Hindawi
Security and Communication Networks
Volume 2021, Article ID 5536722, 12 pages
https://doi.org/10.1155/2021/5536722

Research Article

Towards a Statistical Model Checking Method for Safety-Critical Cyber-Physical System Verification

Jian Xie,[1,2,3] **Wenan Tan**,[1,2,3] **Bingwu Fang**,[2,4] **and Zhiqiu Huang**[1,2,3]

[1]*College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China*
[2]*Key Laboratory of Safety-Critical Software, Nanjing University of Aeronautics and Astronautics, Nanjing, China*
[3]*Collaborative Innovation Center of Novel Software Technology and Industrialization, Nanjing, China*
[4]*College of Information Engineering, Anhui Finance and Trade Vocational College, Hefei, China*

Correspondence should be addressed to Bingwu Fang; bingwufang@163.com

Received 10 February 2021; Revised 2 April 2021; Accepted 16 April 2021; Published 18 May 2021

Academic Editor: Weizhi Meng

Safety-Critical Cyber-Physical System (SCCPS) refers to the system that if the system fails or its key functions fail, it will cause casualties, property damage, environmental damage, and other catastrophic consequences. Therefore, it is vital to verify the safety of safety critical systems. In the community, the SCCPS safety verification mainly relies on the statistical model checking methodology, but for SCCPS with extremely high safety requirements, the statistical model checking method is difficult/infeasible to sample the extremely small probability event since the probability of the system violating the safety is very low (rare property). In response to this problem, we propose a new method of statistical model checking for high-safety SCCPS. Firstly, with the CTMC-approximated SCCPS path probability space model, it leverages the maximum likelihood estimation method to learn the parameters of CTMC. Then, the embedded DTMC can be derived from CTMC, and a cross-entropy optimization model based on DTMC can be constructed. Finally, we propose an algorithm of iteratively learning the optimal importance sampling distribution on the discrete path space and an algorithm to check the statistical model of verifying the rare attribute. Eventually, experimental results show that the method proposed in this paper can effectively verify the rare attributes of SCCPS. Under the same sample size, comparing with the heuristic importance sampling methods, the estimated value of this method can be better distributed around the mean value, and the related standard deviation and relative error are reduced by more than an order of magnitude.

1. Introduction

Safety-Critical Cyber-Physical System (SCCPS) is characterized with high safety and high reliability and are widely used in fields closely related to the national economy and people's livelihoods, such as aerospace, nuclear industry, public transportation, finance, and medical care. Once the execution of such system fails, it will deeply threaten the safety of human's life and property [1–3]. Therefore, it is vital to analyze and verify the safety and reliability of safety-critical systems, and it is of great significance to the design and development of safety-critical systems. Indeed, it has attracted wide attention from researchers and has extensively grown as a prominent research topic in the community [4–7].

Essentially, SCCPS is a kind of complex cyber-physical fusion system [8–10]. For this kind of systems, the continuously changing behavior in their physical layer is intertwined with the discrete changing behavior in their decision control layer. Their state spaces are infinite as well. It increases the difficulty and brings severe challenges to the safety analysis and verification of SCCPS. However, the traditional model checking has the problem of state space explosion, and it is difficult to effectively verify it [11].

With the execution path of the sampling system, Statistical Model Checking (SMC) uses statistical analysis techniques to approximate the probability that the target system meets the sequential logic attributes and can provide arbitrarily small error limits [12–14]. Because SMC does not need to analyze the complex logic inside the target system to verify the timing logic properties of the system, it can effectively avoid the complexity of the system and the explosion of the state space [15, 16]. Therefore, SMC is the

most effective solution to verify the timing properties of complex SCCPS [12, 17–19]. However, for SCCPS requiring extremely high safety, the probability of occurrence of the negative events of its safety attributes and the probability of system failures are extremely low. It is infeasible for SMC to sample extremely low probability events. Thus, how to use SMC to verify the extremely secure SCCPS is an urgent problem to be solved [20, 21].

To date, verification of the SMC rare attributes mainly relies on the importance sampling method. For CTMC and DTMC random models, Reijsbergen et al. [22] and Barbot et al. [23] utilized the heuristic methods to obtain an importance sampling distribution to complete the attribute verification of the two models, respectively. Clarke and Zuliani [24] proposed the cross-entropy minimization importance sampling-based SMC method to verify the safety properties of the Stateflow/Simulink model system. Zuliani et al. [17] used the SMC method in his study [24] to verify the secure attribute of the discrete-time SHS. The methods proposed by Clarke and Zuliani assume that the distribution of the system path space is an exponential distribution. By simply increasing the failure rate of the system parameters, several paths that satisfy the rare attributes are extracted at one time to calculate the optimal parameters for the exponential distribution to obtain an importance sampling distribution [25]. J´egourel et al. [26] leveraged the cross-entropy minimum optimization method in the random model of a random guardian command system, which can approximate the path distribution of the system by increasing the number of commands (number of parameters), to obtain an importance sampling distribution in the random model. However, the optimal importance sampling distribution obtained with the aforementioned methods is not from the distribution family of the system path space, but essentially is a heuristic importance sampling method. Thus, the verification results are only rough approximation.

In this paper, we propose a method with the SCCPS path space to construct a cross-entropy optimization model and use an iterative learning method to obtain an optimal importance sampling distribution from the parameterized distribution cluster of the path space. It can ensure that the optimal importance sampling distribution is from the spatial distribution family in the SCCPS path, and the iterative learning method can ensure that the distribution evenly covers the unsafe path distribution area. As evaluated in our experiments, the accuracy and efficiency of the rare attribute verification are significantly improved.

2. Background

2.1. Statistical Model Checking. Statistical Model Checking (SMC) can be simply described as follows: given a system model M and system properties φ described by the bounded linear temporal logic (BLTL) [18], it uses the Monte Carlo sampling, model checking, and statistical analysis techniques to qualitatively/quantitatively verify the following two questions:

(i) The probability that M satisfies the attribute φ: $\Pr(M \vDash \pi)$

(ii) Whether the probability of M satisfying the attribute φ is higher than or equal to the threshold θ: $M \vDash \Pr(\geq \theta)$ (φ)

In SMC, it first simulates the execution of the system model M to extract a random execution path ω. Then, the BLTL model detector is used to determine whether ω satisfies the attribute φ, and a certain number of samples will be generated after multiple simulations. It further leverages the statistical method to perform statistical analysis on the samples to assess the probability of the system model M satisfying the attribute φ, as well as give the confidence interval or the estimated error margin. Let $I(\omega)$ represent the output result of the BLTL model detector. If $\omega \vDash \pi$, $I(\omega) = 1$; otherwise, it is 0. $I(\omega)$ is a Bernoulli random variable, so the behavior of M can be modeled by the Bernoulli distribution with a parameter p:

$$\begin{cases} \Pr(I(\omega) = 1) = p, \\ \Pr(I(\omega) = 0) = 1 - p. \end{cases} \tag{1}$$

The parameter p represents the probability that the model M satisfies the BLTL attribute φ. With the Bernoulli distribution, we note that $p = E[I(\omega)]$, $\mathrm{var}[I(\omega)] = p \times (12212p)$. Since the value of p is unknown, the goal of SMC is to estimate the value of p.

SMC can be divided into two categories: hypothesis testing and parameter estimation. The hypothesis testing is used to determine whether the probability of the system satisfying the temporal logic attribute is greater than or equal to a given threshold, which is a qualitative result, while the parameter estimation is a quantitative result to represent the approximate probability of the system satisfying the temporal logic attribute. SMC qualitative algorithms include the single sampling plan (SSP) algorithm [27], the sequential probability ratio test (SPRT) algorithm [27], and the Bayesian hypothesis test (BHT) algorithm [18]. SMC quantitative algorithms mainly include the approximate probabilistic model checking (APMC) [28] algorithm and the Bayesian interval estimation testing (BIET) algorithm [18]. Kim et al. [29] conducted an empirical evaluation on the performance and applicability of the four algorithms (i.e., SSP, SPRT, BHT, and BIET).

