A Generalized Fault Coverage Model for Linear Time-Invariant Systems

The MIT Faculty has made this article openly available. Please share how this access benefits you. Your story matters.
A Generalized Fault Coverage Model for Linear Time-Invariant Systems

Alejandro D. Domínguez-García, Member, IEEE, John G. Kassakian, Life Fellow, IEEE, and Joel E. Schindall, Fellow, IEEE

Abstract—This paper proposes a fault coverage model for Linear Time-Invariant (LTI) systems subject to uncertain input. A state-space representation, defined by the state-transition matrix, and the input matrix, is used to represent LTI system dynamic behavior. The uncertain input is considered to be unknown but bounded, where the bound is defined by an ellipsoid. The state-transition matrix, and the input matrix must be such that, for any possible input, the system dynamics meets its intended function, which can be defined by some performance requirements. These performance requirements constrain the system trajectories to some region of the state-space defined by a symmetrical polytope. When a fault occurs, the state-transition matrix, and the input matrix might be altered; and then, it is guaranteed the system survives the fault if all possible post-fault trajectories are fully contained in the region of the state-space defined by the performance requirements. This notion of guaranteed survivability is the basis to model (in the context of LTI systems) the concept of fault coverage, which is a probabilistic measure of the ability of the system to keep delivering its intended function after a fault. Analytical techniques to obtain estimates of the proposed fault coverage model are presented. To illustrate the application of the proposed model, two examples are discussed.

Index Terms—Convex optimization, fault coverage, invariant sets, linear time-invariant systems, Markov reliability modeling.

I. INTRODUCTION

ANY ENGINEERING SYSTEM can be thought of as a collection of components interconnected in a specific way to form a certain structure with the intent of delivering some function. The system components may be subject to faults, which are random events resulting in the alteration of the system structure. This alteration may result in the system failing to deliver its intended function.

The safety-critical/mission-critical nature of certain systems, such as the US electric power system, the guidance navigation and control system of an aircraft, or an automotive steer-by-wire system, mandates that the system’s intended function be delivered despite the presence of faults. To achieve this, component redundancy, and appropriate fault detection, isolation, and system reconfiguration (FDIR) mechanisms are often engineered into the system [1].
However, despite the presence of component redundancy and FDIR mechanisms, there might be instances in which there is not complete certainty of the system delivering its function in the presence of a fault due to several factors. First, it is difficult to understand the effect of every possible fault on the system structure; therefore, the models used to determine the appropriate level of redundancy, and the appropriate FDIR mechanisms, may not be complete. Second, the uncertainty in the operational environment makes it difficult to ensure that the component redundancy, and the FDIR mechanisms, will be effective in every possible operational scenario. Finally, for large complex systems, even if extensive testing of the system is carried out before its deployment, it is usually not possible to carry it out exhaustively.

The concept of fault coverage was introduced in response to the fact that it may not be possible to forecast with complete certainty if a system will be able to deliver its function after a fault [2]. Fault coverage can be interpreted as the conditional probability that, given a fault has occurred, altering the system structure, the system recovers, and keeps delivering its intended function. As has been shown in [2], and [3], fault coverage plays an important role in predicting system reliability.

A. Analytical Characterization of Fault Coverage

Several analytical models for predicting fault coverage have been proposed in the fault-tolerant computing field. These analytical models are developed using probabilistic characterizations of the fault mechanism, and recovery process, including discrete and continuous-time Markov chains, non-homogeneous and semi-Markov models, and extended stochastic Petri nets (ESPN) [4].

For example, among the Markovian-types, the fault coverage model proposed in [5] is based on a continuous-time Markov chain, where the states of the chain represent the possible outcomes after the fault occurrence. This model assumes that the time constants of the fault recovery process are very small compared with the rate at which the fault occurs. Therefore, the fault coverage is estimated by obtaining the steady-state distribution of the Markov chain associated with the possible outcomes of the fault. The assumption that fault occurrences and associated recovery mechanisms can be decoupled is known as behavioral decomposition [6]. It also applies to the model proposed in this paper, as will be explained in Section II.

ESPN has been used to formulate other analytical fault coverage models [4], the advantage of which is its flexibility to describe more complex recovery processes than those possibly described with Markov chains [7]. A detailed discussion of other analytical fault coverage models based on probabilistic characterizations of the fault and recovery processes can be found in [4], [7].

B. Statistical Estimation of Fault Coverage

Fault coverage estimation through statistically processing observations collected in fault injection experiments (at the hardware and software levels) has been the subject of extensive research in the field of fault-tolerant computing. Fault injection experiments can be simulation-based, where the faults are injected in a computer model of the system; or prototype-based, where the faults are injected in a physical realization of the system [8].

The effect of a fault on the system’s intended function depends on the system input at the time of fault occurrence. Following this idea, the sample space of a fault injection experiment is composed of all possible combinations of faults and system inputs [9]. Therefore, the fault injection experiment consists of observing the system response to each fault/input pair. The outcomes of the experiment are statistically processed to obtain an estimation of the fault coverage [10]–[12]. Additional work on fault injection experiments has been conducted assuming that, not only the type of fault and input value at the time of fault occurrence influence the coverage, but so does the time at which the fault occurs [13], [14].

C. Scope and Structure of This Paper

The goal of this paper is to propose an analytically tractable method for estimating fault coverage in Linear-Time-Invariant (LTI) systems. The dynamic behavior of LTI systems can be defined by a set of differential equations, which can be expressed using a state-space representation [15]:

$$\frac{dx(t)}{dt} = Ax + Bu, \quad x(0) = x_0,$$  \hspace{1cm} (1)

where $A \in \mathbb{M}^{n \times n}$, and $B \in \mathbb{M}^{n \times m}$ are constant matrices. $x \in \mathbb{R}^n$ is the state vector, and $w \in \mathbb{R}^m$ is the system input. The matrices $A$, and $B$ are defined by the system structure, i.e., the components constituting the system, and how these components are interconnected. The system structure given by the pair $A$, $B$ is such that the system is able to deliver some intended function, which is defined by some performance requirements.

To illustrate the idea of the state-space representation, consider the linear circuit displayed in Fig. 1. The state-space representation of this circuit is defined by

$$\frac{di(t)}{dt} = -\frac{R}{L}i(t) + \frac{1}{L}v(t), \quad i(0) = i_0.$$  \hspace{1cm} (2)

As mentioned before, the system components may be subject to faults that could alter the system structure. In the context of this work, a fault is defined as a random event that will result in the alteration of the system state-space representation, thus altering the pair $\{A, B\}$ in (1). This alteration would result in a new pair of matrices $\{\tilde{A}, \tilde{B}\}$. In the circuit of Fig. 1, a short circuit in the inductor terminals is an example of a fault altering the circuit dynamics defined by (2).

The central question is whether the system is still able to deliver its intended function after the fault occurrence. For example, assume that a certain fault alters the matrix $A$ so as
to cause one of the eigenvalues of the matrix $\hat{A}$ to become a positive number. In this case, the system becomes unstable. Even if the fault does not cause the system to become unstable, it may fail to meet some other dynamic performance requirements, e.g., overshoot. Additionally, it may be the case that the system input $w$ is not deterministic, i.e., there is some uncertainty as to the values $w$ can take. Thus, after the fault occurs, depending on the value of the input $w$, the system may or may not recover. Finally, even if the system input $w$ is deterministic, but time-varying, the time at which the fault occurs may influence whether the system recovers or not.

The purpose of this paper is to propose a fault coverage model for LTI systems that can be analytically formulated in terms of the system structure matrices before, and after the fault ($A$, $B$, and $\hat{A}$, $\hat{B}$ respectively); and includes the uncertainty in the values the input can take at the time of fault occurrence. The proposed model assumes that behavioral decomposition holds, i.e., the time constants associated with the system dynamics are much smaller than the time constants associated with fault occurrences. In a simulation environment, this model could be useful when analyzing the reliability of existing systems, or when designing new ones.

In terms of computation, estimating fault coverage with the proposed model seems to be less expensive than estimating it with a simulation-based fault injection experiment. In a fault injection experiment, the number of experiments to be conducted is given by $\mu \times \rho \times \zeta$, where $\mu$ is the number of possible faults, $\rho$ the number of possible fault occurrence times (obtained by discretizing the time axis), and $\zeta$ is the number of different inputs to the system (obtained by quantizing the input space). In the proposed model, it is only necessary to obtain the matrices of the state-space representation for each fault $\rho$. Additionally, it is not necessary to have a probabilistic characterization of the fault and recovery processes, as is necessary in existing analytical models. This characterization might be difficult to specify, as noted in [4], [7].

The idea of using a model of the system dynamics to understand the effect of faults on the overall system performance also has been proposed in the nuclear engineering field to compute the likelihood of different accident sequences in a reactor [16]–[18]. The resulting methodology is commonly referred to as Dynamic Probabilistic Risk Assessment (DPRA). However, there are several features of DPRA that makes it only suitable for simulation-based fault injection experiments. First, DPRA is formulated in terms of a non-linear space state representation of the reactor dynamics [18]. Second, the time constants associated with the system dynamics of a nuclear reactor are not negligible with respect to the rates at which faults can occur [19]. Therefore, analytical solutions are intractable, even for simple problems. Several techniques based on discretization of time and state variables, combined with simulation-based fault injection, have been proposed to obtain solutions [20].

