A Generalized Fault Coverage Model for Linear Time-Invariant Systems

Alejandro D. Domínguez-García, *Member, IEEE,*
John G. Kassakian, *Fellow, IEEE,* Joel E. Schindall, *Member, 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 system 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. In order to illustrate the application of the proposed model two examples are discussed.

Index Terms

Fault Coverage, Linear time-invariant systems, Invariant sets, Convex optimization, Markov Reliability Modeling.

A. D. Domínguez-García is with the Department of Electrical and Computer Engineering of the University of Illinois at Urbana-Champaign, 1406 W. Green Street, Urbana, IL 61801. E-mail: aledan@illinois.edu. J. G. Kassakian, and J. E. Schindall are with the Laboratory for Electromagnetic and Electronic Systems at the Massachusetts Institute of Technology.

ACRONYMS

DPRA	Dynamic Probabilistic Risk Assessment
FDIR	Fault Detection Isolation and Reconfiguration
LTI	Linear Time-Invariant
ESPN	Extended Stochastic Petri Net

NOTATION

A	Fault-free system dynamics state-transition matrix
$\hat{A}$	Post-fault system dynamics state-transition matrix
B	Fault-free system dynamics input matrix
$\hat{B}$	Post-fault system dynamics input matrix
C	Fault coverage
c	Fault coverage lower bound estimate
Q	Matrix associated with the ellipsoid Ω_w
t	Pre-fault time variable
$\hat{t}$	Post-fault time variable
T	Random variable representing time to a first fault
w	System dynamics input vector
x	System dynamics state variables vector
Ψ	Matrix associated with the ellipsoid Ω
Ψ_0	Matrix associated with the ellipsoid Ω_0
$\mathcal{E}$	Steady-set value of the ellipsoid Ω
$\hat{\mathcal{X}}$	Largest invariant ellipsoid with respect to the post-fault dynamics contained in $\hat{\Phi}$
$\hat{\mathcal{E}}$	Largest ellipsoid contained in $\mathcal{E} \cap \hat{\mathcal{X}}$
$\mathcal{R}$	Fault-free reach set
Υ	Matrix associated with the ellipsoid $\mathcal{E}$
$\hat{\Xi}$	Matrix associated with the ellipsoid $\hat{\mathcal{X}}$
$\hat{\Upsilon}$	Matrix associated with the ellipsoid $\hat{\mathcal{E}}$
Ω	Fault-free reach set bounding ellipsoid
Ω_0	Value of the ellipsoid Ω at $t = 0$
Ω_w	System input bounding ellipsoid
$\hat{\Phi}$	Post-fault state-space region defined by the performance requirements
$\hat{\Theta}$	Subset of Ω that results in post-fault trajectories fully contained in $\hat{\Phi}$

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 is 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 to the system delivering its function in the presence of a fault. This is 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 by 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], [11], [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 also 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

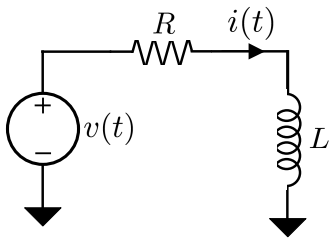


Fig. 1. RL Circuit.

by a set of differential equations, which can be expressed using a state-space representation [15]:

$$\frac{dx(t)}{dt} = Ax + Bw,\ x(0) = x_0, \tag{1}$$

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 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

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

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 would result in a new pair of matrices $\{\hat{A}, \hat{B}\}$. 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. For example, electric energy systems, aircraft and spacecraft control systems, and automotive control systems.

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 μ is the number of possible faults, ρ the number of possible fault occurrence times (obtained by discretizing the time axis), and ζ 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 ρ. 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], [17], [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 state space representation of the reactor dynamics [18]. Second, the time constants associated with the system dynamics of a nuclear reactor are not neglectable 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 with 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 to describe the overall system dynamic behavior in the presence of input uncertainty. Then, we define our fault coverage model and provide with 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

$$\begin{aligned} \frac{dx(t)}{dt} &= Ax(t) + Bw(t), \\ x(0) \in \Omega_0 &= \{x : x'\Psi_0^{-1}x \leq 1\}, \\ w(t) \in \Omega_w &= \{w : w'Q^{-1}w \leq 1\}, \end{aligned} \tag{3}$$

where $A \in \mathbb{M}^{n\times n}$ is the system state-transition matrix, $B \in \mathbb{M}^{n\times m}$ is the system input matrix, $x \in \mathbb{R}^n$ is the vector of system state variables, and $w \in \mathbb{R}^m$ is the vector of system input variables. $\Psi_0 \in \mathbb{M}^{n\times n}$, $Q \in \mathbb{M}^{m\times m}$ 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 Φdefined by the symmetric polytope

$$\Phi = \{x : |\pi_i' \, x| \leq 1 \; \forall i = 1, 2, \ldots, p\}, \tag{4}$$

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

$$\begin{gathered} \Omega(t) = \{x : x'\Psi(t)^{-1}x \leq 1\}, \\ \tfrac{d\Psi(t)}{dt} = A\Psi(t) + \Psi(t)A' + \beta\Psi(t) + \tfrac{1}{\beta}BQB', \\ \Psi(t=0) = \Psi_0, \end{gathered} \tag{5}$$

with $\beta > 0$, and $\Psi(t) \in \mathbb{M}^{n\times n}$ positive definite. The derivation of (5) can be found in [22] and [23], and the reader is referred to those for extensive treatments of the use of ellipsoids in dynamic systems and control. Let Υ 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

$$\begin{gathered} \mathcal{E} = \{x : x'\Upsilon^{-1}x \leq 1\}, \\ A\Upsilon + \Upsilon A' + \beta\Upsilon + \tfrac{1}{\beta}BQB' = 0, \end{gathered} \tag{6}$$

with $\beta > 0$ and $\Upsilon \in \mathbb{M}^{n\times n}$ positive definite.