2.2. Safety Requirement Specification. In this paper, we use Bounded Linear Temporal Logic (BTCL) as our specification language. BLTL restricts Linear Temporal Logic (LTL) with time bounds on the temporal operators. Formally, the syntax of BLTL is given as

$$\varphi ::= x \sim v \mid (\varphi\_1) \vee \varphi\_2 \mid (\varphi\_1 \wedge \varphi\_2) \mid \varphi\_1 \varphi\_1 \cup^{t} \varphi\_2, \tag{2}$$

where $\sim \in \{\leq, \geq, =\}$, $x \in SV$ (the finite set of state variables), $v \in \mathbb{R}$, $t \in \mathbb{R}_{\geq 0}$, and $\vee$, $\wedge$, and are the usual Boolean connectives. The formulas $x \sim v$ is called the atomic propositions (AP). The formula $\varphi\{\_1\} \cup^{t} \varphi\{\_2\}$ will return true if and only if $\varphi\{\_2\}$ is true and $\varphi\{\_1\}$ will hold within the time t. The

operators $\Diamond_t$ and $\Box_t$ can be defined as follows by using the $\cup t$ operator: $\Diamond t\varphi = \text{True} \cup t\varphi$, which required φ to hold true within time t (true). $\Box t\varphi = \neg\Diamond t\neg\varphi$ requires φ to hold true up to time t.

The semantics of BLTL formulas [28, 30, 31] is defined with respect to system traces (or executions). A trace is a sequence $\sigma = (s_0, t_0), (s_1, t_1), \ldots$, where s_i is the state of the system at the represented time t_i. The pair (s_i, t_i) expresses the fact that the system moved to state s_{i+1} after having spent t_i time units in state s_i. If the trace σ satisfies the property φ, we write $\sigma \vDash \varphi$. The trace suffix of σ starting at $k \in \mathbb{N}$ is denoted by σ^k, and σ^0 denotes the full trace σ.

The semantics of BLTL for a trace σ^k is defined as follows:

(i) $\sigma^k \vDash x \sim v$, iff $x \sim v$ holds true in state s_k

(ii) $\sigma^k \vDash \varphi_1 \wedge \varphi_2$, iff $\sigma^k \vDash \varphi_1$ and $\sigma^k \vDash \varphi_2$

(iii) $\sigma^k \vDash \varphi_1 \vee \varphi_2$, iff $\sigma^k \vDash \varphi_1$ or $\sigma^k \vDash \varphi_2$

(iv) $\sigma^k \vDash \varphi_1$, iff $\sigma^k \vDash \varphi_1$ does not hold ($\sigma^k \nvDash \varphi_1$)

(v) $\sigma^k \vDash \varphi\_1 \cup^t \varphi\{\_2\}$, iff $\exists i \in \mathbb{N}$ such that (a) $\sum_{l=0}^{i-1} t_{k+1} < t$ and (b) $\sigma^{k+i} \vDash \varphi_2$, as well as (c) $\forall 0 \le j < i$, $\sigma^{k+j} \vDash \varphi_1$

The sampling bound: $\#(\varphi) \in\in Q \ge 0$ of a BLTL formula φ is the maximum nested sum of time bounds

(vii) $\#(x \sim v) := 0$

(viii) $\#(\varphi_1) := \#(\varphi)$

(ix) $\#(\varphi_1 \vee \varphi_2) := \max(\#(\varphi_1), \#(\varphi_2))$

(x) $\#(\varphi_1 \wedge \varphi_2) := \max(\#(\varphi_1), \#(\varphi_2))$

(xi) $\#(\varphi_1 \cup^t \varphi_2) := t + \max(\#(\varphi_1), \#(\varphi_2))$

Lemma 1 (Bounded sampling). *The problem "$\sigma \vDash \varphi$" is well-defined and can be checked for BLTL formulas φ and traces σ based on only a finite prefix of σ of bounded duration.*

Proof. According to Lemma 1, the decision "$\sigma \vDash \varphi$" is uniquely determined (and well-defined) by considering only a prefix of σ of duration $\#(\varphi) \in\in Q \ge 0$. By divergence of time, σ reaches or exceeds this duration $\#(\varphi)$ in some finite number of steps n. Let σ^0 denote a finite prefix of σ of length n, such that $\sum_{0 \le l < n} tl \ge \#(\varphi)$. Again by Lemma 3, the semantics of $\sigma^0 \vDash \varphi$ is well-defined because any extension σ" of σ' satisfies σ"$\vDash\varphi$ if and only if $\sigma' \vDash \varphi$. Consequently, the semantics of $\sigma' \vDash \varphi$ coincides with the semantics of $\sigma \vDash \varphi$. On the finite trace σ^0, it is easy to see that BLTL is decidable by evaluating the atomic formulas $x \sim v$ at each state s_i of the system simulation. □

Lemma 2 (BLTL on bounded simulation traces). *Let φ be a BLTL formula, $k \in N$. Then, for any two infinite traces, $\sigma = (s_0, t_0), (s_1, t_1), \ldots$ and $\overline{\sigma} = (\overline{s}_0, \overline{t}_0), (\overline{s}_1, \overline{t}_1), \ldots$ with $s_{k+I} = \overline{s}_{k+I}$ and $t_{k+I} = \overline{t}_{k+I}$ $\forall I \in N$ with $\sum_{t_{k+I}} \le \#(\phi)$ [17]. We have that $\sigma_k \vDash \varphi$ if $\overline{\sigma_k} \vDash \varphi$.*

Proof. IH is short for induction hypothesis.

(1) If φ is of the form $x \sim v$, $\sigma_k \vDash \varphi$ if $\overline{\sigma_k} \vDash \varphi$ since $s_{k+I} = \overline{s}_{k+I}$ and $t_{k+I} = \overline{t}_{k+I}$ by using [17] for $i = 0$.

(2) If φ is of the form $\varphi_1 \vee \varphi_2$,

$$\sigma_k \vDash \varphi_1 \vee \varphi_2 \begin{cases} \text{iff } \sigma_k \vDash \varphi_1 \text{ or } \sigma_k \vDash \varphi_2, \\ \text{iff } \overline{\sigma}_k \vDash \varphi_1 \text{ or } \overline{\sigma}_k \vDash \varphi_2, \\ \text{iff } \overline{\sigma}_k \vDash \varphi_1 \vee \varphi_2, \end{cases} \tag{3}$$

by induction hypothesis as $\#(\varphi_1 \vee \varphi_2) \ge \#(\varphi_1)$ and $\#(\varphi_1 \vee \varphi_2) \ge \#(\varphi_2)$. The proof is similar to φ_1 and $\varphi_1 \cap \varphi_2$.

(3) If φ is of the form $\varphi_1 \cup^t \varphi_2$, $\sigma_k \vDash \varphi_1 \cup^t \varphi_2$ if the following three conditions are satisfied:

(a'). $\sum_{0 \le l < i} t_{k+l}^{\sim} \le t$ because $\#(\varphi_1 \cup^t \varphi_2) \ge t$ such that the durations of trace σ and $\overline{\sigma}$ are $t_{k+l} = t_{k+l}^{\sim}$ for each index l with $0 \le l < i$ by the assumption [17].

(b'). $\overline{\sigma}_{k+i} \vDash \varphi_2$ by induction hypothesis as follows: we know that the traces σ and $\overline{\sigma}$ match at k for duration $\#(\varphi_1 \cup^t \varphi_2)$ and need to show that the semantics of $\varphi_1 \cup^t \varphi_2$ matches at k. By IH, we know that φ_2 has the same semantics at $k + i$ (that is, $k + i \vDash \varphi_2$ if $k + i \vDash \varphi_2$) provided that we can show that the traces σ and $\overline{\sigma}$ match at $k + i$ for duration $\#(\varphi_2)$. For this case, it considers any $I \in N$ with $\sum_{0 \le l < I} t_{k+i+l} \le \#(\varphi_2)$. Then, $\#(\varphi_2) \ge \sum_{0 \le l < I} t_{k+i+l} = \sum_{0 \le l <} It_{k+l} - \sum_{0 \le l < I} t_{k+l} \ge \sum_{0 \le l < i+l} t_{k+l} - t$. Thus, $\sum_{0 \le l < i+I} t_{k+l} \le t + \#(\varphi_2) \le t + \max(\#(\varphi_1), \#(\varphi_2)) = \#(\varphi_1 \cup^t \varphi_2)$. As $I \in N$ was arbitrary, we conclude from this with assumption [17] that, indeed $s_I = s_I^{\sim}$ and $t_I = t_I^{\sim}$ for all $I \in N$ with $\sum_{0 \le l < I} t_{k+i+l} \le \#(\varphi_2)$. Thus, the IH for φ_2 yields the equivalence of $\sigma_{k+i} \vDash \varphi_2$ and $\overline{\sigma}_{k+i} \vDash \varphi_2$ when using the equivalence of (a) and (a').