The structure of this paper is as follows. In Section II, the mathematical formulation of the proposed fault coverage model is presented. This section also provides a computationally tractable method to compute fault coverage estimates. Section III illustrates the ideas presented in Section II, with an example of a first-order electric circuit. In Section IV, the fault coverage model is generalized to the case of a sequence of $k$ faults. Section V shows how this fault coverage model can be naturally included in a Markov model for reliability estimation purposes. Section VI applies the ideas discussed in this paper to the reliability analysis of a dc power distribution system. Concluding remarks, and future work are presented in Section VII.

II. FAULT COVERAGE IN LTI SYSTEMS

In this section, we present the general framework for fault coverage modeling in LTI systems that are described by state-space models where 1) the system input is considered to be unknown but bounded, where the bound is described by an ellipsoid; 2) the performance requirements constrain the system trajectories to regions of the state-space defined by a symmetrical polytope; and 3) behavioral decomposition holds, i.e., the time constants associated with the system dynamics are much smaller than the time constants associated with fault occurrences. First, we introduce general concepts used in reachability analysis of LTI systems which allow us to describe the overall system dynamic behavior in the presence of input uncertainty. Then, we define our fault coverage model, and provide amenable procedures to compute fault coverage estimates based on the LTI system reachability analysis techniques discussed previously.

A. Fault-Free System Dynamics

Let the dynamics of a system operating with no faults be represented by

$$\frac{dx(t)}{dt} = Ax(t) + Bu(t),$$

$$x(0) \in \Omega_0 \equiv \{x : x^t \psi_0^{-1} x \leq 1\},$$

$$w(t) \in \Omega_w \equiv \{w : w^t Q^{-1} w \leq 1\},$$

where $A \in M^{m \times m}$, $B \in M^{m \times n}$, $x \in \mathbb{R}^n$, and $w \in \mathbb{R}^m$. $\psi_0 \in M^{n \times n}$, $Q \in M^{m \times m}$ are positive definite, and the inequalities in (3) define ellipsoids. Then, $\forall t \geq 0$, if the system is stable, the system state $x(t)$ will be contained in some set $\mathcal{R}(t)$ called the reach set, or attainability domain [21].

1) Performance Requirements: The system must be properly designed to deliver its intended function, which is defined by some dynamic performance requirements. These performance requirements will constrain the state-vector $x$ to some region of the state-space $\Phi$ defined by the symmetric polytope

$$\Phi \equiv \{x : \left|\pi_i^t x\right| \leq 1 \ \forall i = 1, 2, \ldots, p\},$$

where $\pi_i \in \mathbb{R}^n$ is a column vector. Then, for the system to deliver its function properly, it is necessary to ensure that any $w(t) \in \Omega_w$, with $t \geq 0$, results in $x(t) \in \Phi$, which is equivalent to ensure that $\mathcal{R}(t) \subseteq \Phi$, $\forall t \geq 0$. Therefore, it is necessary to obtain the reach set $\mathcal{R}(t)$.

2) Ellipsoidal Bound: The computation of the exact shape of $\mathcal{R}(t)$ is usually not easy; even if the initial conditions and inputs are constrained by ellipsoids, $\mathcal{R}(t)$ is not an ellipsoid in general. However, it is possible to compute a bounding ellipsoid, denoted
by \( \Omega(t) \), such that \( \mathcal{R}(t) \subseteq \Omega(t) \forall t \geq 0 \). This bounding ellipsoid is defined by

\[
\Omega(t) = \{ x : x' \Psi(t)^{-1} x \leq 1 \},
\]

with \( \beta > 0 \), and \( \Psi(t) \in \mathbb{R}^{n 	imes n} \) positive definite. The derivation of (5) can be found in [22], and [23]; the reader is referred to those references for extensive treatments of the use of ellipsoids in dynamic systems and control. Let \( \Upsilon \) denote the steady-state value of \( \Psi(t) \). Then, the state variables \( x \) will be contained in some set bounded by an ellipsoid \( \mathcal{E} \) defined by

\[
\mathcal{E} = \{ x : x' \Upsilon^{-1} x \leq 1 \},
\]

\[
\begin{align*}
A \Upsilon + \Upsilon A' + \beta \Upsilon + \frac{1}{\beta} B Q B' &= 0, \\
\Upsilon(t = 0) &= \Upsilon_0,
\end{align*}
\]

with \( \beta > 0 \), and \( \Upsilon \in \mathbb{R}^{n \times n} \) positive definite.

The value of \( \beta \) in (5), and (6) will determine how “tight” the bounding ellipsoid. There are several criteria to pick \( \beta \) such that the resulting bounding ellipsoid is optimal in some sense. For example, ellipsoids with minimum volume can be obtained by making \( \beta = \sqrt{\text{tr}[\Upsilon^{-1} B Q B']/n} \) [24]; ellipsoids with minimum sum of squared semi-axes can be obtained by making \( \beta = \sqrt{\text{tr}[B Q B']/\text{tr}[\Upsilon]} \) [24]; and ellipsoids with minimum projection in a given direction \( \eta \) can be obtained by making \( \beta = \sqrt{\eta' B Q B' \eta/\eta' \Upsilon \eta} \) [25].

B. System Dynamics After a First Fault

Let \( T \) be a random variable representing the time to a first fault. This fault alters the pair of matrices \( A, B \) in (3), resulting in a new pair \( \bar{A}, \bar{B}. \) Let \( \tau \) be a realization of \( T \). Then, the system state-space representation after the fault can be defined by

\[
\frac{dx(\hat{t})}{d\hat{t}} = A_{\tau}x(\hat{t}) + \bar{B}w(\hat{t}),
\]

\[
x(\hat{t} = 0) = x(t = \tau) \in \mathcal{R}(\tau),
\]

\[
w(\hat{t}) \in \Omega_w = \{ w : w'Q^{-1}w \leq 1 \},
\]

where \( \hat{t} = t - \tau \), and \( \mathcal{R}(\tau) \) is the reach set for (3) at the time of fault occurrence. Computing the reach set \( \mathcal{R}(\hat{t}) \) for (7) might be even more complicated than for (3) as not even the set of initial conditions is an ellipsoid. However, if instead of using \( \mathcal{R}(\tau) \) as the set of initial conditions, we use its bounding ellipsoid \( \Omega(\tau) \), as explained before, it is possible to obtain an ellipsoidal approximation of the reach set \( \mathcal{R}(\hat{t}) \). It is important to note that, if \( \tau \) is much larger that the largest time constant associated with (5), then \( \Omega(\tau) \equiv \mathcal{E} \). It is also important to note that, so far, we have not imposed any condition on the random variable \( T \), representing the time to a fault occurrence.

1) Performance Requirements: As stated before, in fault-free conditions, the performance requirements constrain the system trajectories to some region of the state space \( \Phi \). It is reasonable that, after a fault, the performance requirements imposed on the system might be less stringent than those requirements imposed when the system is operating with no faults. In other words, after a fault, the system could partially deliver some functionality with some degraded performance. Therefore, for the system to deliver some function (even in a degraded mode), its trajectories ought to be constrained to some other region of the state-space, denoted by \( \hat{\Phi} \), and defined by the symmetric polytope

\[
\hat{\Phi} = \{ x : |x'x| \leq 1 \forall i = 1, 2, \ldots, p \},
\]

where \( \hat{x}_i \in \mathbb{R}^n \) is a column vector.

C. Fault Coverage Definition

To define fault coverage in the context of LTI systems, it is necessary to define the notions of system failure, and system recovery. Let the dynamics of a system after a first fault be defined by (7). Let \( \Phi \) be the region of the state space defined by the dynamic performance requirements the system must meet after the fault. Then, the system fails to deliver its function if, for some \( \hat{t} > 0 \) (with \( \hat{t} = t - \tau \)), the state variables \( x \) do not remain in \( \Phi \). Thus, the system survives, and recovers from the fault if, at the time the fault occurs, the system state variables are such that the system trajectory remains at all times in the region of the state space defined by \( \Phi \).

Fig. 2 depicts the trajectories followed by a system after a fault occurrence for three different values of the state variables at the time of fault occurrence. The first trajectory \( T_1 \) represents the case where the state variables at the time of fault \( x(\hat{t} = 0) \) are such that the state variables at subsequent times remain within the set \( \Phi \). Therefore, the system survives this fault. The second trajectory \( T_2 \) represents the case where the state variables at the time of fault \( x(\hat{t} = 0) \) are in \( \Phi \), but there is some \( \hat{t} > 0 \) such that \( x(\hat{t}) \notin \Phi \). Therefore, the system does not survive this fault, even if \( x(\hat{t} = 0) \in \Phi \). Trajectory \( T_3 \) represents the case when \( x(\hat{t} = 0) \notin \Phi \). Therefore, the system does not survive this fault.