The value of β in (5) and (6) will determine how "tight" is the bounding ellipsoid. There are several criterions to pick β such that the resulting bounding ellipsoid is optimal in some sense. For example, ellipsoids with minimum volume can be obtained by making $\beta = \sqrt{\text{tr}[\Upsilon^{-1}BQB']/n}$ [24]; ellipsoids with minimum sum of squared semi-axes can be obtained by making $\beta = \sqrt{\text{tr}[BQB']/\text{tr}[\Upsilon]}$ [24]; and ellipsoids with minimum projection in a given direction η can be obtained by making $\beta = \sqrt{\eta' BQB'\eta/\eta'\Upsilon\eta}$ [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 $\hat{A}, \hat{B}$. Let τ be a realization of T. Then, the system state-space representation after the fault can be defined by

$$\begin{aligned} \tfrac{dx(\hat{t})}{d\hat{t}} &= \hat{A}x(\hat{t}) + \hat{B}w(\hat{t}), \\ x(\hat{t}=0) &= x(t=\tau) \in \mathcal{R}(\tau), \\ w(\hat{t}) &\in \Omega_w = \{w : w'Q^{-1}w \leq 1\}, \end{aligned} \tag{7}$$

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 $\hat{\mathcal{R}}(\hat{t})$ 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 $\hat{\mathcal{R}}(\hat{t})$. It is important to note that if τ 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 Φ. 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

$$\hat{\Phi} = \{x : |\hat{\pi}_i' \, x| \leq 1 \ \forall i = 1, 2, \ldots, p\}, \tag{8}$$

where $\hat{\pi}_i \in \mathbb{R}^n$ 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 $\hat{\Phi}$ 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 $\hat{\Phi}$. 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 $\hat{\Phi}$.

Figure 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 $\mathcal{T}_1$ 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 $\hat{\Phi}$. Therefore, the system survives this fault. The second trajectory $\mathcal{T}_2$ represents the case where the state variables at the time of fault $x(\hat{t} = 0)$ are in $\hat{\Phi}$ but there is some $\hat{t} > 0$ such that $x(\hat{t}) \notin \hat{\Phi}$. Therefore, the system does not survive this fault even if $x(\hat{t} = 0) \in \hat{\Phi}$. Trajectory $\mathcal{T}_3$ represents the case when $x(\hat{t} = 0) \notin \hat{\Phi}$. 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 τ. Then, the system is *guaranteed* to survive a fault whenever the state variables at the time of fault occurrence are contained in some set $\hat{\Theta}(\tau) \subseteq \mathcal{R}(\tau) \cap \hat{\Phi}$, such that if $x(t = \tau) = x(\hat{t} = 0) \in \hat{\Theta}(\tau)$, then $x(\hat{t}) \in \hat{\Phi}$ for all $\hat{t} > 0$. Thus, if $\hat{\Theta}(\tau) \equiv \emptyset$, then the system is guaranteed to survive the fault with probability zero. If $\hat{\Theta}(\tau) \not\equiv \emptyset$, then the system is guaranteed to survive the fault with probability greater than zero. The definition of fault coverage follows from these ideas.

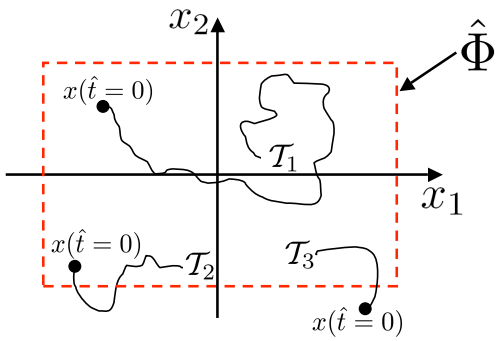


Fig. 2. Trajectories followed by a second order system after a first fault occurrence for different values of the state variables at the time the fault occurs.

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 $x(t = \tau) = x(\hat{t} = 0) \in \hat{\Theta}(\tau)$, then $x(\hat{t}) \in \hat{\Phi}$ for all $\hat{t} > 0$. Then, for any $t > 0$, **fault coverage** is defined by

$$C = Pr\{X(T) \in \hat{\Theta}(T) | T < t\}. \tag{9}$$

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; and 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).