(c'). For each $0 \le j < i$, $\sigma_{k+i} \vDash \varphi_1$. The proof of equivalence to (c) is similar to that for (b') using $j < i$. The existence of an $i \in N$ for which these conditions (a'), (b'), and (c') hold is equivalent to $k \vDash \varphi_1 \cup^t \varphi_2$. □

2.3. Safety Critical System Model. Safety-Critical Systems (SCCPS) [32] are defined as a tuple, SCCPS = (L, X, E, Inv, D, G, R), where

(i) L is a finite set of discrete states (control mode);

(ii) $X \subseteq \mathbb{R}^n$ is a finite set of continuous variables;

(iii) $E \subset L \times L$ is a collection of discrete changes;

(iv) Inv: $L \longrightarrow 2^X$ represents the mapping from the discrete state set L to the continuous state space. For $\forall l \in L$, Inv (l) is the invariant-position set of l;

(v) D: $L \longrightarrow (X \longrightarrow X)$ is a mapping of a vector domain, which assigns a set of Stochastic Differential Equations (SDE) to each control mode $l \in L$ to describe the continuous random dynamic behavior with respect to the different control modes l, $d_x(t) = f(l, x(t))d_t + g(l, x(t))d_{B_t}$. B_t is a

standard Wiener process defined in the real number field. It assumes that $\forall l \in L$, $f(l,\cdot)$, and $g(l,\cdot)$ are bounded and Lipschitz continuous;

(vi) G: $E \longrightarrow 2^X$ is to assign a guardian condition to each discrete transition, satisfying the following conditions:

** $\forall e = (l,l') \in E, G(e)$ denotes a measurable subset of ∂ Inv (l)

** $\forall l \in L, \{G(e)\colon e = (l,l') \in E, l' \in L\}$ is a disjoint subset of ∂ Inv (l)

(vii) R: $E \times X \longrightarrow \mathscr{P}(X)$ is a reset mapping. $\mathscr{P}(X)$ represents a set of probability measures defined on X, and continuous variables are reset according to the probability distribution.

According to the definition, the SCCPS hybrid state space is $L \times X$, and $(l,x) \in L \times X$ represents the hybrid state. The continuous dynamics of SCCPS evolves according to the SDE in the current control mode. However, the discrete dynamics refers to migrating one control mode to another control mode with the guardian condition on the discrete transition, when the continuous variable cannot reach the boundary of the invariant.

Let $x_l(t)$ be the SDE solution of the initial state $x_l(0)$; $\tau(l) = \inf\{t \in \mathbb{R}_{>0}, x_l(t) \notin \text{Inv}(l)\}$ means that, in the control mode l, the first time that the evolution of a continuous variable violates the invariant, that is, the first time of exiting the control mode l.

SCCPS execution semantics: a random execution of SCCPS is defined as a random process $(l(t), x(t)) \in L \times X$ in the SCCPS state space. If there is a stop-time sequence $T_0 = 0 < T_1 < T_2 < \cdots$ that makes $\forall k \in \mathbb{N}$, where

(i) $(l_0, x_0) \in L \times X$ indicates the initial state of SCCPS.

(ii) $t \in (T_k, T_{k+1}), l(t) = l(T_k)$ is a const, and $x(t)$ is a continuous solution of the SDE $d_x(t) = f(l(T_k), x(t))d_t + g(l(T_k), x(t))d_{B_t}$;

- $T_{k+1} = T_k + \tau(l(T_k))$;
- the probability distribution of $x(T_{k+1})$ is determined by the reset map $R(e_k, x(T_{k+1}^-))$, where $e_k = (l(T_k), l(T_{k+1})) \in E$ and $x(T_{k+1}^-) = \lim_{t \longrightarrow} T_{k+1} x(t)$.

SCCPS path: a SCCPS execution path is defined as an infinite sequence $\sigma = ((l_0, x_0), t_0), ((l_1, x_1), t_1), \ldots$ from the initial state (l_0, x_0), where $(l_i, x_i) \in L \times X$ represents the SCCPS state. $t_i \in R_{\geq 0}$ means the time that transitions the state (l_i, x_i) to the next state (l_{i+1}, x_{i+1}).

3. Our Approach

In this section, we present our proposed method with the SCCPS path space to construct a cross-entropy optimization model and use an iterative learning method to obtain an optimal importance sampling distribution from the parameterized distribution cluster of the path space.

3.1. SCCPS Path Space Model

3.1.1. Model Representation. To avoid the complexity of the dynamic evolution of SCCPS, SMC does not pay attention to the structure of SCCPS, but focus on sampling the execution path of SCCPS. The behavior of SCCPS evolving over time can be characterized by the path of the system. According to the execution semantics of SCCPS, the execution path generation process of SCCPS can be described as follows: in the current control mode l_i, the continuous variable x_i evolves according to the SDE. When the evolution of x_i satisfies the guardian condition $(x_i \in G(l_i, l_{i+1}))$, it migrates to the next control mode l_{i+1} and the initial value of x_{i+1} is determined by the random reset kernel R. The residence time of l_i is $t_i = \inf\{t \in R_{>0}, x_i(t) \notin \text{Inv}(l_i)\}$. t_i is a random variable, and its value depends on the SDE of l_i and the initial values $x_i(0)$ and Inv (l_i). According to the generation process of the SCCPS execution path, the next state of SCCPS depends on the current state and the related residence time of the current state. Therefore, the execution path of the SCCPS can be regarded as that it is generated in the continuous-time Markov process in the hybrid state space. As the residence time of l_i is longer, the probability of migration from l_i is higher. It can further presume that the residence time of l_i obeys the exponential distribution, and the continuous-time Markov process then becomes CTMC.

Let G_l denote the guard condition set of all edges starting from l:

$$G_l = \{G(e)\colon e = (l,l') \in E, l' \in \text{Loc}\}, \tag{4}$$

where $G(e) \in \partial$ Inv (l) and $G(e_i) \cap G(e_j) = \varnothing$, $i \neq j$. In l, the time for the continuous variable evolving to satisfying the conditions of each guard is $\tau_1, \tau_2, \ldots, \tau_{|G_l|}$. Then, the residence time in l is $t_l = \min\{\tau_1, \tau_2, \ldots, \tau_{|G_l|}\}$. Supposing $\tau_1, \tau_2, \ldots, \tau_{|G_l|}$, respectively, obey the exponential distribution of parameters $\{\lambda_{l,l'}, l' \in L, (l,l') \in E\}$, then the residence time t_l in l obeys the exponential distribution of parameters $\sum_{l' \in \text{Loc}, (l,l') \in E} \lambda_{l,l'}$. With this assumption, the execution path of SCCPS can be generated by the CTMC random process.

Definition 1. SCCPS path generation model: the path generation model on the SCCPS state space is defined as CTMC $= (S, s_0, \lambda)$, where

(i) $S = L$ represents the discrete state set of SCCPS

- $s_0 \in L$ denotes the initial state of SCCPS
- Migration rate function λ: $S \times S \longrightarrow R_{\geq 0}$, and all migration rate function values form the migration rate matrix λ

It can be seen from this definition that when the CTMC structure is known, its behavior is controlled by the migration rate matrix λ, whose value comes from SCCPS. The value of λ is estimated with the maximum likelihood method according to simulating the execution of SCCPS to obtain the time samples of the state transition.

3.1.2. Algorithm of Learning Model Parameters. The rarity of the path does not necessarily imply that the conversion rate between two adjacent discrete states is low, and the rarity of the safety attributes in the path space does not necessarily imply that the optimal parameters in the parameter space are rare. Based on this observation, this section introduces our approach of leveraging the maximum likelihood estimation method to estimate the migration rate of two adjacent discrete states of SCCPS and obtain the migration rate matrix λ. With the simulation operation of each discrete state of SCCPS, the discrete state is sampled to migrate to the next discrete state time; we then use the maximum likelihood estimation to obtain an estimate of λ.