Thus, it is clear that, depending on the value of the state variables at the time of fault, the system may or may not survive a fault. Let \( \mathcal{R}(\tau) \) be the system reach set at the time of fault occurrence \( \tau \). Then, the system is guaranteed to survive a fault whenever the state variables at the time of fault occurrence are contained in some set \( \hat{\mathcal{R}}(\tau) \subseteq \mathcal{R}(\tau) \cap \Phi \), such that if \( x(t = \tau) = x(\hat{t} = 0) \in \hat{\mathcal{R}}(\tau) \), then \( x(\hat{t}) \in \Phi \) for all \( \hat{t} > 0 \). Thus, if \( \hat{\mathcal{R}}(\tau) \neq \emptyset \), then the system is guaranteed to survive the fault with probability zero. If \( \hat{\mathcal{R}}(\tau) \neq \emptyset \), then the system is guaranteed to survive the fault with probability greater than zero. The definition of fault coverage follows from these ideas.

1) Definition: Let \( T \) be a random variable representing the time to a first fault. Let \( X(T) \) be a random variable representing...
the system state variables at the time of fault occurrence. Let \( \hat{\Theta}(\tau) \) be the largest set contained in \( \mathcal{R}(\tau) \cap \hat{\Phi} \) such that, if \( x(t = \tau) = x(\ell) = 0 \in \hat{\Theta}(\tau) \), then \( x(\ell) \in \hat{\Phi} \) for all \( \ell > 0 \). Then, for any \( \ell > 0 \), fault coverage is defined by

\[
C = Pr \left\{ X(T) \in \hat{\Theta}(T) \middle| T < \ell \right\}.
\]

(9)

D. Fault Coverage Estimation

There are three issues that make difficult the exact computation of fault coverage as defined in (9). First, it is necessary to obtain the probability distribution of the state variables \( X(T) \) over the reach set \( \mathcal{R}(T) \). Second, it is necessary to obtain the exact shape of the set \( \hat{\Theta}(\tau) \). Third, it is necessary to know the probability distribution of the time to fault occurrence \( T \). Even if all the above are solved, the dependence of the distribution of \( X(T) \), and the shape of the set \( \hat{\Theta}(T) \) on the distribution of \( T \) makes the exact computation of fault coverage still a hard problem. In the remainder of this section, we will address these issues, and propose a method to obtain an estimate of (9).

1) Dependence of the Distribution of \( X(T) \), and the Shape of the Set \( \hat{\Theta}(T) \) on the Distribution of \( T \): We assume the time constants associated with the system dynamics are much smaller than the time constants associated with fault occurrences (behavioral decomposition). This assumption allows us to simplify the computation of an estimate of (9).

Let \( f_T(\tau) \) represent the probability density function of \( T \), and \( f_{X|T}(x|\tau) \) the probability density function of \( X(T) \). Then, (9) can be rewritten as

\[
C = \frac{Pr \left\{ T < t, X(T) \in \hat{\Theta}(T) \right\}}{Pr\{T < t\}},
\]

(10)

where

\[
Pr \left\{ T < t, X(T) \in \hat{\Theta}(T) \right\} = \int_0^t \int_{x(\tau) \in \hat{\Theta}(\tau)} f_{X|T}(x|\tau) f_T(\tau) dx d\tau.
\]

(11)

If the distribution of \( w \) over \( \Omega_w \) is stationary, and the system is stable, then \( \mathcal{R}(\tau) \) will reach some steady-state, and so will \( \hat{\Theta}(\tau) \). Let \( \hat{\Theta}_{ss} \) be the steady-state value of \( \hat{\Theta}(\tau) \), and \( \ell = t_{ss} \) be much larger than the largest time constant associated with (5). Then, we can rewrite (11) as

\[
\int_0^{t_{ss}} \int_{x(\tau) \in \hat{\Theta}(\tau)} f_{X|T}(x|\tau) f_T(\tau) dx d\tau + \int_{t_{ss}}^t \int_{x(t_{ss}) \in \hat{\Theta}_{ss}} f_{X|T}(x|t_{ss}) f_T(\tau) dx d\tau.
\]

(12)

The generalized mean value theorem for integrals allows us to rewrite (12) as

\[
\int_0^{t_{ss}} f_T(\tau) d\tau \int_{x(\xi) \in \hat{\Theta}(\xi)} f_{X|T}(x|\xi) dx + \int_{t_{ss}}^t f_T(\tau) d\tau \int_{x(t_{ss}) \in \hat{\Theta}_{ss}} f_{X|T}(x|t_{ss}) dx.
\]

(13)

This result is reasonable for certain classes of systems, such as aerospace systems, automotive systems, or power systems, where the system dynamics time constants are on the order of seconds; while for example, assuming Poisson distributed faults, typical fault rates for reasonably reliable systems are on the order of \( 10^{-5} \) to \( 10^{-9} \) per hour. Then, by combining (13), and (14), it results that

\[
Pr \left\{ T < t, X(T) \in \hat{\Theta}(T) \right\} \approx \int_0^{t_{ss}} f_T(\tau) d\tau \int_{x(t_{ss}) \in \hat{\Theta}_{ss}} f_{X|T}(x|t_{ss}) dx + \int_{t_{ss}}^t f_T(\tau) d\tau \int_{x(t_{ss}) \in \hat{\Theta}_{ss}} f_{X|T}(x|t_{ss}) dx.
\]

(14)

By combining (10), and (15), it follows that

\[
C \approx \int_{x(t_{ss}) \in \hat{\Theta}_{ss}} f_{X|T}(x|t_{ss}) dx.
\]

(16)

2) Obtaining the Set \( \hat{\Theta}_{ss} \): As stated before, \( \hat{\Theta}_{ss} \) is the steady-state value of the largest set \( \hat{\Theta}(\tau) \subseteq \mathcal{R}(\tau) \cap \hat{\Phi} \) such that if \( x(\tau) \in \hat{\Theta}_{ss} \), then \( x(\ell) \in \hat{\Phi} \) for all \( \ell > 0 \). Because \( \mathcal{R}(\tau) \) is difficult to compute, so is \( \hat{\Theta}(\tau) \), thus precluding the possibility of computing the estimate of the fault coverage as defined in (16). It is possible, though, to obtain a lower bound on the fault coverage estimate by using the ellipsoidal approximation of the steady-state value of \( \mathcal{R}(\tau) \) defined in (6), and denoted by \( \hat{\mathcal{E}} \); and compute, instead of \( \hat{\Theta}_{ss} \), the largest (in some sense) ellipsoid \( \hat{\mathcal{E}} \subseteq \mathcal{E} \cap \hat{\Phi} \) such that if \( x(\tau) \in \hat{\mathcal{E}} \), then \( x(\ell) \in \hat{\Phi} \) for all \( \ell > 0 \). This can be accomplished by first obtaining the largest (in some sense) invariant ellipsoid \( \hat{\mathcal{X}} \) with respect to (7) contained in \( \hat{\Phi} \); and then by obtaining \( \hat{\mathcal{E}} \) as the largest (in some sense) ellipsoid contained in the intersection of \( \hat{\mathcal{E}} \), and \( \hat{\mathcal{X}} \). For a two-dimensional system, a graphical interpretation of \( \hat{\mathcal{E}}, \hat{\Phi}, \hat{\Theta}_{ss}, \hat{\mathcal{X}}, \) and \( \hat{\mathcal{E}} \) is shown in Fig. 3.

We measure ellipsoid largeness in terms of its content (other criteria can be used as explained in Section II-A). Let \( \hat{\mathcal{P}} = \{x : x^T \hat{M}^{-1} x \leq 1 \} \) be the smallest invariant ellipsoid with respect to
(7), i.e., any trajectory with initial conditions in \( \tilde{P} \) remains in \( \tilde{P} \) at all times [26]. Then
\[
\dot{\tilde{\Phi}} + \hat{\alpha} \tilde{\Phi} + \frac{1}{\hat{\alpha}} \tilde{B}Q\tilde{B}' = 0,
\]
with \( \hat{\alpha} \in \mathbb{R}^{m \times n} \) positive definite [24]. Let \( \pi_i \in \mathbb{R}^p \) be the \( i \) vector that defines \( \tilde{\Phi} \) in (8). Then, if \( \pi_i^T \pi_i \geq 1 \) for some \( i = 1, 2, \ldots, p \), it follows that \( \tilde{P} \subseteq \tilde{\Phi} \), and therefore \( \tilde{\mathcal{X}} \equiv \tilde{\Omega}_{ss} \equiv \emptyset \), which results in the fault coverage being 0.