Dependence of the distribution of $X(T)$ and the shape of the set $\hat{\Theta}(T)$ on the distribution of T

We show how the behavioral decomposition assumption, i.e, the time constants associated with the system dynamics are much smaller than the time constants associated with fault occurrences, 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

$$C = \frac{Pr\{T < t, X(T) \in \hat{\Theta}(T)\}}{Pr\{T < t\}}, \tag{10}$$

where

$$Pr\{T < t, X(T) \in \hat{\Theta}(T)\} = \int_0^t \int_{x(\tau) \in \hat{\Theta}(\tau)} f_{X|T}(x|\tau) f_T(\tau) dx d\tau. \tag{11}$$

If the distribution of w over Ω_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 let $t = t_{ss}$

be much larger than the largest time constant associated with (5). Then, we can rewrite (11) as

$$\int_0^{t_{ss}} \int_{x(\tau)\in\hat{\Theta}(\tau)} f_{X|T}(x|\tau) f_T(\tau) dx d\tau + \int_{t_{ss}}^{t} \int_{x(t_{ss})\in\hat{\Theta}_{ss}} f_{X|T}(x|t_{ss}) f_T(\tau) dx d\tau. \tag{12}$$

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

$$\int_0^{t_{ss}} f_T(\tau) d\tau \int_{x(\xi)\in\hat{\Theta}(\xi)} f_{X|T}(x|\xi) dx + \int_{t_{ss}}^{t} f_T(\tau) d\tau \int_{x(t_{ss})\in\hat{\Theta}ss} f_{X|T}(x|t_{ss}) dx, \tag{13}$$

for some ξ, such that $0 \leq \xi \leq t_{ss}$. Now since behavioral decomposition holds, it follows that

$$\begin{aligned} \int_0^{t_{ss}} f_T(\tau) d\tau &\approx 0, \\ \int_{t_{ss}}^{t} f_T(\tau) d\tau &\approx \int_0^{t} f_T(\tau) d\tau. \end{aligned} \tag{14}$$

This 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 in the order of $10^{-5} - 10^{-9}$ /h. Then, by combining (13) and (14), it results that

$$\begin{aligned} Pr\{T < t, X(T) \in \hat{\Theta}(T)\} \approx \int_{t_{ss}}^{t} f_T(\tau) d\tau \int_{x(t_{ss})\in\hat{\Theta}_{ss}} f_{X|T}(x|t_{ss}) dx = \\ Pr\{T < t\} \int_{x(t_{ss})\in\hat{\Theta}_{ss}} f_{X|T}(x|t_{ss}) dx. \end{aligned} \tag{15}$$

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

$$C \approx \int_{x(t_{ss})\in\hat{\Theta}_{ss}} f_{X|T}(x|t_{ss}) dx. \tag{16}$$

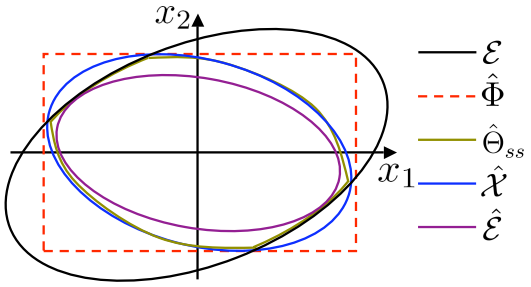


Fig. 3. The initial conditions set $\mathcal{E}$ is not fully contained in the set $\hat{\Phi}$, but the new pair $\hat{A}, \hat{B}$ is such that $\mathcal{E} \cap \hat{\Phi} = \hat{\Theta} \supseteq \hat{\mathcal{E}}$.

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 $x(\hat{t}) \in \hat{\Phi}$ for all $\hat{t} > 0$. Since $\mathcal{R}(\tau)$ 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 $\mathcal{E}$, 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 $x(\hat{t}) \in \hat{\Phi}$ for all $\hat{t} > 0$. 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 $\mathcal{E}$ and $\hat{\mathcal{X}}$. For a two-dimensional system, a graphical interpretation of $\mathcal{E}$, $\hat{\Phi}$, $\hat{\Theta}_{ss}$, $\hat{\mathcal{X}}$ 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 $\hat{\mathcal{P}} = \{x : x'\hat{\Gamma}^{-1}x \leq 1\}$ be the smallest invariant ellipsoid with respect to (7), i.e., any trajectory with initial conditions in $\hat{\mathcal{P}}$ remains in $\hat{\mathcal{P}}$ at all times [26]. Then

$$\hat{A}\hat{\Gamma} + \hat{\Gamma}\hat{A}' + \hat{\alpha}\hat{\Gamma} + \frac{1}{\hat{\alpha}}\hat{B}Q\hat{B}' = 0,$$
$$\hat{\alpha} = \sqrt{\frac{\text{tr}[\hat{\Gamma}^{-1}\hat{B}Q\hat{B}']}{n}} \tag{17}$$

with $\hat{\Gamma} \in \mathbb{M}^{n\times n}$ positive definite [24]. Let $\hat{\pi}_i \in \mathbb{R}^n$ be the i vector that defines $\hat{\Phi}$ in (8). Then if $\hat{\pi}_i' \, \hat{\Gamma} \, \hat{\pi}_i \geq 1 \; for \; some \; i = 1, 2, \ldots, p$, it follows that $\hat{\mathcal{P}} \nsubseteq \hat{\Phi}$ and therefore $\hat{\mathcal{X}} \equiv \hat{\Theta}_{ss} \equiv \emptyset$, which results in the fault coverage being 0.