For the state $s_i \in S$, we simulate executing the SDE in the running state s_i to obtain the migration time $t_k (k = 1, \ldots, N)$ samples of the adjacent state s_j. Assuming that the migration time between s_i and s_j obeys the exponential distribution of the parameter λ_{ij}, then the likelihood function of λ_{ij} can be obtained:

$$L\left(\lambda_{ij}\right) = \prod_{k=1}^{N} \lambda_{ij} e^{-\lambda_{ij} t_k}, \tag{5}$$

and its log likelihood function is as follows:

$$\ln L\left(\lambda_{ij}\right) = \sum_{k=1}^{N} \ln \lambda_{ij} - \lambda_{ij} \sum_{k=1}^{N} t_k. \tag{6}$$

We further take the derivative of λ_{ij} with the log-likelihood function and make it equal to 0, and its estimated value can be resolved, $\widehat{\lambda}_{ij} = (1/N) \sum_{k=1}^{N} t_k$. With $E(\widehat{\lambda}_{ij}) = (1/N) \sum_{k=1}^{N} E(\widehat{\lambda}_{ij}) = (1/\lambda_{ij})$, it can be seen that the estimated value is an unbiased estimate of λ_{ij}. The estimated variance is

$$\mathrm{Var}\left(\widehat{\lambda}_{ij}\right) = \mathrm{Var}\left(\frac{1}{N} \sum_{k=1}^{N} t_k\right) = \frac{1}{N^2} \sum_{j=1}^{N} \mathrm{Var}\left(t_k\right) = \frac{1}{N\lambda_{ij}^2}, \tag{7}$$

but the estimated variance is biased, and the variance will be decreased as the samples increase.

In most cases, it is difficult to obtain a clear expression for the random execution of SCCPS. However, what the safety concerned is the accessibility analysis of discrete states. The discrete state set S and its transitions can capture all necessary information. Therefore, we derive the DTMC from the SCCPS path generation model to represent the path space of SCCPS. The value of DTMC's migration probability matrix P: $S \times S \longrightarrow [0, 1]$ can be obtained from the migration rate matrix λ of the SCCPS path generation model. For two states s_i and $s_j \in S$,

$$P\left(s_i, s_j\right) = \begin{cases} \dfrac{\lambda_{ij}}{\lambda_i}, & s_i \neq s_j, \\ 1, & s_i = s_j, \end{cases} \tag{8}$$

where $\lambda_i = \sum_{s_j \in S} \lambda_{ij}$.

3.2. Method of Sampling Rare Attributes. In the path space of the high-safety SCCPS, it is difficult to obtain samples satisfying the rare attributes, which makes the SMC infeasible. To address this challenge, we propose a method for sampling the rare attributes. It uses the cross-entropy method to learn an optimal-importance sample distribution from the path space of the SCCPS. With this sample distribution, it is easy to obtain the samples that satisfy the rare attributes. Thus, the convergence of the SMC can be accelerated. The importance sampling distribution is corrected by the likelihood ratio weighting to ensure that the SMC verification result is unbiased.

3.2.1. Zero-Variance Importance Sampling Distribution. The basic idea of the importance sampling method [33, 34] is to change the probability density distribution of random variables, so as to obtain the samples of extremely small probability events with a higher probability. We now present the SMC method based on the importance sampling. Let $f(\omega)$ be the true distribution of path ω, and let $g(\omega)$ be the importance sampling distribution, and $g(\omega)$ can obtain the samples of the extremely small probability events with a higher probability when $g(\omega) \neq 0$ and $f(\omega) \neq 0$. In the case of verifying the extremely small probability events, it is difficult to sample from $f(\omega)$ to meet the requirements, but the importance sampling method is to sample from $g(\omega)$. The probability $p = E_f[I(\omega)]$ satisfying the system attribute can be described as

$$\begin{aligned} p = E_f[I(\omega)] &= \int I(\omega) f(\omega) \mathrm{d}_\omega = \int I(\omega) \frac{f(\omega)}{g(\omega)} g(\omega) \mathrm{d}_\omega \\ &= \int I(\omega) W(\omega) g(\omega) \mathrm{d}_\omega = E_g[I(\omega) W(\omega)], \end{aligned} \tag{9}$$

where $W(\omega) = (f(\omega)/g(\omega))$ is the likelihood ratio, and $g(\omega)$ is for the importance sampling. We leverage the likelihood ratio to correct the weighting to ensure that the estimated value of p is unbiased. We then randomly sample N independent execution paths $\omega_i, i \in \{1, \ldots, N\}$ from the importance distribution $g(\omega)$ and obtain the unbiased estimate:

$$\widehat{p} = \frac{1}{N} \sum_{i=1}^{N} I\left(\omega_i\right) W\left(\omega_i\right), \tag{10}$$

and estimated variance

$$\mathrm{Var}_g[\widehat{p}] = \frac{1}{N}\left(E_g\left[I^2(\omega) W^2(\omega)\right] - p^2\right), \tag{11}$$

for p, respectively.

The efficiency and accuracy of importance sampling rely on the selection of the distribution $g(\omega)$. If the selection is inadequate, the importance sampling method is difficult to effectively achieve the acceleration effect and may play a decelerating effect. The key problem of importance sampling is to find a density function for the optimal sampling

probability to minimize the estimated variance. With formula (10) returning 0, it can obtain the following formula:

$$g^*(\omega) = \frac{I(\omega) f(\omega)}{p}, \tag{12}$$

where $g^*(\omega)$ is a zero-variance importance sampling distribution, which means that extracting only one sample from the zero-variance importance sampling distribution can be used to calculate its estimated value, that is, any sample is an unbiased estimate of its mean. However, the zero-variance importance sampling distribution depends on the true value p, and the value of p is unknown. Therefore, it is impossible to sample from $g^*(\omega)$. This paper proposes to use the cross-entropy method to find an approximate optimal importance sampling distribution closest to $g^*(\omega)$ from the parameterized distribution family of the sample path space, so as to reduce the SMC variance and accelerate the convergence of the SMC algorithm.

3.2.2. Cross-Entropy Optimization Model. This section is to obtain the optimal importance sampling distribution by minimizing the cross entropy between the two probability distributions. According to the definition of cross entropy [35], this section provides the definition of cross entropy for the SCCPS path space.

Definition 2. Cross entropy for the SCCPS path space: the cross entropy between two probability measures $f(\omega)$ and $f'(\omega)$ for the SCCPS path space Ω is as follows:

$$\mathrm{CE}\left(f(\omega), f'(\omega)\right) = \int_{\Omega} f(\omega) \ln \frac{f(\omega)}{f'(\omega)} \mathrm{d}_{\omega}. \tag{13}$$

The cross entropy is used to assess the similarity of two probability distributions. The value of cross entropy is smaller, and $f(\omega)$ and $f'(\omega)$ are more similar, i.e., $\mathrm{CE}(f(\omega), f'(\omega)) = 0$ if and only if $f(\omega) = f'(\omega)$.

According to Definition 2, the construction of the cross-entropy optimization model on the SCCPS path space is given below. Assume that the original distribution $f(\omega)$ of the SCCPS path ω comes from the parameterized distribution family $\{f(\omega, \theta)\}$, The cross-entropy optimization method is used to select a distribution $f(\omega, \lambda^*)$, $\lambda^* \in \theta$ in the parameterized distribution family, $\lambda^* \in \theta$ and the optimal distribution $g^*(\omega)$ have the smallest cross-entropy. This optimization problem can be described for

$$\begin{aligned} \min_{\lambda} \mathrm{CE}\left(g^*(\omega), f(\omega, \lambda)\right) &= \min_{\lambda} \int_{\Omega} g^*(\omega) \ln \frac{g^*(\omega)}{f(\omega, \lambda)} \mathrm{d}_{\omega} \\ &= \min_{\lambda} \int_{\Omega} g^*(\omega) \ln g^*(\omega) \mathrm{d}_{\omega} \\ &\quad - \int_{\Omega} g^*(\omega) \ln f(\omega, \lambda) \mathrm{d}_{\omega}. \end{aligned} \tag{14}$$

The first term of formula (13) has nothing to do with λ and minimizing cross entropy is equivalent to maximizing the second term. Let $D(\lambda) = \int_{\Omega} g^*(\omega) \mathrm{Inf}(\omega, \lambda) \mathrm{d}_{\omega}$; the minimization problem of formula (13) is equivalent to the maximization problem of formula (14):

$$\begin{aligned} \max_{\lambda} \int_{\Omega} g^*(\omega) \ln f(\omega, \lambda) \mathrm{d}_{\omega} &= \max_{\lambda} \int_{\Omega} I(\omega) f(\omega) \ln f(\omega, \lambda) \mathrm{d}_{\omega} \\ &= \max_{\lambda} E[I(\omega) \ln f(\omega, \lambda)]. \end{aligned} \tag{15}$$

Solving the optimization problem of formula (14) requires sampling from the true distribution $f(\omega)$. However, in the case of rare attribute verification, it is difficult to sample from $f(\omega)$ to the path sample that satisfies the rare attribute. By using importance again, the sampling method samples from the distribution $f(\omega, \mu)$ and the selection of parameter μ should be able to increase the probability of the path that meets the rare attribute. Therefore, the optimization problem of formula (14) can be re-formed as

$$\begin{aligned} &\max_{\lambda} \int_{\Omega} I(\omega) \frac{f(\omega)}{f(\omega, \mu)} f(\omega, \mu) \ln f(\omega, \lambda) \mathrm{d}_{\omega} \\ &= \max_{\lambda} \int_{\Omega} I(\omega) W(\omega, \mu) f(\omega, \mu) \ln f(\omega, \lambda) \mathrm{d}_{\omega}. \\ &= \max_{\lambda} E_{\mu}[I(\omega) W(\omega, \mu) \ln f(\omega, \lambda)]. \end{aligned} \tag{16}$$

Among them, the likelihood ratio function $W(\omega, \mu) = (f(\omega)/f(\omega, \mu))$. In formula (16), the optimal solution of its optimization problem λ^* can be estimated by the path sample, and the sample mean is replaced by the expectation Get the estimated value of λ^*

$$\widehat{\lambda^*} = \mathrm{argmax}_{\lambda} \frac{1}{N} \sum_{i=1}^{N} I(\omega_i) W(\omega_i, \mu) \ln f(\omega_i, \lambda), \tag{17}$$

where $\omega_1, \omega_2, \ldots, \omega_N$ is a sample from the distribution $f(\omega, \mu)$.