Now assume \( \tilde{P} \neq \emptyset \), and let \( \tilde{\mathcal{X}} = \{ x : x^T \tilde{\Gamma}^{-1} x \leq 1 \} \) be the largest invariant ellipsoid with respect to (7) contained in \( \tilde{\Phi} \). Then, because in an \( n \)-dimensional space the content of an ellipsoid is proportional to the square root of the determinant of the positive-definite matrix defining the ellipsoid [27], \( \tilde{\mathcal{X}} \) can be obtained by solving the following optimization problem.

\[
\text{maximize} \quad \det \tilde{\mathcal{X}} \quad \text{(18)}
\]
\[
\text{subject to} \quad \pi_i^T \tilde{\pi}_i \leq 1, \quad \forall i = 1, 2, \ldots, p \quad \text{(19)}
\]
\[
\frac{1}{\hat{\alpha}} \tilde{\mathcal{X}} + \tilde{\mathcal{X}} \hat{\alpha} + \hat{\alpha} \tilde{\Phi} + \frac{1}{\hat{\alpha}} \tilde{B}Q\tilde{B}' \leq 0, \quad \text{(20)}
\]

in the variable \( \tilde{\mathcal{X}} \) with implicit constraint \( \tilde{\mathcal{X}} \) positive definite, where \( \hat{\alpha} \) is the parameter that defines \( \tilde{\mathcal{P}} \) in (17), and where “\( \leq \)” in (20) means that the left hand side of the inequality is negative-semidefinite. As explained in [28], this optimization problem can be cast into a convex optimization problem, which is tractable from theoretical, and practical points of view [29], [30]. The constraint given by (19) imposes that the projection of the ellipsoid \( \tilde{\mathcal{X}} \) in the direction of \( \pi_i \) lies within the requirements imposed on \( x_i \) by (8), from where it follows that, if \( \tilde{\mathcal{X}} \) exits, it is contained in \( \tilde{\Phi} \) [29]. The constraint given by (20) ensures that, if \( \tilde{\mathcal{X}} \) exits, it is invariant with respect to (7), i.e., any trajectory with initial conditions in \( \tilde{\mathcal{X}} \) remains in \( \tilde{\mathcal{X}} \) at all times [26].

Let \( \tilde{E} = \{ x : x^T \tilde{\Gamma}^{-1} x \leq 1 \} \). As before, we measure the largeness of \( \tilde{E} \) in terms of its content. Then, \( \tilde{\mathcal{E}} \) can be obtained by solving another optimization problem given by

\[
\text{maximize} \quad \det \tilde{\mathcal{E}} \quad \text{(21)}
\]
\[
\text{subject to} \quad \tilde{\mathcal{E}} - \mathcal{E} \leq 0, \quad \text{(22)}
\]
\[
\tilde{\mathcal{E}} - \tilde{\mathcal{E}} \leq 0, \quad \text{(23)}
\]

in the variables \( \tilde{\mathcal{E}} \) with implicit constraint \( \tilde{\mathcal{E}} \) positive definite, which can also be casted into a convex optimization problem as explained in [29]. The constraint given by (22) ensures that, if \( \tilde{\mathcal{E}} \) exists, it is contained in \( \tilde{\mathcal{E}} \); and the constraint given by (23) ensures that, if \( \tilde{\mathcal{E}} \) exits, it is contained in \( \tilde{\mathcal{X}} \) [29]. Then, if \( \tilde{\mathcal{E}} \) exists, it is contained in the intersection of \( \mathcal{E} \) and \( \tilde{\mathcal{X}} \), and as a result, a lower bound on the fault coverage is given by

\[
c = \int_{x(t_w) \in \tilde{\mathcal{E}}} f_{X|T}(x|t_{ss})dt_w. \quad \text{(24)}
\]

3) Obtaining the Probability Density Function of \( X(T) \): The probability density function of \( X(T) \) will depend on the time structure of the system input, and its distribution over the set \( \Omega_w \). There are systems in which these are completely known. In these cases, it is possible to obtain the probability density function of \( X(T) \). For example, in the RL circuit example of Fig. 1 described by
\[
\frac{di(t)}{dt} = -\frac{R}{L} i(t) + \frac{1}{L} v(t), \quad i(0) = -\frac{V}{R}, \quad \text{(25)}
\]
we assume that the input \( v(t) \) is a square signal with amplitude \( V \), and period much larger than the time circuit constant \( L/R \). Then, it is clear that if we pick a time at random, the input \( v(t) \) can be regarded also as random, taking values \( V \) and \( -V \) with equal probability 1/2. In this case, it is easy to obtain the distribution of \( X(T) \).

There might be other systems in which there is partial information about the time structure of the input, but the distribution of the magnitude of the system input is completely characterized. For example, in (25), we assume that the magnitude of the voltage \( v(t) \) can take any value in the interval \([-V, V]\) with equal probability. Once \( v(t) \) takes a value in \([-V, V]\), it remains constant for an uncertain period of time much larger than the time constant \( L/R \) before randomly changing to another value in \([-V, V]\), in which it remains for an uncertain period of time until \( v(t) \) changes again. This example can be generalized to an \( n \)-dimensional system, where the time structure of the input, and the matrices \( A \) and \( B \) are such that the time distribution of the states over the ellipsoid \( \mathcal{E} \) can be assumed to be approximately uniform. This is the case when the following conditions hold: 1) although not completely characterized, the time-structure of \( w(t) \) is quasi-static with respect to the system dynamics, i.e., the timeframe for changes in the value of the input \( w(t) \) is much larger that the time constants of the system; 2) the operator defined by \( A^{-1}B \) is full-column rank; 3) the random vector associated with the input \( W \) is uniformly distributed over \( \Omega_w \). Condition 1) ensures that the state variables are in steady-state most of the time (except for short periods of time after a jump in the system input). Condition 2) ensures that there is a one-to-one mapping between the state variables steady-state values, and system inputs when these are assumed to be constant. Thus, by assuming condition 1) holds, and applying results on convergence of random variables [31], it can be shown that the distribution of \( X \) converges to the steady-state distribution obtained by the transformation \( X = A^{-1}BU \). Now, because conditions 2) and 3) hold, by applying results on transformation of random variables [31], the density function of \( X \) is just a scaled version of the (uniform) density function of \( W \). Then, for this special case, the coverage estimate \( c \) can be expressed as
\[
c = \frac{\text{cont}(\mathcal{E})}{\text{cont}(\tilde{\mathcal{E}})} = \sqrt{\frac{\det(\tilde{\mathcal{Y}})}{\det(\tilde{\mathcal{Y}})}}. \quad \text{(26)}
\]
There might be other systems where we only have information about a few moments of $W(t)$. For example, assume $W(t)$ is a second-order process (bounded second moment), and we know its mean and covariance. Then, the mean of $X(t)$ is obtained by convolving the mean of $W(t)$ with the impulse response of the system (defined by the matrices $A$ and $B$), and the covariance is obtained by convolving twice the covariance of $W(t)$ with the impulse response of the system [32]. Because only the first two moments of the probability density function of $X(t)$ are available, it is not possible to compute an estimate of the fault coverage as defined in (24). In this case, it is possible to upper bound the integral in (24) by using the Chebyshev inequality generalized to the $n$-dimensional case [33], [34]. Caution must be taken in this case as over-estimates of the fault coverage would be obtained. A way around this problem is to compute an upper bound of $1 - c$, which would arise from changing the integration domain in (24) from $\mathcal{E}$ to $\mathcal{E} \cap \mathcal{E}^c$.

III. A FIRST-ORDER SYSTEM EXAMPLE

The purpose of this section is to illustrate the concepts introduced in Section II. Consider the series RL circuit displayed in Fig. 4, and assume the following.

(a) The initial current $i(0)$ flowing through the circuit is unknown, but it is such that $|i(0)| = I$, with $I > 0$.

(b) The voltage source $v(t)$ is unknown, but it is such that $|v(t)| \leq V$, with $V > 0$.

(c) The maximum currents that resistors $R_1$, and $R_2$ can process are $i_{\text{max}}^{R_1}$ and $i_{\text{max}}^{R_2}$, respectively; and once this current is reached, the resistor fails open.

(d) The values of $V$, $R_1$, $R_2$, $i_{\text{max}}^{R_1}$, and $i_{\text{max}}^{R_2}$ are such that $V/R_1 < i_{\text{max}}^{R_1}$ and $V/R_2 < i_{\text{max}}^{R_2}$.

(e) The only faults considered are caused by the resistors failing open.

(f) The time to a fault occurrence in the resistors $R_1$, and $R_2$ is exponentially distributed with rates $\lambda_{R_1}$, and $\lambda_{R_2}$ respectively.

(g) The system fails with probability 1 if both resistors fail.

A. Fault-Free System Dynamics

Before any fault occurrence, the current $i(t)$ is governed by

$$\frac{di(t)}{dt} = -\frac{R_{\text{eq}}}{L}i(t) + \frac{1}{L}v(t),$$

$$i(t = 0) \in \omega_i = \{i : |i| \leq I\},$$

$$v(t) \in \omega_v = \{v : |v| \leq V\}.$$  \(27\)

where $R_{\text{eq}} = (R_1R_2)/(R_1 + R_2)$. Let $\omega(t) = \{i : \gamma(t) \leq 1\}$ be an interval in $\mathbb{R}$ that contains all possible current for $t > 0$, where $\gamma(t)$ can be computed by solving

$$\frac{d\gamma(t)}{dt} = -2\frac{R_{\text{eq}}}{L}\gamma(t) + \beta\gamma(t) + \frac{1}{\beta I^2}V^2,$$

$$\gamma(0) = I^2,$$  \(28\)

with $\gamma(t) \geq 0$, and $\beta > 0$ [22]. By taking $\beta = R_{\text{eq}}/L$, which is the value that minimizes $\gamma(\infty)$, the solution to (28) is

$$\gamma(t) = \left(\frac{V}{R_{\text{eq}}}\right)^2 + \left(I^2 - \left(\frac{V}{R_{\text{eq}}}\right)^2\right)e^{-\frac{R_{\text{eq}}}{L}t},$$  \(29\)

and the steady-state value of $\gamma(t)$ is given by

$$\gamma(\infty) = \left(\frac{V}{R_{\text{eq}}}\right)^2.$$  \(30\)

Thus, the steady-state set of $\omega(t)$, denoted by $\varepsilon$, is given by

$$\varepsilon = \left\{i : |i| \leq \frac{V}{R_{\text{eq}}}\right\}.$$  \(31\)

Fig. 5 represents, for $I < (V/R_{\text{eq}})$, the evolution of the interval bounding the current flowing through the circuit.