Now assume $\hat{\mathcal{P}} \not\equiv \emptyset$ and let $\hat{\mathcal{X}} = \{x : x'\hat{\Xi}^{-1}x \leq 1\}$ be the largest invariant ellipsoid with respect to (7) contained in $\hat{\Phi}$. Then, since 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], $\hat{\Xi}$ can be obtained by solving the following optimization problem

$$\text{maximize} \qquad \det \hat{\Xi} \tag{18}$$
$$\text{subject to} \quad \hat{\pi}_i' \, \hat{\Xi} \, \hat{\pi}_i \leq 1, \; \forall i = 1, 2, \ldots, p \tag{19}$$
$$\hat{A}\hat{\Xi} + \hat{\Xi}\hat{A}' + \hat{\alpha}\hat{\Xi} + \frac{1}{\hat{\alpha}}\hat{B}Q\hat{B}' \preceq 0, \tag{20}$$

in the variable $\hat{\Xi}$ with implicit constraint $\hat{\Xi}$ positive definite, where $\hat{\alpha}$ is the parameter that defines $\hat{\mathcal{P}}$ in (17), and where "$\preceq$" in (20) means that the left hand side of the inequality is

negative-semidefinite. As explained in [28], this optimization problem can be casted 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 $\hat{\mathcal{X}}$ in the direction of $\hat{\pi}_i$ lies within the requirements imposed on x_i by (8), from where it follows that if $\hat{\mathcal{X}}$ exits, it is contained in $\hat{\Phi}$ [29]. The constraint given by (20) ensures that, if $\hat{\Xi}$ exits, it is invariant with respect to (7), i.e., any trajectory with initial conditions in $\hat{\mathcal{X}}$ remains in $\hat{\mathcal{X}}$ at all times [26].

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

$$\text{maximize} \qquad \det \hat{\Upsilon} \tag{21}$$

$$\text{subject to} \quad \hat{\Upsilon} - \Upsilon \preceq 0, \tag{22}$$

$$\hat{\Upsilon} - \hat{\Xi} \preceq 0, \tag{23}$$

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

$$c = \int_{x(t_{ss})\in\hat{\mathcal{E}}} f_{X|T}(x|t_{ss})dx. \tag{24}$$

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 Ω_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

$$\frac{di(t)}{dt} = -\frac{R}{L}i(t) + \frac{1}{L}v(t), i(0) = -\frac{V}{R}, \tag{25}$$

if the input $v(t)$ is a square signal with amplitude V and period much larger than the time circuit constant $\frac{L}{R}$, 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 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 $\frac{L}{R}$ 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 Ω_w. Condition 1) ensures that the system 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, since 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

$$c = \frac{\text{cont}(\hat{\mathcal{E}})}{\text{cont}(\mathcal{E})} = \sqrt{\frac{\det(\hat{\Upsilon})}{\det(\Upsilon)}}. \tag{26}$$

There are many practical systems in which the aforementioned conditions hold. For example, in the dc power distribution system discussed in Section VI, the voltages driving the system can be modeled as unknown-but-bounded. In this case, the input voltages might be constant for a period of time and then, change to a different value, remaining constant until another change occurs.

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]. Since 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] and [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 $\hat{\mathcal{E}}$ to $\mathcal{E} \cap \hat{\mathcal{E}}^c$.

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 that: (a) the initial current $i(0)$ flowing through the circuit is unknown, but it is such that $|i(0)| \leq I$, with $I > 0$; (b) the voltage source $v(t)$ is unknown, but it is such that that $|v(t)| \leq V$, with $V > 0$; (c) the maximum currents that resistors R_1 and R_2 can process are $i_{max}^{R_1}$ and $i_{max}^{R_2}$, respectively, and once this current is reached the resistor fails open; (d) the values of V, R_1, R_2, $i_{max}^{R_1}$, and $i_{max}^{R_2}$ are such that $\frac{V}{R_1} < i_{max}^{R_1}$, $\frac{V}{R_2} < i_{max}^{R_2}$; (e) the only faults considered are caused by the resistors failing open circuit; (f) the time to a fault occurrence in the resistors R_1 and R_2 is exponentially distributed with rates λ_{R_1} and λ_{R_2} respectively; and (g) the system fails with probability 1 if both resistors fail.

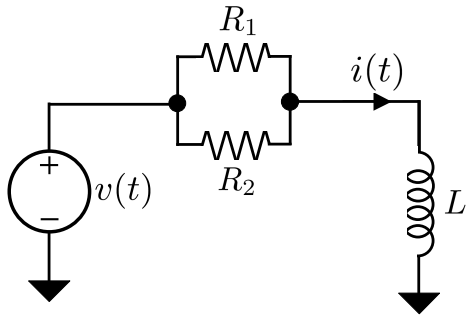


Fig. 4. Series RL Circuit.

A. Fault-Free System Dynamics

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

$$\begin{aligned} \frac{di(t)}{dt} &= -\frac{R_{eq}}{L}i(t) + \frac{1}{L}v(t), \\ i(t=0) &\in \omega_0 = \{i : |i| \leq I\}, \\ v(t) &\in \omega_v = \{v : |v| \leq V\}, \end{aligned} \tag{27}$$

where $R_{eq} = \dfrac{R_1 R_2}{R_1 + R_2}$. Let $\omega(t) = \{i : \gamma(t)^{-1} i^2 \leq 1\}$ be an interval in $\mathbb{R}$ that contains all possible current for $t > 0$, where $\gamma(t)$ can be computed by solving

$$\begin{aligned} \frac{d\gamma(t)}{dt} &= -2\frac{R_{eq}}{L}\gamma(t) + \beta\gamma(t) + \frac{1}{\beta L^2}V^2, \\ \gamma(0) &= I^2, \end{aligned} \tag{28}$$

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

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

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

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

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

$$\varepsilon = \{i : |i| \leq \frac{V}{R_{eq}}\}. \tag{31}$$

Figure 5 represents, for $I < \frac{V}{R_{eq}}$, the evolution of the interval bounding the current flowing through the circuit.