3.3. Algorithm of Verifying the Cross-Entropy Safety. In Section 3.1, we provide a DTMC-based method to approximate the SCCPS path space. SMC mainly considers the system execution path $\omega = s_0, s_1, \ldots, s_k (k > 0)$ within a bounded time T, where k is a random variable to represent the number of state transitions, and its value varies with ω. Let $\langle l, m \rangle$ denote two adjacent and ordered state pairs in ω, $S(\omega)$ represent the set of ordered state pairs in ω, $n_{lm}^{(\omega)}$ represent the number of transitions from state l to state m in ω, and $n_l^{(\omega)}$ represent the number of occurrences of the state l in ω; then, the probability measure function of path ω under system parameter p can be formulated as

$$f(\omega, p) = \iota_{\mathrm{init}}(s_0) \prod_{\langle l,m \rangle \in S[\omega]} (p_{lm})^{n_{lm}^{(\omega)}}. \tag{18}$$

Substituting $f(\omega_i, \lambda)$ of formulas (16) with (17), we obtain

$$\max_p \quad \frac{1}{N}\sum_{i=1}^{N} I(\omega_i)W(\omega_i,\mu)\left(\ln t_{\text{init}}(s_0)+\sum_{\langle l,m\rangle\in S(\omega_i)} n_{lm}^{(\omega_i)}\ln p_{lm}\right) \text{s.t.} \sum_{m\in S} p_{lm}=1, \tag{19}$$

and formula (18) can be transformed by the Lagrangian multiplier method into the following optimization problem:

$$\max_p \sum_{i=1}^{N} I(\omega_i)W(\omega_i,\mu)\left(\ln t_{\text{init}}(s_0)+\sum_{\langle l,m\rangle\in S(\omega_i)} n_{lm}^{(\omega_i)}\ln p_{lm}\right)+\nu_i\left(\sum_{m\in S} p_{lm}-1\right), \tag{20}$$

where ν_i is the Lagrangian multiplier. Taking the derivative of formula (19) to p_{lm} and making it equal to 0, the solution can be

$$p_{lm}=\frac{\sum_{i=1}^{N} I(\omega_i)W(\omega_i,\mu)n_{lm}^{(\omega_i)}}{\sum_{i=1}^{N} I(\omega_i)W(\omega_i,\mu)n_{l}^{(\omega_i)}}, \tag{21}$$

where ω_i $(1\le i\le N)$ is the sample path from the distribution $f(\omega,\mu)$, and $f(\omega_i)$ represents the true probability distribution of the SCCPS path.

With formula (20), it indicates that the estimated value of the optimal solution relies on the initial distribution $f(\omega,\mu)$. However, the distribution of $f(\omega,\mu)$ is generally far from the optimal distribution. Therefore, in order to reduce the influence of the initial distribution $f(\omega,\mu)$ on the optimal importance sampling distribution, this paper proposes the iterative solution in the path space. Through the iteration, the algorithm can explore a wider path space, so as to obtain a better approximate optimal solution.

Let the initial distribution parameter be $u=p^{(0)}$, and an iterative formula can be obtained from formula (20):

$$p_{lm}^{(j+1)}=\frac{\sum_{i=1}^{N} I\left(\omega_i^{(j)}\right)W\left(\omega_i^{(j)},p^{(j)}\right)n_{lm}^{\left(\omega_i^{(j)}\right)}}{\sum_{i=1}^{N} I\left(\omega_i^{(j)}\right)W\left(\omega_i^{(j)},p^{(j)}\right)n_{l}^{\left(\omega_i^{(j)}\right)}}, \tag{22}$$

where N is the number of samples per iteration, $W(\omega_i^{(j)},p^{(j)})=(f(\omega_i^{(j)})/f(\omega_i^{(j)},p^{(j)}))$ represents the likelihood ratio of the nth iteration, and $\omega_i^{(j)}$ is the ith sample path sampled from the distribution $f(\omega_i^{(j)},p^{(j)})$.

Usually, only a few state transitions can be seen in each simulated execution. During each iteration, some parameters do not work in the path that satisfies the extremely small probability event. Formula (21) will set these parameter values to zero so that these parameters will not work in all subsequent iterations. As a result, the iterative algorithm converges too prematurely to detect a wider parameter space. To avoid this situation, this paper adopts a smoothing strategy to temporarily reduce the importance of inoperative parameters in the iteration instead of simply setting them to zero. The smoothing strategy is to weight current iteration value and the parameters of the previous iteration:

$$p_{lm}^{(j+1)}=\alpha p_{lm}^{(j)}+(1-\alpha)\frac{\sum_{i=1}^{N} I\left(\omega_i^{(j)}\right)W\left(\omega_i^{(j)},p^{(j)}\right)n_{lm}^{\left(\omega_i^{(j)}\right)}}{\sum_{i=1}^{N} I\left(\omega_i^{(j)}\right)W\left(\omega_i^{(j)},p^{(j)}\right)n_{l}^{\left(\omega_i^{(j)}\right)}},$$
$$\alpha\in(0,1). \tag{23}$$

The smoothing strategy can retain important but not yet effective parameters. Iterative formula (21) and smoothing formula (22) can jointly ensure that approximately uniform sampling is obtained from the path set of events satisfying the minimal probability.

The selected initial distribution $f(\cdot;p^{(0)})$ should be able to produce some paths that satisfy the event with minimal probability in the first iteration, that is, the selected parameter $p^{(0)}$ should be able to increase the probability of occurrence of the extremely small probability events. Therefore, in this paper, we set the initial parameter $p^{(0)}$ to a uniform distribution, and the uniform distribution can quickly obtain the sample path that satisfies the extremely small probability event. The condition for stopping the iteration can be that the coefficient of variance or the distance between two iteration parameter vectors are not higher than a certain constant or the maximum number of iterations. For example, given any small positive number $\epsilon>0$, if $\|p^{(j)}-p(j-1)\|<\epsilon$ is satisfied, the iteration will be stopped. To facilitate the comparison, we limit the maximum number of iterations in the experiment. To sum up, Algorithm 1 presents the description of the importance sampling distribution learning algorithm, which iteratively solves the approximate optimal importance sampling distribution in the SCCPS path space of the attributes for being verified.

Regardless of sample acquisition time and BLTL model checking time, the time complexity of Algorithm 1 is $O(j_{\max}|p|N)$. Since the optimized objective function is convex, there is a unique optimal solution. If Algorithm 1 can converge, it must converge to the vicinity of the unique optimal solution [36]. Since the number of samples in each iteration is limited, the convergence is probabilistic but not necessarily monotonic. By simply limiting the maximum number of iterations $j_{\max}$, the algorithm can be guaranteed to be terminated with 100% probability. For the proof of convergence of cross-entropy optimization, please refer to [37]; thus, a formal proof of convergence is not provided in this paper. In experiments, we observe that the parameters

are convergent. Once the parameters converge, the last set of simulated samples is used to estimate the probability $\widehat{p}$ that SCCPS satisfies the safety attribute with the optimal importance sampling distribution. Algorithm 2 describes the verification process of the safety verification algorithm.