B. System Dynamics After a Resistor Failure

Let $\tau$ be the time at which a fault occurs, causing resistor $R_1$ to fail open circuit. Assume $\tau$ is large enough so the steady-state value of $\omega(t)$ has been reached. The current flowing through the circuit is governed by

$$\frac{di(\hat{t})}{d\hat{t}} = -\frac{R_2}{L}i(\hat{t}) + \frac{1}{L}v(\hat{t}),$$

$$i(\hat{t} = 0) \in \varepsilon = \left\{i : |i| \leq \frac{V}{R_{\text{eq}}}\right\},$$

$$v(\hat{t}) \in \omega_v = \{v : |v| \leq V\}.$$  \(32\)

where $\hat{t} = t - \tau$.

C. Fault Coverage

As stated in Section II-D, if we assume that the random variable $V$ associated with the input voltage is uniformly distributed over $\omega_v$, and assume that the voltage $v(t)$ is quasi-static with respect to the circuit dynamics, it is reasonable to assume that the random variable $I(T)$ associated with the current at the time of fault is uniformly distributed over $\gamma(T)$.

From assumption c), it is clear that the maximum current that can flow through the circuit after the fault of resistor $R_1$ is limited by $i_{\text{max}}^{R_2}$, which is the maximum current allowed through $R_2$. By assumptions c) and g), a system failure occurs if, for some $\hat{t} > 0$, $i(\hat{t}) \notin \phi$, where $\phi = \{i(\hat{t}) : |i(\hat{t})| \leq i_{\text{max}}^{R_2}\}$.
A. Fault Coverage After \( k \geq 1 \) Faults

Assume that the system survives, with probability greater than one, a unique sequence of \( k - 1 \) faults, denoted by \([j, k-1]\) where \( k \geq 2 \). Let \([i, k]\) be a sequence of \( k \) faults originating from \([j, k-1]\) after an additional fault occurrence. Let \( T_{i,j,k}^{\text{f}} \) be a random variable that represents the time elapsed between the last fault of the sequence \([j, k-1]\), and the next fault occurrence leading to sequence \([i, k]\). Let \( t_{i,k}^{\text{f}} \) be a realization of \( T_{i,j,k}^{\text{f}} \). Then the system dynamics after the \([i, k]\) fault is defined by

\[
\begin{align*}
\frac{dx(t_{i,k}^{\text{f}})}{dt} & = A_{i,k} x + B_{i,k} w, \\
x(t_{i,k}^{\text{f}} = 0) & \in \mathcal{E}_{j,k-1} = \\{x : x' (Y_{j,k-1})^{-1} x \leq 1\}, \\
w & \in \mathcal{W} = \{w : w'Q^{-1}w \leq 1\},
\end{align*}
\]

where \( t_{i,k}^{\text{f}} = t_{i,j,k}^{\text{f}} - t_{j,k-1}^{\text{f}} \). The existence of the ellipsoid \( \mathcal{E}_{j,k-1} \) is ensured by the assumption that the system survived, with probability greater than one, each of the previous \( k - 1 \) faults in the sequence \([j, k-1]\).

Let the symmetric polytope \( \Phi_{i,k} \) be defined as \( \{x : \|a_{i,k}^T x\|_1 \leq 1, \ l = 1, 2, \ldots, p\} \). Define the region of the state space where the system state variables \( x \) must remain at all times for the system to fulfill its intended function. Then, if the system survives the additional fault after surviving the previous \( k - 1 \) fault with probability greater than one, there exists \( \Xi_{i,k} \in \mathbb{R}^{n \times p} \) positive definite such that

\[
\begin{align*}
A_{i,k}^{\text{f}} \Xi_{i,k} & + \Xi_{i,k} (A_{i,k}^{\text{f}})^T + \frac{1}{n} \text{tr} \left( (T_{i,k}^{\text{f}})^{-1} B_{i,k} Q B_{i,k}^T \right) \Xi_{i,k} \\
& + \sqrt{\text{tr}\left((T_{i,k}^{\text{f}})^{-1} B_{i,k} Q B_{i,k}^T\right)} \Xi_{i,k} \leq 0, \\
(\pi_{i,k}^l)^T \Xi_{i,k} (\pi_{i,k}^l) & \leq 1, \ \forall l = 1, 2, \ldots, p.
\end{align*}
\]

IV. GENERALIZED FAULT COVERAGE ESTIMATE FORMULATION

The method for estimating fault coverage presented in Section II-D is generalized to the case where a system survived a sequence of \( k - 1 \) faults, with \( k \geq 2 \), and then an additional fault \( k \) occurs. It is assumed that the likelihood of two fault occurrences within a time on the order of the system dynamic time constants is negligible relative to the likelihood of just one fault occurrence, which is a generalization of the behavioral decomposition assumption already discussed. In Section II, the symbol "**A**" was used in the formulation of the system dynamics after any first fault occurrence. In this section, we will use a double index notation \([i, k]\), where \( i \) indexes every unique sequence of faults of size \( k \) (number of fault occurrences).
in the variables $\mathcal{Y}_t$ with implicit constraint $\mathcal{Y}_t$ positive definite. Then a lower bound on the fault coverage probability after the $k$ fault occurrence can be obtained by computing

$$c_{tk}^j \triangleq \int_{x \in \mathcal{E}_t} f_x \mathcal{X}_t^j (x) dx.$$  \hspace{1cm} (46)

V. MARKOV RELIABILITY MODEL FORMULATION

We include the generalized fault coverage estimate presented in Section IV in the formulation of a Markov reliability model. Let’s assume that the system was operating with no fault at $t = 0$. Then, at any time $t \geq 0$, the system survived a sequence of $k = 1$ faults, denoted by $[j, k]$, with a probability denoted by $p_{2j-1,k}(t)$. Let an additional fault occur, leading to the sequences of faults $[i,j, k]$. Let $p_{2j,i,k}(t)$ be the probability that, at any time $t \geq 0$, the system survived the $[i,j, k]$ sequence of faults; and let $p_{2j,k}(t)$ denote the probability that, at any time $t \geq 0$, the system did not survive the $[i,j, k]$ sequence of faults. Then

$$d \bigg[ p_{2j-1,k}(t), p_{2j,k}(t) \bigg] = \left[ p_{2j-1,k-1}, p_{2j-1,k} \right] \times
$$

$$\times \begin{bmatrix}
\lambda_{i,j,k}^1 \lambda_{i,j,k}^{k-1} & (1 - \lambda_{i,j,k}^1) \lambda_{i,j,k}^{k-1} \\
-\sum_{N_k} N_k & 0
\end{bmatrix},$$  \hspace{1cm} (47)

where $\lambda_{i,j,k}^1$ is the rate at which the last fault occurs in the sequence $[i,j, k]$. \lambda_{i,j,k}^{m+1} is the rate at which a particular fault will occur next, and $N_k$ is the number of possible faults that can occur after the last fault in the sequence $[i,j, k]$. Each sequence of faults will generate a block similar to the one in (47). By assembling all these blocks, the state-transition matrix $A$ associated with the Markov reliability model is obtained. Let $P(t)$ be the fault sequences’ probability vector, obtained by assembling the individual fault sequence probabilities, then

$$\frac{dP(t)}{dt} = P(t)A, \hspace{1cm} P(0) = \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 \end{bmatrix}.$$  \hspace{1cm} (48)

It is important to note that even if the sum of the entries in each row of the 2×2 matrix in (47) do not add up to zero, after all the blocks have been assembled, the sum of entries in each row of the resulting matrix $A$ will indeed add up to zero, which is an important property of continuous-time discrete-space Markov chains.

A. Markov Model for the First-Order System Example

We will complete the RL circuit example discussed in Section III by formulating its Markov reliability model. The analysis is constrained to the effect on the current flowing through the inductor caused by faults in the resistors. The fault coverage after a fault caused by resistor $R_1$ is given in (37), and a similar calculation for $R_2$ yields $c_{R_1} = \frac{R_2}{\max(R_{eq}/V)}$, and $c_{R_2} = \frac{R_1}{\max(R_{eq}/V)}$.

Given that at time $t = 0$ no faults have occurred yet, let’s define the following probabilities at time $t$:

- the probability that no faults have occurred is $p_{1,0}(t)$;
- the probability that the circuit survived a fault in resistor $R_1$ is $p_{1,1}(t)$;
- the probability that the circuit did not survive a fault in resistor $R_1$ is $p_{2,1}(t)$;
- the probability that the circuit survived a fault in resistor $R_2$ is $p_{3,1}(t)$;
- the probability that the circuit did not survive a fault in resistor $R_2$ is $p_{4,1}(t)$;
- the probability that the circuit did not survive a sequence of faults in $R_1$, and $R_2$ in that order is $p_{2,2}(t)$;
- the probability that the circuit did not survive a sequence of faults in $R_2$, and $R_1$ in that order is $p_{4,2}(t)$.