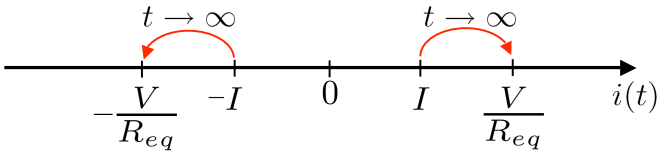
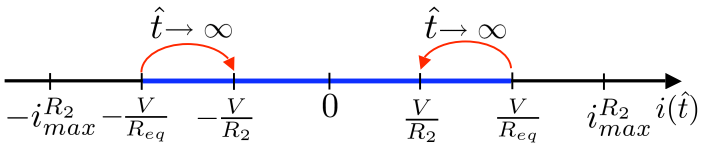
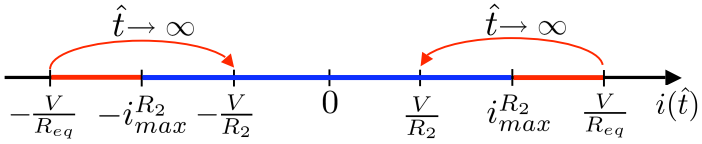


Fig. 5. Series RL circuit current evolution for $I < \frac{V}{R_{eq}}$.



(a) The values of V, R_1, R_2, and $i_{max}^{R_2}$ such that $i_{max}^{R_2} > \frac{V}{R_{eq}} > \frac{V}{R_2}$.



(b) The values of V, R_1, R_2, and $i_{max}^{R_2}$ such that $\frac{V}{R_{eq}} > i_{max}^{R_2} > \frac{V}{R_2}$.

Fig. 6. Series RL circuit current evolution after a fault caused by R_1 failing open circuit.

B. System Dynamics After a Resistor Failure

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

$$\begin{aligned} \frac{di(\hat{t})}{d\hat{t}} &= -\frac{R_2}{L}i(\hat{t}) + \frac{1}{L}v(\hat{t}), \\ i(\hat{t}=0) \in \varepsilon &= \{i : |i| \leq \frac{V}{R_{eq}}\}, \\ v(\hat{t}) \in \omega_v &= \{v : |v| \leq V\}, \end{aligned} \tag{32}$$

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 ω_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 $i_{max}^{R_2}$, which is the maximum current allowed through R_2. By assumptions c) and g), a system failure occurs if, for some $\hat{t} > 0$, $i(\hat{t}) \notin \hat{\phi}$, where $\hat{\phi} = \{i(\hat{t}) : |i(\hat{t})| \leq i_{max}^{R_2}\}$. By using $\hat{\gamma}$ instead of $\hat{\Gamma}$, we can rewrite (17) as $-2\frac{R_2}{L}\hat{\gamma} + \hat{\alpha}\hat{\gamma} + \frac{1}{\hat{\alpha}L^2}V^2 = 0$,

where $\hat{\alpha} = V/L\sqrt{\hat{\gamma}^{-1}}$, resulting in $\hat{\alpha} = R_2/L$, and $\hat{\gamma} = (V/R_2)^2$, which ensures the system will survive with probability greater than zero since $(V/R_2)^2 < (i_{max}^{R_2})^2$ (assumption d)). Now let $\hat{\varepsilon} = \{i : \hat{\upsilon}^{-1}i^2 \leq 1\}$, where $\hat{\upsilon} > 0$ is obtained from specializing the procedure laid down in and (18)-(23) to this particular example as follows

$$\text{maximize} \qquad \hat{\upsilon} \tag{33}$$

$$\text{subject to} \quad -2\frac{R_2}{L}\hat{\upsilon} + \hat{\alpha}\hat{\upsilon} + \frac{1}{\hat{\alpha}L^2}V^2 \leq 0, \tag{34}$$

$$\hat{\upsilon} \leq (\frac{V}{R_{eq}})^2, \tag{35}$$

$$\hat{\upsilon} \leq (i_{max}^{R_2})^2, \tag{36}$$

with $\hat{\alpha} = R_2/L$. Two cases are possible depending on the value of $i_{max}^{R_2}$. It is easy to see that when $i_{max}^{R_2} > \frac{V}{R_{eq}} > \frac{V}{R_2}$ (case depicted in Fig. 6(a)), it results that $\hat{\upsilon} = (V/R_{eq})^2$, and the fault coverage is $c_{R_1} = 1$. For the case when $\frac{V}{R_{eq}} \geq i_{max}^{R_2} > \frac{V}{R_2}$ (depicted in Fig. 6(b)), it results that $\hat{\upsilon} = (i_{max}^{R_2})^2$, and the fault coverage is

$$c_{R_1} = \frac{\text{length}(\hat{\varepsilon})}{\text{length}(\varepsilon)} = i_{max}^{R_2}\frac{R_{eq}}{V}. \tag{37}$$

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 "$\hat{}$" 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).