4. Experiment and Analysis

To evaluate the effectiveness and performance of the Cross-Entropy Safety Verification Algorithm (CESVA) method proposed in this paper, we apply CESVA to a fault-tolerant controller for an aircraft elevator system (FTC4AE), that is, a Stateflow/Simulink hybrid system modeling case from MATLAB. It introduces the randomness in terms of the fault injection and simulates with MATLAB to obtain the system execution path. Path checking is realized by the BLTL model detector of Plasma-Lab [38]. In the experiment, the rare attributes of FTC4AE is verified with the CESVA method, which is further compared with the Heuristic Importance Sampling (HIS) method [17].

4.1. Validity Measurement of Experimental Results. In the case of nonrare attribute verification, the confidence interval is used to assess the accuracy of various methods, while in the case of rare attribute verification, the relative error of sampling is used to assess the accuracy of the estimation:

$$\mathrm{RE}(\widehat{p}) = \frac{\sqrt{\mathrm{Var}[\widehat{p}]}}{E[\widehat{p}]} \approx \sqrt{\frac{1}{N\widehat{p}}}, \tag{24}$$

where $E[\widehat{p}]$ is replaced by the current estimated value $\widehat{p}$, $\mathrm{Var}[\widehat{p}] = (1/N-1)\sum_{i=1}^{N}(I(\sigma_i)W(\sigma_i,\mu,\lambda^*)-\widehat{p})^2$.

Skewness is a measure of assessing the skewing direction and degree of data distribution and is the characteristic number that characterizes the degree of asymmetry of the probability distribution density curve with respect to the average. Skewness is defined as the third-order standardized moment of the sample, and the skewness of the normal distribution is 0, and its estimator is evenly distributed around the mean:

$$\mathrm{skew}(\widehat{p}) = \frac{N}{(N-1)(N-2)} \frac{\sum_{i=1}^{N}\left(\widehat{p} - (1/N)\sum_{j=1}^{N}\widehat{p}_j\right)^3}{(\mathrm{Var}[\widehat{p}])^{(3/2)}}. \tag{25}$$

The negative skewness means that the distribution is left-tailed. At this time, the data on the left of the mean are less than the data on the right. Intuitively, the tail on the left is longer than the tail on the right. In contrast, the positive skewness means that the distribution is right-tailed. The data on the right of the mean is less than the left. Intuitively, the tail on the right is longer than the tail on the left.

4.2. Experiment and Analysis on a Fault-Tolerant Controller for the Aircraft Elevator System. The fault-tolerant controller for an aircraft elevator system is a part of a large Simulink model of HL-20 rescuers developed by the National Aeronautics and Space Administration [39]. The two horizontal tails on the two side of the aircraft's fuselage are controlled by two elevators, respectively. Each elevator has two independent hydraulic actuators. In the normal operation process, each elevator is positioned by its corresponding external actuator, and its internal actuator can be used when the external actuator does not work. The two external actuators are driven by two independent hydraulic circuits, and the two internal actuators are both connected to the third hydraulic circuit. The system should ensure that only one set of actuators (i.e., external or internal) locates the elevator at any given time. If the external actuator or its corresponding hydraulic circuit fails, the system will activate the internal actuator. If the fault still exists, the external actuator will be shut down and eventually isolated. The fault in the hydraulic circuit may be temporary, and if the fault is cleared, the hydraulic circuit can always be restored to the online state. The control logic of the system is implemented in the form of a state flow diagram, while the hydraulic actuators and elevators are modeled by using Simulink.

According to modifying the Stateflow/Simulink model, we add random faults into three hydraulic circuits. Setting the fault model with an out-of-bounds' reading of circuit pressure, we model the fault injection as three independent Poisson processes. When the hydraulic circuit fails, the circuit will stay in the fault state for one second. Then, the pressure reading will restore to its normal value, and the fault state will be terminated. In our experiments, the being estimated safety attribute is the probability that, within 25 seconds, the horizontal tails will not respond to the control inputs in the duration of 1 second.

We estimated the probability of the BLTL formula φ:

$$\varphi = F_{25}G_1\left(\left(H_1\mathrm{fail} \vee H_3\mathrm{fail}\right) \wedge H_2\mathrm{fail}\right), \tag{26}$$

where H_1 and H_3 represent the hydraulic circuit that drives the external actuator, while H_2 represents the hydraulic circuit that drives the internal actuator.

In the experiment, the failure rate of the three hydraulic circuits is set to 0.001, and the failure repair rate is 1. With the two parameters, the parameter ν in Algorithm 1 can be calculated. It still is difficult to obtain samples that satisfy the attribute φ with the previous parameters. Therefore, to ensure that the obtained samples can satisfy the attribute φ, the initial failure rate is set as 0.1 and the fault repair rate is set as 1. According to these two parameters, the initial parameter of iteration $p^{(0)}$ in Algorithm 1 can be calculated. In order to assess the performance of verifying the rare attributes with the CESVA method, 20 iterations of Algorithm 1 are performed. In each iteration, the number of samples is $N = 104$, the smoothing factor $\alpha = 0.2$, and the total number of required samples is 2.0×10^5.

Figure 1 shows the change trend of the failure rate parameters during the 20 iterations of the CESVA method. At the beginning of the iteration, the parameters converge rapidly. When the parameters are close to their optimal values, the convergences of their values slow down with random fluctuations. From the 16th iteration, the failure rate parameters start to converge to the stable values. From the

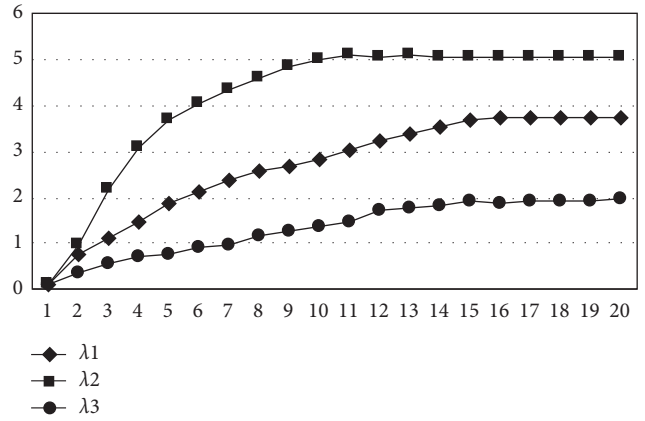

Figure 1: Convergence of parameters during 20 iterations.

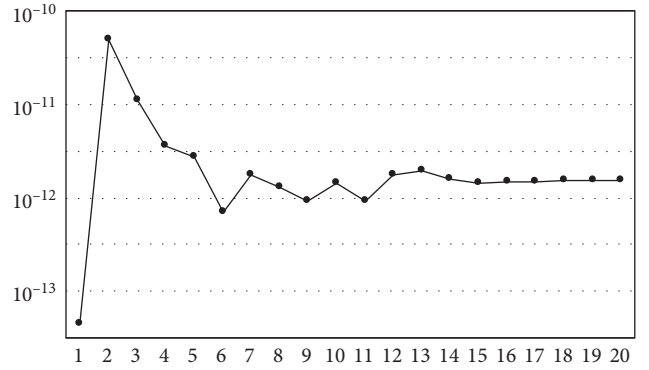

Figure 2: Distribution of estimated values of CESVA during 20 iterations.

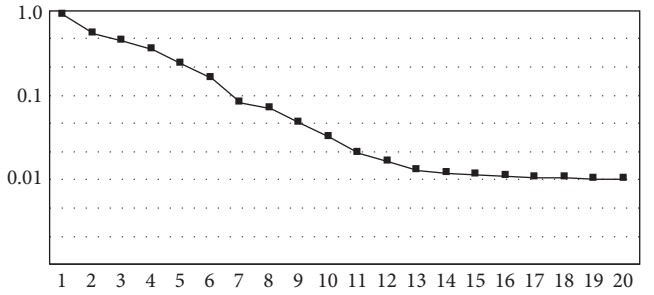

Figure 3: Distribution of relative error of CESVA during 20 iterations.

perspective of the parameter convergence trend, it seems that the value of the failure rate parameter increases with the increasing iteration times. It indicates that the proportion of sampling the paths satisfying the rare attribute is gradually increasing.

Figure 2 illustrates the distribution of the estimated values of the CESVA method during the iterations. The estimated value gradually converges from the 17th iteration. Figure 3 presents the distribution of the relative error of the CESVA method during the iterations. The relative error gradually converges from the 16th iteration. Finally, the probability estimated value of the security attribute φ is 1.682×10^{-12}, and the value of the relative error is 0.01.