Then, following the notation of (48), it results that $P(t) = \begin{bmatrix} 1, 0, 0, 0, 0, 0, 0, 0 \end{bmatrix}$. The non-zero elements of the matrix $A$ are $[A]_{i1} = -\lambda_{R_1} - \lambda_{R_2}$, $[A]_{12} = \frac{R_2}{\max(R_{eq}/V)} \lambda_{R_1}$, $[A]_{13} = (1 - \frac{R_2}{\max(R_{eq}/V)} \lambda_{R_1})$, $[A]_{14} = \frac{R_1}{\max(R_{eq}/V)} \lambda_{R_2}$, $[A]_{15} = (1 - \frac{R_1}{\max(R_{eq}/V)} \lambda_{R_2})$, $[A]_{22} = -\lambda_{R_2}$, $[A]_{26} = -\lambda_{R_1}$, $[A]_{44} = -\lambda_{R_1}$, and $[A]_{47} = \lambda_{R_1}$.

Note that the Markov reliability model is not only formulated in terms of the rates at which faults occur, $\lambda_{R_1}$ and $\lambda_{R_2}$, but also in terms of physical parameters of the system, the maximum currents that can flow through the resistors, and the maximum amplitude $V$ of the voltage driving the circuit.

VI. DC POWER DISTRIBUTION SYSTEM CASE-STUDY

We apply the proposed fault coverage model to analyze the reliability of the DC network displayed in Fig. 7, which is an abstraction of a distributed DC power system for telecommunications applications [35]. The purpose of this system is to reliably provide power to two loads, represented by resistors $R_{1}$, and $R_{2}$, maintaining their voltage within some tolerance around some nominal values $V_{1}$, and $V_{2}$ respectively. These loads could correspond to clusters of telephone switches, or computer servers in a telecommunications center. To ensure fault-tolerant operation, each load is connected directly to its own power source, and indirectly connected to the power source of the other load through a double redundant link between buses 1, and 2.

Each power source is modeled as a three series voltage sources, where the first voltage source $V_{1}(DC)$ is constant, and represents the nominal input voltage; the second one $V_{2}(DC)$ represents uncontrollable variations in the input voltage; and the third one $\tilde{v}_{2}(DC)$ represents controlled variations in the input voltage. Let the system states be $i_{1}(t) = i_{1}(t) + \tilde{i}_{1}(t)$, and $v_{1}(t) = V_{1}(DC) + \tilde{v}_{1}(t)$, where capitalized variables represent the state variables behavior due to the constant input voltages $V_{1}(DC)$, and variables with tilde represent the state variables behavior due to uncontrollable variations in the input voltage $V_{1}(DC)$. Because the system is linear, the behavior of capitalized variables can be analyzed separately, and only results in a shifting of the center of the ellipsoids bounding the behavior of the variables with tilde [22].

With this in mind, we focus the subsequent analysis on the effect of uncontrollable variations in the input voltage $V_{1}(DC)$ on $i_{1}(t)$, and $\tilde{v}_{1}(t)$. We assume that the quasi-static assumption explained in Section II-D holds. Controlled variations in the input voltage $\tilde{v}_{1}(t)$ are specified by a constant-gain feedback control law of...
the form \( \vec{v}_1 = k_{11} \vec{\gamma}_1 + k_{13} \vec{\gamma}_2 + k_{14} \vec{\gamma}_2 \), where \( \vec{\gamma}_1 \) is measured by sensor \( S_{11} \), \( \vec{\gamma}_2 \) is measured by sensor \( S_{12} \), and \( \vec{\gamma}_2 \) is measured by sensor \( S_{12} \). And \( \vec{v}_2 = k_{22} \vec{\gamma}_2 + k_{23} \vec{\gamma}_1 + k_{24} \vec{\gamma}_2 \), where \( \vec{\gamma}_1 \) is measured by sensor \( S_{12} \), \( \vec{\gamma}_1 \) is measured by sensor \( S_{11} \), and \( \vec{\gamma}_2 \) is measured by sensor \( S_{12} \).

A. Fault-Free Network Dynamics

Let \( \vec{x} = [\vec{\gamma}_1, \vec{\gamma}_2, \vec{\gamma}_1, \vec{\gamma}_2]^T \), and \( \vec{w} = [V_1, V_2]^T \). Then, it follows that

\[
\dot{\vec{x}} = A \vec{x} + B \vec{w},
\]

\[
V \in \Omega_V = \{ V : V'Q^{-1}V \leq 1 \},
\]

\[
\Delta(0) = [0, 0, 0, 0]^T,
\]

and the equation shown at the bottom of the page with the parameters of \( A, B, \) and \( Q \) taking the values in Table I. In this case, we assume the initial conditions to be known, and equal to 0. We impose that variations around the nominal values must remain within the “box-shaped” symmetrical polytope described by

\[
\Phi = \{ \vec{x} : |x_i| \leq \pi_i, i = 1, 2, 3, 4 \}, \quad (50)
\]

where \( \pi_1 = [1.66 \cdot 10^{-3}, 0, 0, 0]^T \), \( \pi_2 = [0, 0, 0, 0, 0]^T \), \( \pi_3 = [0, 0, 0, 0]^T \), and \( \pi_4 = [0, 0, 0, 0]^T \).

By using (6), we can compute the positive definite matrix \( \Sigma \) defining the ellipsoid \( \mathcal{E} \) that bounds \( \vec{\gamma}_1, \vec{\gamma}_2, \vec{\gamma}_1, \) and \( \vec{\gamma}_2 \). To solve (6), we consider a minimum volume criterion, which results in \( \beta = 1.45 \cdot 10^3 \), with the entries of \( \Sigma \), and its determinant taking the values in Table II. To visualize this 4-dimensional ellipsoid, we project it on to the subspaces defined by the \( \vec{\gamma}_1, \vec{\gamma}_2 \) axes, and the \( \vec{\gamma}_1, \vec{\gamma}_2 \) axes; and denote these projections as \( \Pi_T(\mathcal{E}) \), and \( \Pi_E(\mathcal{E}) \) respectively. Fig. 8 shows \( \Pi_T(\mathcal{E}) \), and \( \Pi_E(\Phi) \), where it can be seen that both projections are contained within the corresponding projections \( \Pi_T(\Phi) \), and \( \Pi_E(\Phi) \) of \( \Phi \) defined by (50).

\[
A = \begin{bmatrix}
-(R_1 - k_{11}) / L_1 & 0 & -(1 - k_{13}) / L_1 & k_{14} / L_2 \\
0 & -(R_2 - k_{22}) / L_2 & -(1 - k_{23}) / L_2 & -(1 - k_{24}) / L_2 \\
1 / C_1 & 0 & (1 / R_3 + 1 / R_4 + 1 / R_1) / C_1 & (1 / R_3 + 1 / R_4 + 1 / R_2) / C_1 \\
0 & 1 / C_2 & (1 / R_3 + 1 / R_4) / C_2 & (1 / R_3 + 1 / R_4 + 1 / R_2) / C_2
\end{bmatrix},
\]

\[
B = \begin{bmatrix}
1 / L_1 & 0 & 0 & 0 \\
0 & 1 / L_2 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix}, \quad Q = \begin{bmatrix} q_{11} & 0 & 0 & q_{22} \end{bmatrix},
\]
B. Network Dynamics After One Fault

We consider the effect on the system dynamics of the following single faults:

- an open circuit in one of the links $R_3$, and $R_4$ between buses 1 and 2;
- a 50% capacitance drop due to electrolyte degradation in one of the capacitors $C_1$, or $C_2$;
- an output omission in one of the current sensors $S_{i1}$, or $S_{i2}$;
- an output omission in one of the voltage sensors $S_{v1}$, $S_{v2}$, $S_{v3}$, or $S_{v2}$.

The second column of Table III shows the effects of each fault on the parameters of $A$, and $B$. We impose the same requirements on variations around nominal values of the state variables, i.e., $\Phi \equiv \Phi$. To compute fault coverage, we first solve (17), for which we use MATLAB. Then we solve the two convex optimization problems defined by (18)–(20), and by (21)–(23) respectively. To solve these problems, we use CVX, a package for solving convex programs in MATLAB [30], [36].

For faults in the current sensors $S_{i1}$, $S_{i2}$, and in the voltage sensors $S_{v1}$, $S_{v2}$, the smallest invariant ellipsoid with respect to the post-fault dynamics, defined by the solution of (17), failed to be fully contained in the region $\Phi$ (equivalent to $\Phi$ in this case). Therefore, the fault coverage for these faults is 0 as shown in the fourth column of Table III. For faults in $R_3$ and $R_4$, the capacitors $C_1$ and $C_2$, and $S_{v1}$ and $S_{v2}$, the solution of (17) yields an ellipsoid fully contained in $\Phi$. Therefore, there exists a solution to (18)–(20), and (21)–(23). For each particular fault, the entries of the matrix $\Xi$ obtained from (18)–(20) take the values in Table IV, and the entries of the corresponding matrix $\hat{\Xi}$ that results from the second convex optimization problem (21)–(23) are collected in Table V. The fault coverage (we assume the quasi-static assumption holds) is given by the square root of the ratio of the determinant of $\hat{\Xi}$ (fourth column of Table III), and the determinant of $\Xi$ (first column of Table II).