A. Fault Coverage After $k \geq 1$ Faults

Let's 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 $T_{j,k-1}^{i,k}$ 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 $\tau^{i,k}_{j,k-1}$ be a realization of $T^{i,k}_{j,k-1}$. Then the system dynamics after the $[i,k]$ fault is defined by

$$\frac{dx(t^{i,k})}{dt^{i,k}} = A^{i,k}x + B^{i,k}w,$$
$$x(t^{i,k}=0) \in \mathcal{E}^{j,k-1} = \{x : x'(\Upsilon^{j,k-1})^{-1}x \leq 1\},$$
$$w \in \Omega_w = \{w : w'Q^{-1}w \leq 1\}, \tag{38}$$

where $t^{i,k} = t^{j,k-1} - \tau^{i,k}_{j,k-1}$, $A^{i,k}$ is the system state-transition matrix, and $B^{i,k}$ is the system input matrix, both for the system dynamics after the fault occurred. 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 $\Phi^{i,k} = \{x : |(\pi^{i,k}_l)'x| \ \leq 1 \ l = 1,2,\ldots p\}$ define the region of the state space where the system state variables x are to remain at all times for the system to fulfill its intended function. Then, if the system survives the additional fault after surviving the previous $k-1$ with probability greater than one, there exists $\Gamma^{i,k} \in \mathbb{M}^{n\times n}$ positive definite such that

$$A^{i,k}\Gamma^{i,k} + \Gamma^{i,k}(A^{i,k})' + \sqrt{\frac{\text{tr}[(\Gamma^{i,k})^{-1}\hat{B}Q\hat{B}']}{n}}\Gamma^{i,k} + \sqrt{\frac{n}{\text{tr}[(\Gamma^{i,k})^{-1}\hat{B}Q\hat{B}']}}B^{i,k}Q(B^{i,k})' = 0,$$
$$(\pi^{i,k}_l)'\Gamma^{i,k}(\pi^{i,k}_l) \leq 1, \quad \forall l = 1,2,\ldots,p. \tag{39}$$

Let $\alpha^{i,k} = \sqrt{\text{tr}[(\Gamma^{i,k})^{-1}\hat{B}Q\hat{B}']/n}$ and let $\mathcal{X}^{i,k} = \{x : x'(\Xi^{i,k})^{-1}x \leq 1\}$ the largest invariant ellipsoid with respect to (38) contained in $\Phi^{i,k}$, where $\Xi^{i,k}$ is obtained from solving

$$\text{maximize} \qquad \det \Xi^{i,k} \tag{40}$$
$$\text{subject to} \qquad (\pi^{i,k}_l)' \ \Xi^{i,k} \ (\pi^{i,k}_l) \leq 1, \ \forall l = 1,2,\ldots,n \tag{41}$$
$$A^{i,k}\Xi^{i,k} + \Xi^{i,k}(A^{i,k})' + \alpha^{i,k}\Xi^{i,k} + \frac{1}{\alpha^{i,k}}B^{i,k}Q(B^{i,k})' \preceq 0, \tag{42}$$

in the variable $\Xi^{i,k}$, with implicit constraint $\Xi^{i,k}$ positive definite. Let $\mathcal{E}^{i,k} = \{x : x'(\Upsilon^{i,k})^{-1}x \leq 1\}$ be the largest ellipsoid contained in $\mathcal{X}^{i,k}$ and $\mathcal{E}^{j,k-1}$, where $\Upsilon^{i,k}$ is obtained from solving

$$\text{maximize} \qquad \det \Upsilon^{i,k} \tag{43}$$
$$\text{subject to} \quad \Upsilon^{i,k} - \Upsilon^{j,k-1} \preceq 0, \tag{44}$$
$$\Upsilon^{i,k} - \Xi^{i,k} \preceq 0, \tag{45}$$

in the variables $\Upsilon^{i,k}$ with implicit constraint $\Upsilon^{i,k}$ positive definite. Then a lower bound on the fault coverage probability after the k fault occurrence can be obtained by computing

$$c_{j,k-1}^{i,k} = \int_{x \in \mathcal{E}^{i,k}} f_{X|T_{j,k-1}^{i,k}}(x|t)dx. \tag{46}$$

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 $[j, k-1]$, with a probability denoted by $p_{2j-1,k-1}(t)$. Let an additional fault occur, leading to the sequences of faults $[i, k]$. Let $p_{2i-1,k}(t)$ be the probability that, at any time $t \geq 0$, the system survived the $[i, k]$ sequence of faults and let $p_{2i,k}(t)$ denote the probability that, at any time $t \geq 0$, the system did not survive the $[i, k]$ sequence of faults, then

$$\frac{d}{dt}\left[\begin{array}{cc} p_{2i-1,k}, & p_{2i,k} \end{array}\right] = \left[\begin{array}{cc} p_{2j-1,k-1}, & p_{2i-1,k} \end{array}\right] \left[\begin{array}{cc} c_{j,k-1}^{i,k}\lambda_{j,k-1}^{i,k} & (1-c_{j,k-1}^{i,k})\lambda_{j,k-1}^{i,k} \\ -\sum_{N_k} \lambda_{i,k}^{m,k+1} & 0 \end{array}\right], \tag{47}$$

where $\lambda_{j,k-1}^{i,k}$ is the rate at which the last fault occurs in the sequence $[i, k]$, $\lambda_{i,k}^{m,k+1}$ 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 $[i, k]$. Each sequence of faults will generate a block similar to the one in (47). By assembling all these blocks, the state-transition matrix Λ 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

$$\frac{dP(t)}{dt} = P(t)\Lambda, \;\; P(0) = [1 \; 0 \; 0 \; ... \; 0]. \tag{48}$$

It is important to note that even if the sum of the entries in each rows 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 Λ 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 given in (37) and a similar calculation for R_2 yields $c_{R_1} = i_{max}^{R_2} \frac{R_{eq}}{V}$, and $c_{R_2} = i_{max}^{R_1} \frac{R_{eq}}{V}$.