In order to verify the statistical performance of the CESVA method, 100 experiments were carried out under the above parameters, and 2.0×10^5 samples were used in each experiment. Compared with the performance of the HIS method under the same sample size, Table 1 shows the mean, skewness, and statistical indicators such as standard deviation (likelihood ratio standard deviation), relative error, and sample size for each experiment. As presented in Table 1, with the same sample size, the estimated values of the CESVA method are more closely distributed around the mean value, and the likelihood is over 10 times less than the standard deviation and relative error, when comparing against the HIS method. Although the true probability is unknown, statistical indicators such as the standard deviation, skewness, and relative error of the likelihood ratio illustrate that the true probability and the mean are very close.

5. Related Work

The verification of the rare attribute for SMC mainly includes the importance sampling method, the importance splitting method, and the statistical learning method.

The importance sampling method is an effective method to solve the verification of rare attributes. For the CTMC and DTMC random models, Reijsbergen et al. [40] and Barbot et al. [23] leveraged the heuristic methods to obtain an importance sampling distribution to complete the attribute verification of the two types of models. For the Stateflow/Simulink model, Clarke and Zuliani [24] proposed the SMC method of cross-entropy minimization importance sampling to verify its safety properties. Zuliani et al. [17] further used the SMC method in paper [24] to verify the safety properties of a class of discrete-time SHS. The method proposed by Clarke and Zuliani [24] assumes that the distribution of the system path space is exponential distribution. By simply increasing the failure rate of the system parameters and calculating the optimal parameters of the exponential distribution with the paths satisfying the rare attributes extracted at one time, an importance sampling distribution can be obtained. J´egourel et al. [26] used a random guardian command to the importance sampling distribution. This model can approximate the path distribution of the system by increasing the number of commands (the number of parameters) and uses the minimized cross-entropy method to obtain an importance sampling distribution in the random model. However, the optimal importance sampling distribution obtained by the above method does not come from the distribution family of the system path space, and these methods actually belong to the heuristic importance sampling method.

The importance segmentation method [34] is a method of reducing the estimated variance. Based on the importance segmentation method, J´egourel et al. [33] proposed the SMC algorithm for the verification of small probability events. The key idea is to decompose the system logic

Input: N, the number of samples per iteration.
Input: v, the true path distribution parameter of SCCPS.
Input: $p^{(0)}$, the initialization parameter.
Input: $j_{\max}$, the maximum number of iterations.
Output: p^* Optimal parameters.
(1) Function learningAlg (N, v, $p^{(0)} j_{\max}$)
(2) $j = 0$;
(3) while $j < j_{\max}$ do
(4) $A = 0$, $B = 0$, $i = 1$
(5) while $i \leq N$ do
(6) generate a path ω_i according to the pdf $f(., p^{(j)})$
(7) if $\omega_i \models \varphi$ then
(8) $W_i = \sum_{\langle l,m \rangle \in S(\omega_i)} (v_{lm}/p_{lm})^{n_{lm}^{(\omega_i)}}$;
(9) $A = A + W_i n_{lm}^{(\omega_i)}$;
(10) $B = B + W_i n_l^{(\omega_i)}$;
(11) $i = i + 1$;
(12) $p_{lm}^{(j+1)} = \alpha p_{lm}^{(j)} + (1 - \alpha)(A/B)$;
(13) $j = j + 1$
(14) return $p^{(j-1)}$

Algorithm 1: Importance sampling distribution learning algorithm.

Input: $N_I S$, The number of samples.
Input: v, the true path distribution parameter of SCCPS.
Input: p^*, the optimal parameters calculated by Algorithm 1.
Output: $\widehat{p}$, Probability of SCCPS meeting safety attributes.
(1) Function verifyingAlg (N, v, $p^{(0)} j_{\max}$)
(2) $A = 0$, $i = 1$
(3) while $i \leq N$ do
(4) generate a path ω_i according to the pdf $f(., p^{(j)})$
(5) if $\omega_i \models \varphi$ then
(6) $W_i = \sum_{\langle l,m \rangle \in S(\omega_i)} (v_{lm}/p_{lm})^{n_{lm}^{(\omega_i)}}$:
(7) $A = A + W_i$;
(8) $i = i + 1$
(9) return (A/N_{IS})

Algorithm 2: Safety verification algorithm.

Table 1: Comparison of statistical performance between CESVA and HIS.

Algorithm	Mean	Skewness	Standard deviation	Relative error
CESVA	1.687×10^{-12}	0.029	1.853×10^{-14}	0.011
HIS	1.986×10^{-12}	1.264	2.654×10^{-13}	0.133

attributes into embedded attributes, which makes its probability easier to be estimated and reduces the number of sample paths required by verification. To improve the performance, the attributes need to be decomposed into multiple levels with different probabilities. During the decomposition process, copying or eliminating paths depend on their intermediate behavior. When the decomposition is over, an estimated probability that the attribute is satisfied can be obtained. The importance segmentation method is essentially heuristic and depends on the model, but lacks the support of theoretical results.

Applying statistical learning methods to SMC is also an important research direction. Du et al. [19] proposed a learning SMC framework based on support vector machine-based two classifiers. It uses cost-sensitive and resampling methods to solve the unbalanced data learning problem of support vector machines and implements predicting and assessing the probability of occurrence of small-probability events with a relatively small number of samples. However, this method cannot obtain rare attribute samples. For the low-probability attributes of hardware circuits with multiple failure regions, Kumar et al. [41] assumed that the system failure distribution is a Gaussian mixture model, thus proposed to use the variational Bayes method to learn an optimal importance sampling distribution from the Gaussian mixture model. However, the optimal importance sampling distribution is not a distribution family from the system path space. Kalajdzic et al. [42] proposed an SMC method based on the principle of feedback control. This method learns a model of a cyber-physical fusion system by

using importance sampling to estimate the system state and importance division to control the system. So it can infer the probability that the system satisfies the given attributes.

The method proposed in this paper starts from the SCCPS path probability space, constructs a cross-entropy optimization model, and uses an iterative learning method to obtain an optimal importance sampling distribution from the parameterized distribution clusters of the path space. It ensures that the optimal importance sampling distribution can come from the distribution family in the path probability space of SCCPS. And, the iterative learning method ensures that the distribution can evenly cover the unsafe path distribution area. Therefore, the accuracy and efficiency of the rare attribute verification can be improved significantly.

6. Conclusion

SMC has been successfully applied to SCCPS safety attribute verification and has become the most effective solution, but rare attribute verification is still a challenge for SMC. To be able to extract samples satisfying the rare attributes from SCCPS, CTMC is used to construct the probability space model of the execution path of SCCPS given with the probability measure of the random execution path as well as the parameterized probability distribution function family, to construct the cross-entropy iterative model. According to the iteratively learning from finding the approximate optimal importance sampling distribution in the SCCPS path probability space, the efficient sampling of rare attribute samples in SCCPS is achieved. With the evaluating experiments, the experimental results show that, for the verification of rare attributes, comparing against the heuristic importance sampling method with the same number of samples, the estimated value of our method is better distributed around the mean, and the standard deviation and relative error are reduced by more than an order of magnitude. Based on the method proposed in this paper, combining with the current mainstream SMC method to develop an adaptive SMC tool is set as the future work.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request. The authors apply CESVA to a fault-tolerant controller for an aircraft elevator system (FTC4AE) that is a State-flow/Simulink hybrid system modeling case from MATLAB.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Key Research and Development Program of China (no.2018YFB1003900), National Natural Science Foundation of China (no. 61772270), Key Laboratory of Safety-Critical Software (Nanjing University of Aeronautics and Astronautics), and Ministry of Industry and Information Technology Research Project (NJ2019006).

References

[1] N. A. Tanner, J. R. Wait, C. R. Farrar, and H. Sohn, "Structural health monitoring using modular wireless sensors," *Journal of Intelligent Material Systems and Structures*, vol. 14, no. 1, pp. 43–56, 2003.

[2] S. K. Kampf, M. Salazar, and S. W. Tyler, "Preliminary investigations of effluent drainage from mining heap leach facilities," *Vadose Zone Journal*, vol. 1, no. 1, pp. 186–196, 2002.

[3] G. Chunpeng, Z. Liu, J. Xia, and F. Liming, "Revocable identitybased broadcast proxy re-encryption for data sharing in clouds," *IEEE Transactions on Dependable and Secure Computing*, vol. 99, 2019.

[4] L. Yu and J.-p. Wang, "Review of the current and future technologies for video compression," *Journal of Zhejiang University Science C*, vol. 11, no. 1, pp. 1–13, 2010.

[5] H.-h. Xu and J. Zhu, "Aniterative approach to Bayes risk decoding and system combination," *Journal of Zhejiang University SCIENCE C*, vol. 12, no. 3, pp. 204–212, 2011.

