, et al., 2009. Stochastic and deterministic performance evaluation of automotive CAN communication. *Comput Netw*, 53(8):1171-1185. https://doi.org/10.1016/j.comnet.2009.02.008

Lei Y, Djurdjanovic D, Ni J, 2010. DeviceNet reliability assessment using physical and data link layer parameters. *Qual Reliab Eng Int*, 26(7):703-715. https://doi.org/10.1002/qre.1131

Mary GI, Alex ZC, Jenkins L, 2013. Reliability analysis of controller area network based systems—a review. *Int J Commun Netw Syst Sci*, 6(4):155-166. https://doi.org/10.4236/ijcns.2013.64019

Murata T, 1989. Petri nets: properties, analysis and applications. *Proc IEEE*, 77(4):541-580. https://doi.org/10.1109/5.24143

Navet N, Song YQ, 2001. Validation of in-vehicle real-time applications. *Comput Ind*, 46(2):107-122. https://doi.org/10.1016/S0166-3615(01)00123-3

Navet N, Song YQ, Simonot F, 2000. Worst-case deadline failure probability in real-time applications distributed over controller area network. *J Syst Archit*, 46(7):607-617. https://doi.org/10.1016/S1383-7621(99)00016-8

Pohren DH, dos Santos Roque A, Kranz TAI, et al., 2020. An analysis of the impact of transient faults on the performance of the CAN-FD protocol. *IEEE Trans Ind Electron*, 67(3):2440-2449. https://doi.org/10.1109/TIE.2019.2901639

Sun YC, Yang F, Lei Y, 2015. Message response time distribution analysis for controller area network containing errors. Chinese Automation Congress, p.1052-1057. https://doi.org/10.1109/CAC.2015.7382654

Syed WA, Khan S, Phillips P, et al., 2013. Intermittent fault finding strategies. *Proc CIRP*, 11:74-79. https://doi.org/10.1016/j.procir.2013.07.062

Wang ZY, Guo XS, Yu CQ, 2010. Research of fault-tolerant redundancy and fault diagnosis technology based on CAN. 2nd Int Conf on Advanced Computer Control, p.287-291. https://doi.org/10.1109/ICACC.2010.5487002

Zago GM, de Freitas EP, 2018. A quantitative performance study on CAN and CAN FD vehicular networks. *IEEE Trans Ind Electron*, 65(5):4413-4422. https://doi.org/10.1109/TIE.2017.2762638

Zhang LM, Tang LH, Yang F, et al., 2015. CAN node reliability assessment using segmented discrete time Markov chains. IEEE Int Conf on Automation Science and Engineering, p.231-236. https://doi.org/10.1109/CoASE.2015.7294067

Zhang LM, Tang LH, Lei Y, 2017a. Controller area network node reliability assessment based on observable node information. *Front Inform Technol Electron Eng*, 18(5):615-626. https://doi.org/10.1631/FITEE.1601029

Zhang LM, Yuan Y, Lei Y, 2017b. Data driven CAN node reliability assessment for manufacturing system. *Chin J Mech Eng*, 30(1):190-199. https://doi.org/10.3901/CJME.2016.1021.124

Zhang LM, Sun YC, Lei Y, 2019. Message delay time distribution analysis for controller area network under errors. *Front Inform Technol Electron Eng*, 20(6):760-772. https://doi.org/10.1631/FITEE.1700815