Given that at time $t = 0$ no faults have occurred yet, let's define, at time t, the following probabilities: probability no faults have occurred, $p_{1,0}(t)$; probability the circuit survived a fault in resistor R_1, $p_{1,1}(t)$; probability the circuit did not survive a fault in resistor R_1, $p_{2,1}(t)$; probability the circuit survived a fault in resistor R_2, $p_{3,1}(t)$; probability the circuit did not survive a fault in resistor R_2, $p_{4,1}(t)$; probability the circuit did not survive a sequence of faults in R_1 and R_2 respectively, $p_{2,2}(t)$; probability the circuit did not survive a sequence of faults in R_2 and R_1 respectively, $p_{4,2}(t)$. Then, following the notation of (48), it results that: $P(t) = [p_{1,0}(t),\ p_{1,1}(t),\ p_{2,1}(t),\ p_{3,1}(t),\ p_{4,1}(t),\ p_{2,2}(t),\ p_{4,2}(t)]$, $P(0) = [1,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0]$, and the non-zero elements of the matrix Λ are: $[\Lambda]_{11} = -\lambda_{R_1} - \lambda_{R_1}$, $[\Lambda]_{12} = i_{max}^{R_2} \frac{R_{eq}}{V} \lambda_{R_1}$, $[\Lambda]_{13} = (1 - i_{max}^{R_2} \frac{R_{eq}}{V} \lambda_{R_1})$, $[\Lambda]_{14} = i_{max}^{R_1} \frac{R_{eq}}{V} \lambda_{R_2}$, $[\Lambda]_{15} = (1 - i_{max}^{R_1} \frac{R_{eq}}{V} \lambda_{R_2})$, $[\Lambda]_{22} = -\lambda_{R_2}$, $[\Lambda]_{26} = \lambda_{R_2}$, $[\Lambda]_{44} = -\lambda_{R_1}$, $[\Lambda]_{47} = \lambda_{R_1}$.

It is important to note that the Markov reliability model is not only formulated in terms of the rates at which faults occur, λ_{R_1} and λ_{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 telecommuni-

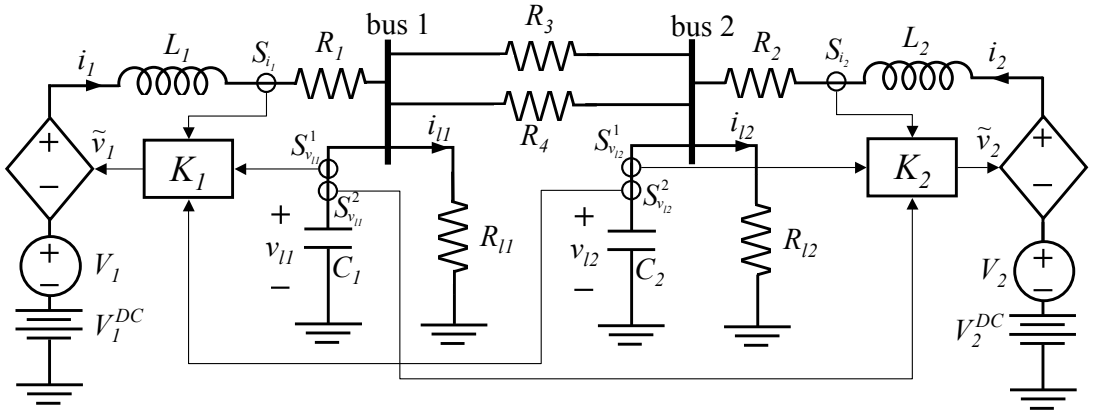


Fig. 7. Abstraction of fault-tolerant distributed dc power system for telecommunications applications.

cations applications [35]. The purpose of this system is to reliably provide power to two loads, represented by resistors R_{l1} and R_{l2}, maintaining their voltage within some tolerance around some nominal values V_{l1} and V_{l2} 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 three series voltage sources, where the first voltage source $V_{1(2)}^{DC}$ is constant, and represents the nominal input voltage, the second one $V_{1(2)}$ represents uncontrolled variations in the input voltage, and the third one $\tilde{v}_{1(2)}$ represents controlled variations in the input voltage. Let the system states be $i_{1(2)} = I_{1(2)} + \tilde{i}_{1(2)}$, and $v_{l1(2)} = V_{l1(2)} + \tilde{v}_{l1(2)}$, where capitalized variables represent the state variables behavior due to the constant input voltages $V_{1(2)}^{DC}$, and variables with tilde represent the state variables behavior due to uncontrolled variations in the input voltage $V_{1(2)}$. Since 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 uncontrolled variations in the input voltage $V_{1(2)}$ on $\tilde{i}_{1(2)}$ and $\tilde{v}_{l1(2)}$. We assume that the quasi-static assumption explained in Section II-D holds. Controlled variations in the input voltage $\tilde{v}_{1(2)}$ are specified by a constant-gain feedback control law of the form $\tilde{v}_1 = k_{11}\tilde{i}_1 + k_{13}\tilde{v}_{l1} + k_{14}\tilde{v}_{l2}$, where $\tilde{i}_1$ is measured by sensor S_{i_1}, $\tilde{v}_{l1}$ is measured by sensor $S^1_{v_{l1}}$, and $\tilde{v}_{l2}$ is measured by sensor $S^2_{v_{l2}}$; and $\tilde{v}_2 = k_{22}\tilde{i}_2 + k_{23}\tilde{v}_{l1} + k_{24}\tilde{v}_{l2}$, where $\tilde{i}_2$ is measured by sensor S_{i_2}, $\tilde{v}_{l1}$ is measured by sensor $S^2_{v_{l1}}$, and $\tilde{v}_{l2}$ is measured by sensor $S^1_{v_{l2}}$.