In all Tables III–V, following the notation used in Section IV, we replace "\&" by a double index when referring to each particular $\Xi$ and $\hat{\Xi}$. For the case when one of the links between buses 1 and 2 fails, Fig. 9 shows the projections of the ellipsoids $E_1$, $E_2$, and $E_3$ on to the subspaces defined by the $\hat{\Gamma}_1$, $\hat{\Gamma}_2$ axes, and the $\hat{\Gamma}_1$, $\hat{\Gamma}_2$, axes. These projections are denoted by $\Pi_1(\hat{\Xi})$, $\Pi_2(\hat{\Xi}(2),1)$, $\Pi_3(\hat{\Xi}(2),1)$, and $\Pi_6(\Xi)$. $\Pi_6(\Xi(2),1)$, $\Pi_6(\hat{\Xi}(2),1)$ respectively.

![Diagram](image1.png)

**Fig. 8.** DC power system dynamic behavior before any fault occurrence; (a) projections of $E$ and $\Phi$ on to the subspace defined by $\hat{\tau}_1$, $\hat{\tau}_2$; (b) projections of $E$ and $\Phi$ on to the subspace defined by $\hat{\tau}_1$, $\hat{\tau}_2$.

![Diagram](image2.png)

**Fig. 9.** DC power system dynamic behavior after an open-circuit fault in $R_3$, or $R_4$: (a) projections of $E$, $E^{1(2),1}$, $E^{1(2),1}$, and $\Phi^{1(2),1}$ on to the subspace defined by $\hat{\tau}_1$, $\hat{\tau}_2$; (b) projections of $E$, $E^{1(2),1}$, $E^{1(2),1}$, and $\Phi^{1(2),1}$ on to the subspace defined by $\hat{\tau}_1$, $\hat{\tau}_2$.

**TABLE III**

<table>
<thead>
<tr>
<th>Component</th>
<th>Fault effect</th>
<th>Index</th>
<th>det($\hat{\Xi}$)</th>
<th>Fault Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R_{3(4)}$</td>
<td>$R_{3(4)} = \infty$</td>
<td>[1(2),1]</td>
<td>$1.22 \cdot 10^5$</td>
<td>$c_r = 0.94$</td>
</tr>
<tr>
<td>$C_{1(2)}$</td>
<td>$C_{1(2)}/2$</td>
<td>[3(4),1]</td>
<td>$7.67 \cdot 10^4$</td>
<td>$c_c = 0.74$</td>
</tr>
<tr>
<td>$S_{v1}^{1,1}$</td>
<td>$k_{1(2)} = 0$</td>
<td>[5(6),1]</td>
<td>$1.23 \cdot 10^5$</td>
<td>$c_r = 0.95$</td>
</tr>
<tr>
<td>$S_{i1}^{1,1}$</td>
<td>$k_{1(2)} = 0$</td>
<td>nil</td>
<td>nil</td>
<td>0</td>
</tr>
<tr>
<td>$S_{v1}^{1,1}$</td>
<td>$k_{1(2)} = 0$</td>
<td>nil</td>
<td>nil</td>
<td>0</td>
</tr>
</tbody>
</table>
TABLE IV
SINGLE FAULT CONDITIONS; ENTRIES OF THE MATRIX $\Xi^{i,4}$, WHERE $i = 1, 2, 3, 4, 5, 6$

<table>
<thead>
<tr>
<th>Index</th>
<th>$\xi_{11}$</th>
<th>$\xi_{12}$</th>
<th>$\xi_{13}$</th>
<th>$\xi_{14}$</th>
<th>$\xi_{22}$</th>
<th>$\xi_{23}$</th>
<th>$\xi_{24}$</th>
<th>$\xi_{33}$</th>
<th>$\xi_{34}$</th>
<th>$\xi_{44}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1(2),1]</td>
<td>3.56 $\cdot 10^3$</td>
<td>1.14 $\cdot 10^3$</td>
<td>$-10.3$</td>
<td>$-8.09$</td>
<td>3.57 $\cdot 10^5$</td>
<td>$-8.08$</td>
<td>$-10.3$</td>
<td>2.08 $\cdot 10^{-1}$</td>
<td>7.00 $\cdot 10^{-2}$</td>
<td>2.69 $\cdot 10^{-1}$</td>
</tr>
<tr>
<td>[3(4),1]</td>
<td>2.59 $\cdot 10^3$</td>
<td>1.39 $\cdot 10^3$</td>
<td>$-3.40$</td>
<td>$-12.4$</td>
<td>3.63 $\cdot 10^5$</td>
<td>$-6.23$</td>
<td>$-15.6$</td>
<td>1.97 $\cdot 10^{-1}$</td>
<td>1.11 $\cdot 10^{-1}$</td>
<td>2.09 $\cdot 10^{-1}$</td>
</tr>
<tr>
<td>[5(6),1]</td>
<td>3.52 $\cdot 10^3$</td>
<td>1.77 $\cdot 10^3$</td>
<td>$-11.1$</td>
<td>$-11.6$</td>
<td>3.66 $\cdot 10^5$</td>
<td>$-14.3$</td>
<td>$-10.9$</td>
<td>2.07 $\cdot 10^{-1}$</td>
<td>1.31 $\cdot 10^{-1}$</td>
<td>1.93 $\cdot 10^{-1}$</td>
</tr>
</tbody>
</table>

TABLE V
SINGLE FAULT CONDITIONS; ENTRIES OF THE MATRIX $\Upsilon^{i,1}$, WHERE $i = 1, 2, 3, 4, 5, 6$

<table>
<thead>
<tr>
<th>Index</th>
<th>$v_{11}$</th>
<th>$v_{12}$</th>
<th>$v_{13}$</th>
<th>$v_{14}$</th>
<th>$v_{22}$</th>
<th>$v_{23}$</th>
<th>$v_{24}$</th>
<th>$v_{33}$</th>
<th>$v_{34}$</th>
<th>$v_{44}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1(2),1]</td>
<td>3.26 $\cdot 10^3$</td>
<td>1.44 $\cdot 10^3$</td>
<td>$-8.19$</td>
<td>$-10.2$</td>
<td>3.27 $\cdot 10^5$</td>
<td>$-10.2$</td>
<td>$-8.23$</td>
<td>1.75 $\cdot 10^{-1}$</td>
<td>1.03 $\cdot 10^{-1}$</td>
<td>1.75 $\cdot 10^{-1}$</td>
</tr>
<tr>
<td>[3(4),1]</td>
<td>2.32 $\cdot 10^3$</td>
<td>1.03 $\cdot 10^3$</td>
<td>$-5.16$</td>
<td>$-10.6$</td>
<td>3.14 $\cdot 10^5$</td>
<td>$-9.24$</td>
<td>$-9.22$</td>
<td>1.68 $\cdot 10^{-1}$</td>
<td>1.10 $\cdot 10^{-1}$</td>
<td>1.86 $\cdot 10^{-1}$</td>
</tr>
<tr>
<td>[5(6),1]</td>
<td>3.40 $\cdot 10^3$</td>
<td>1.63 $\cdot 10^3$</td>
<td>$-10.1$</td>
<td>$-11.2$</td>
<td>3.43 $\cdot 10^5$</td>
<td>$-12.2$</td>
<td>$-9.56$</td>
<td>1.87 $\cdot 10^{-1}$</td>
<td>1.17 $\cdot 10^{-1}$</td>
<td>1.82 $\cdot 10^{-1}$</td>
</tr>
</tbody>
</table>