[6] O. Déniz, M. Castrillón, J. Lorenzo, L. Antón, M. Hernandez, and G. Bueno, "Computer vision based eyewear selector," *Journal of Zhejiang University Science C*, vol. 11, no. 2, pp. 79–91, 2010.

[7] D. Theodoridis, Y. Boutalis, and M. Christodoulou, "Direct adaptive regulation of unknownnonlinear systems with analysis of themodel order problem," *Journal of Zhejiang University Science C*, vol. 12, no. 1, pp. 1–16, 2011.

[8] X.-c. Zhou, H.-b. Shen, and J.-p. Ye, "Integrating outlier filtering in large margin training," *Journal of Zhejiang University Science C*, vol. 12, no. 5, pp. 362–370, 2011.

[9] I. Prigogine, *Order through Fluctuation: Self-Organization and Social System*, pp. 93–134, Addison-Wesley, London, UK, 1976.

[10] C. Ge, W. Susilo, Z. Liu, J. Xia, P. Szalachowski, and F. Liming, "Secure keyword search and data sharing mechanism for cloud computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 5, 2020.

[11] Z. Wu, Y. An, Z. Wang et al., "Study on zoelite enhanced contact-adsorption regeneration-stabilization process for nitrogen removal," *Journal of Hazardous Materials*, vol 156, 2008 in press.

[12] H. L. S. Younes, "Error control for probabilistic model checking," in *Lecture Notes in Computer Science*, E. A. Emerson and K. S. Namjoshi, Eds., pp. 142–156, Springer, Berlin, Germany, 2006.

[13] K. G. Larsen, "Statistical model checking, refinement checking, optimization, . . . for stochastic hybrid systems," in *Lecture Notes in Computer Science*, pp. 7–10, Springer, Berlin, Germany, 2012.

[14] Q. Wang, P. Zuliani, S. Kong, S. Gao, E. M. Clarke, and " SReach, "SReach: a probabilistic bounded delta-reachability analyzer for stochastic hybrid systems," *Computational Methods in Systems Biology*, vol. 9308, pp. 15–27, 2015.

[15] S. Gorini, M. Quirini, A. Menciassi, G. Permorio, C. Stefanini, and P. Dario, "A novel sma-based actuator for a legged endoscopic capsule," in *First IEEE/RAS-EMBS International Conference on Biomedical Robotics and Biomechatronics*, pp. 443–449, Pisa, Italy, February 2006.

[16] U. Rizvi, *Combined Multiple Transmit Antennas and Multi-Level Modulation Techniques*, Stockholm, Sweden, Europe, in Swedish, 2006.

[17] P. Zuliani, C. Baier, and E. M. Clarke, "Rare-event verification for stochastic hybrid systems,," in *Proceedings of the ACM International Conference on Hybrid Systems: Computation & Control*, pp. 217–226, ACM, Quebec, Canada, April 2012.

[18] P. Zuliani, A. Platzer, and E. M. Clarke, "Bayesian statistical model checking with application to stateflow/simulink verification," *Formal Methods in System Design*, vol. 43, no. 2, pp. 338–367, 2013.

[19] D. Du, B. Cheng, and J. Liu, "Statistical model checking for rare-event in safety-critical system," *Journal of Software in Chinese*, vol. 26, no. 2, pp. 305–320, 2015.

[20] L. Sweeney, *Uniqueness of simple demographics in the U.S. population*, Technical Report No. LIDAP-WP4, Carnegie Mellon University, Pittsburgh, PA, USA, 2000.

[21] ISO, "Steels-classification-part 1: classification of steels into unalloyed and alloy steels based on chemical composition," Technical Report ISO 4948-1, ISO, Geneva, Switzerland, 1982.

[22] D. Reijsbergen, P. de Boer, W. R. W. Scheinhardt, and B. R. Haverkort, "Rare event simulation for highly dependable systems with fast repairs," in *Proceedings of the Seventh International Conference on the Quantitative Evaluation of Systems*, pp. 251–260, IEEE, Williamsburg, VA, USA, September 2010.

[23] B. Barbot, S. Haddad, and C. Picaronny, "Coupling and importance sampling for statistical model checking," *Tools and Algorithms for the Construction and Analysis of Systems*, vol. 7214, pp. 331–346, 2012.

[24] E. M. Clarke and P. Zuliani, "Statistical model checking for cyber-physical systems," *Automated Technology for Verification and Analysis*, vol. 6996, pp. 1–12, 2011.

[25] University, *Citing Electronic Sources of Information*, University of Sheffield Library, Howard, UK, 2001, http://www.shef.ac.uk/library/libdocs/hsl-dvc1.pdf.

[26] C. J´egourel, A. Legay, and S. Sedwards, "Command-based importance sampling for statistical model checking," *Theoretical Computer Science*, vol. 649, pp. 1–24, 2016.

[27] H. L. S. Younes and R. G. Simmons, "Statistical probabilistic model checking with a focus on time-bounded properties," *Information and Computation*, vol. 204, no. 9, pp. 1368–1409, 2006.

[28] T. H´erault, R. Lassaigne, F. Magniette, and S. Peyronnet, "Approximate probabilistic model checking," in *Lecture Notes in Computer Science*, pp. 73–84, Springer, Berlin, Germany, 2004.

[29] Y. J. Kim, M. Kim, and T. Kim, "Statistical moHaifa, Israeldel checking for safety critical hybrid systems: an empirical evaluation," in *proceedings of the 8th international haifa verification conference on hardware and software: verification and testing*, pp. 162–177, Haifa, Israel, November 2012.

[30] G. Agha and K. Palmskog, "A survey of statistical model checking," *ACM Transactions on Modeling and Computer Simulation*, vol. 28, no. 1–6, pp. 6–39, 2018.

[31] A. Legay and M. Viswanathan, "Statistical model checking: challenges and perspectives," *International Journal on Software Tools for Technology Transfer*, vol. 17, no. 4, pp. 369–376, 2015.

[32] J. Hu, J. Lygeros, and S. Sastry, "Towards a theory of stochastic hybrid systems," *Hybrid Systems: Computation and Control*, vol. 337, pp. 160–173, 2000.

[33] C. J´egourel, A. Legay, and S. Sedwards, "An effective heuristic for adaptive importance splitting in statistical model checking," in *Lecture Notes in Computer Science*, pp. 143–159, Springer, Berlin, Germany, 2014.

[34] G. Jiang and M. C. Fu, "Importance splitting for finite-time rare event simulation," *IEEE Transactions on Automatic Control*, vol. 63, no. 6, pp. 1670–1677, 2018.

[35] D. P. Kroese, T. Taimre, and Z. I. Botev, *Handbook of monte carlo methods*, John Wiley & Sons, Hoboken, NJ, USA, 2013.

[36] P.-T. de Boer, D. P. Kroese, S. Mannor, and R. Y. Rubinstein, "A tutorial on the cross-entropy method," *Annals of Operations Research*, vol. 134, no. 1, pp. 19–67, 2005.

[37] A. Costa, O. D. Jones, and D. Kroese, "Convergence properties of the cross-entropy method for discrete optimization," *Operations Research Letters*, vol. 35, no. 5, pp. 573–580, 2007.

[38] B. Boyer, K. Corre, A. Legay, and S. Sedwards, "PLASMA-lab: a flexible, distributable statistical model checking library," in *Proceedings of the 10th International Conference on Quantitative Evaluation of Systems*, pp. 160–164, Buenos Aires, Argentina, August 2013.

[39] M. V. Stringfellow, N. G. Leveson, and B. D. Owens, "Safety-driven design for software-intensive aerospace and automotive systems," *Proceedings of the IEEE*, vol. 98, no. 4, pp. 515–525, 2010.

[40] D. Reijsbergen, P. de Boer, W. R. W. Scheinhardt, and B. R. Haverkort, "Rare event simulation for highly dependable systems with fast repairs," *Perform. Evaluation*, vol. 69, no. 7-8, pp. 336–355, 2012.

[41] J. A. Kumar, S. N. Ahmadyan, and S. Vasudevan, "Efficient statistical model checking of hardware circuits with multiple failure regions," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 33, no. 6, pp. 945–958, 2014.

[42] K. Kalajdzic, C. J´egourel, A. Lukina et al., "Feedback control for statistical model checking of cyber-physical systems," in *Proceedings of the leveraging applications of FormalMethods, verification and Validation: foundational techniques - 7th international Symposium, ISoLA 2016*, Imperial, Corfu, Greece, October 2016.