TABLE VI
DOUBLE FAULT CONDITIONS; SEQUENCES OF FAULTS WITH NON-ZERO FAULT COVERAGE

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Second fault effect</th>
<th>Index</th>
<th>$\det(\Upsilon^{i,1})$</th>
<th>$\det(\Upsilon^{i,2})$</th>
<th>Second fault coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R_3 \rightarrow R_4, R_4 \rightarrow R_3$</td>
<td>$R_{4(3)} = \infty$</td>
<td>[1,2], [2,2]</td>
<td>1.23 $\cdot 10^5$</td>
<td>1.11 $\cdot 10^5$</td>
<td>$c_{rv} = 0.95$</td>
</tr>
<tr>
<td>$R_3 \rightarrow C_{1(2)}, R_4 \rightarrow C_{1(2)}$</td>
<td>$C_{1(2)}/2$</td>
<td>[3,4,2], [5,6,2]</td>
<td>1.23 $\cdot 10^5$</td>
<td>9.58 $\cdot 10^{-4}$</td>
<td>$c_{rv} = 0.88$</td>
</tr>
<tr>
<td>$R_3 \rightarrow S_{71(2)}, R_4 \rightarrow S_{71(2)}$</td>
<td>$k_{14(2)} = 0$</td>
<td>[7,8,2], [9,10,2]</td>
<td>1.23 $\cdot 10^5$</td>
<td>1.22 $\cdot 10^5$</td>
<td>$c_{rv} = 0.99$</td>
</tr>
<tr>
<td>$C_1 \rightarrow C_2, C_2 \rightarrow C_1$</td>
<td>$C_{2(1)}/2$</td>
<td>[11,2], [12,2]</td>
<td>7.67 $\cdot 10^{-4}$</td>
<td>4.83 $\cdot 10^{-4}$</td>
<td>$c_{cyc} = 0.79$</td>
</tr>
<tr>
<td>$C_1 \rightarrow R_{3(4)}, C_2 \rightarrow R_{3(4)}$</td>
<td>$R_{3(4)} = \infty$</td>
<td>[13,14,2], [15,16,2]</td>
<td>7.67 $\cdot 10^{-4}$</td>
<td>7.49 $\cdot 10^{-4}$</td>
<td>$c_{cyc} = 0.99$</td>
</tr>
<tr>
<td>$S_{71(2)} \rightarrow S_{72(1)}, S_{72(1)} \rightarrow S_{72(1)}$</td>
<td>$k_{23(14)} = 0$</td>
<td>[17,18,2], [19,20,2]</td>
<td>7.67 $\cdot 10^{-4}$</td>
<td>7.44 $\cdot 10^{-4}$</td>
<td>$c_{cyc} = 0.98$</td>
</tr>
<tr>
<td>$S_{71(2)} \rightarrow C_{1(2)}, S_{72(1)} \rightarrow C_{1(2)}$</td>
<td>$C_{1(2)}/2$</td>
<td>[27,28,2], [29,30,2]</td>
<td>1.23 $\cdot 10^5$</td>
<td>8.88 $\cdot 10^{-4}$</td>
<td>$c_{cyc} = 0.85$</td>
</tr>
</tbody>
</table>

Fig. 10. DC power system dynamic behavior for a 50% capacitance drop in $C_1$ or $C_2$ after an open-circuit fault in $R_3$ or $R_4$: (a) projections of $S, S^{(1)}(2), \chi^{(1)}(2), \chi^{(2)}(1)$, and $\phi^{(1)}(2)$ on to the subspace defined by $i_1, i_2$; (b) projections of $S, S^{(2)}(2), \chi^{(2)}(1), \chi^{(1)}(2)$, and $\phi^{(2)}(1)$ on to the subspace defined by $i_3, i_4$.

C. Network Dynamics After Two Faults

We only consider two-fault sequences where the first fault is any of $R_{3(4)}, C_{1(2)},$ or $S_{71(2)}$, which are the only first faults with non zero fault coverage. From previous results, any two-fault sequence with a second fault in $S_{71(2)}$ or $S_{72(1)}$ will result in zero fault coverage. If (39) holds, then by solving (17), and the optimization problems defined by (40)–(42) and (43)–(45), we obtain the relevant information to compute the fault coverage for all other two-fault sequences. This information, together with the corresponding fault coverage, is collected in Table VI. The case when there is a fault in $C_1$ or $C_2$ after a fault in $R_3$ or $R_4$ is illustrated in Fig. 10.

D. System Reliability Model

The overall system reliability can be estimated by formulating a Markov reliability model as explained in Section V, or in any standard reliability text, e.g., [37]. We only consider up to two-fault sequences, and then use truncation techniques to simplify the construction of the Markov model [38], [39]. We show that the error on the reliability estimate obtained with the
truncated model is negligible with respect to the estimate. We simplify further the Markov reliability model formulation by aggregating equivalent sequences of faults, i.e., sequences with the same faulty components, and the same outcome. To complete the numerical analysis, in Table VII we provide a reasonable order of magnitude for each component failure rate.

For evaluation purposes, we considered a 3 year (23,000 hours) evaluation time, and computed the Markov model state probabilities at the end of this evaluation time. Table VIII displays the fault events associated with each state of the Markov model, the resulting outcome describing whether or not the system is still operational after each fault event, and the associated probabilities for the considered evaluation time.

A lower bound on the reliability estimate is obtained by adding up the probabilities (column 3 of Table VIII) of the fault events after which the system is still operational, resulting in $\bar{R} = 0.999052$. As explained in [39], the probability of the final absorbing state 18 is the upper bound on the reliability estimate error $\epsilon_R = 2.66 \times 10^{-9}$. Thus, the true reliability estimate $\hat{R}$ is bounded as $\hat{R} \leq \bar{R} \leq \hat{R} + \epsilon_R$, from where we conclude that truncating the analysis after sequences of two faults yields an accurate reliability estimate.

### VII. CONCLUDING REMARKS

We proposed a fault coverage model for LTI systems where the system input is considered to be unknown but bounded, and where the bound is described by an ellipsoid. In this model, the performance requirements constrain the system trajectories to regions of the state-space defined by a symmetrical polytope; and we assume that behavioral decomposition holds, i.e., the time constants associated with the system dynamics are much smaller than the time constants associated with fault occurrences. The model includes, in a natural way, the uncertainty associated with the system inputs, and seems to be computationally less expensive than techniques to compute fault coverage based on fault injection experiments, although this statement needs further verification. The proposed coverage model can be naturally included in a Markov reliability model.
Therefore, because our fault coverage model is formulated in terms of the system physical and performance parameters, it enables an integrated framework for analysing system dynamic performance and reliability, and how they influence each other. Furthermore, by formulating the reliability model in terms of physical parameters of the system, it may be possible to formulate a unique problem for jointly optimizing dynamic performance, and system reliability.

To calculate fault coverage, it is necessary to obtain the system reach set before the fault occurrence, the largest set contained in the pre-fault reach set, and the state variables probability distribution. Computing the exact shape of the aforementioned sets is not an easy task. In this regard, we provided a computationally amenable method to obtain approximations to these sets based on obtaining ellipsoidal bounds to the reach set, and solving two convex optimization problems involving the system matrices associated with the system state-space representation. Obtaining the state variables probability distribution is key to computing the fault coverage probability; however, it is usually the case that this distribution cannot be completely defined as we do not have complete information regarding the system input distribution. In this regard, when the first and second moment of the state variables distribution are available, we discussed methods to obtain an upper bound on the fault coverage by using techniques based on generalizing the Chebyshev inequality to the $\eta$-dimensional case. We also discussed an important class of systems where the structure of the input, and the system state-space model matrices are such that the time distribution of the states can be assumed to be approximately uniform.

Note that the fault coverage estimates obtained with the ellipsoidal approximation method provided may be conservative. In further work, we will investigate the use of polyhedral sets to obtain an accurate approximation of the set of the reach set, or even map out its exact shape as the intersection (union) of families of external (internal) ellipsoidal approximations of the reach set [21]. Additionally, to obtain tighter bounds on the fault coverage, further investigation is needed on the use of moment-based inequalities that take into account, when available, higher moments of the distribution rather than just first and second ones [40].

REFERENCES

Alejandro D. Domínguez-García (M’07) received the Ph.D. degree in Electrical Engineering and Computer Science from the Massachusetts Institute of Technology, Cambridge, MA, in 2007; and the degree of Electrical Engineer from the University of Oviedo (Spain) in 2001.

Dr. Domínguez-García is an Assistant Professor in the Electrical and Computer Engineering Department at the University of Illinois, Urbana, where he is affiliated with the Power and Energy Systems area. His research interests lie at the interface of system reliability theory and control theory, with special emphasis on applications to power electronics, electric power systems, and safety-critical/fault-tolerant aircraft, aerospace and automotive systems.

Prior to joining MIT as a graduate student, Dr. Domínguez-García was with the Department of Electrical Engineering of the University of Oviedo where he held the position of Assistant Professor. After finishing the Ph.D., he spent some time as a post-doctoral research associate at the Laboratory for Electromagnetic and Electronic Systems of the Massachusetts Institute of Technology.

John G. Kassakian (S’65–M’73–SM’80–F’89) received the undergraduate and graduate degrees from the Massachusetts Institute of Technology (MIT), and prior to joining the MIT faculty, served a tour of duty in the U.S. Navy. From 1991 to 2008, he was the director of the MIT Laboratory for Electromagnetic and Electronic Systems, in Cambridge.

Dr. Kassakian is the Founding President of the IEEE Power Electronics Society, and is the recipient of the IEEE Centennial Medal, the IEEE William E. Newell Award, the IEEE Power Electronics Societys Distinguished Service Award, and the IEEE Millennium Medal. He is a member of the National Academy of Engineering. He has published extensively in the areas of power electronics, education, and automotive electrical systems; and is a co-author of the textbook Principles of Power Electronics.

Joel E. Schindall (S’61–M’66–SM’08–F’09) re-joined the MIT faculty in June of 2002 after a 35 year career in the defense, aerospace, and telecommunications industries. His research includes the concept and development of a nanotube-enhanced ultracapacitor. He is also supervising research on the integration of performance and reliability evaluation for designing complex systems, noise-canceling headphones, underwater acoustic networking, and a biologically-based pulse interval processor.

Prior to joining MIT, Dr. Schindall was Vice President and Chief Technology Officer of Loral Space and Communications. His responsibilities included overseeing the satellite research and development activities of Space Systems/Loral (originally Ford Aerospace). Earlier in his career, Dr. Schindall served as Senior VP and Chief Engineer for Globalstar, President of Loral’s Conic Division, and Manager of the Recon Division at Watkins-Johnson.

Dr. Schindall received his B.S., M.S. and Ph.D. degrees in Electrical Engineering from the Massachusetts Institute of Technology in 1963, 1964, and 1967.