TABLE I

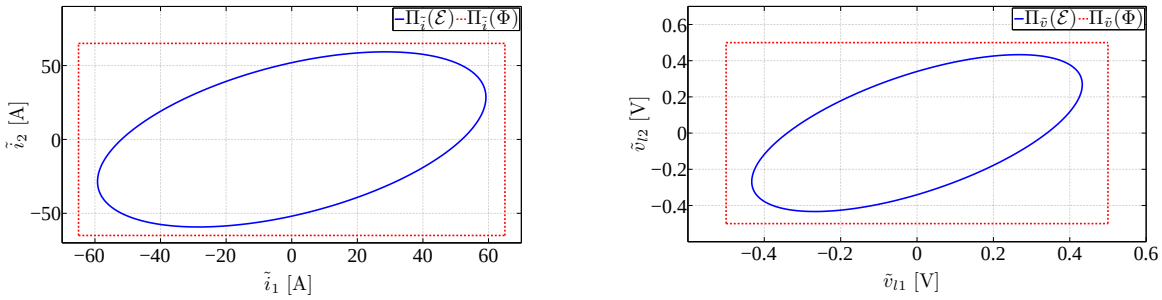
FAULT-FREE CONDITIONS: DC POWER SYSTEM PARAMETERS.

L_1, L_2 [H]	C_1, C_2 [F]	R_1, R_2	R_{12} [Ω]	k_{11}, k_{22} [Ω]	k_{13}, k_{24}	k_{14}, k_{23}	q_{11}, q_{22} [V^2]
$5 \cdot 10^{-5}$	10^{-1}	$2 \cdot 10^{-2}$	$4 \cdot 10^{-2}$	-0.1	-10	-1	25

TABLE II

FAULT-FREE CONDITIONS: DETERMINANT AND ENTRIES OF THE MATRIX Υ THAT DEFINES THE ELLIPSOID $\mathcal{E}$.

det(Υ)	υ_{11}	υ_{12}	υ_{13}	υ_{14}	υ_{22}	υ_{23}	υ_{24}	υ_{33}	υ_{34}	υ_{44}
$1.38 \cdot 10^5$	$3.51 \cdot 10^3$	$1.69 \cdot 10^3$	-9.94	$-1.2 \cdot 10^1$	$3.51 \cdot 10^3$	$-1.19 \cdot 10^1$	-9.98	$1.87 \cdot 10^{-1}$	$1.16 \cdot 10^{-1}$	$1.88 \cdot 10^{-1}$



(a) Subspace defined by $\tilde{i}_1, \tilde{i}_2$: Projection of ellipsoid $\mathcal{E}$ and projection of performance requirements region Φ.

(b) Subspace defined by $\tilde{v}_{l1}, \tilde{v}_{l2}$: Projection of ellipsoid $\mathcal{E}$ and projection of performance requirements region Φ.

Fig. 8. DC power system dynamic behavior before any fault occurrence: projections of the bounding ellipsoid on to the subspaces defined by the $\tilde{i}_1, \tilde{i}_2$ axes, and the $\tilde{v}_{l1}, \tilde{v}_{l2}$ axes.

A. *Fault-Free Network Dynamics*

Let $\tilde{x} = [\tilde{i}_1, \tilde{i}_2, \tilde{v}_{l1}, \tilde{v}_{l2}]'$ and $\tilde{w} = [V_1, V_2]'$. Then, it follows that

$$\dot{\tilde{x}} = A\tilde{x} + B\tilde{w},$$
$$V \in \Omega_V = \{V : V'Q^{-1}V \leq 1\}, \quad \tilde{x}(0) = [0,0,0,0]', \tag{49}$$

where

$$A = \begin{bmatrix} -(R_1 - k_{11})/L_1 & 0 & -(1-k_{13})/L_1 & k_{14}/L_1 \\ 0 & -(R_2 - k_{22})L_2 & k_{23}/L_2 & -(1-k_{24})/L_2 \\ 1/C_1 & 0 & -(1/R_3 + 1/R_4 + 1/R_{l1})/C_1 & 1/(R_{12}C_1) \\ 0 & 1/C_2 & 1/(R_{12}C_2) & -(1/R_3 + 1/R_4 + 1/R_{l2})/C_2 \end{bmatrix},$$

$$B = \begin{bmatrix} 1/L_1 & 0 \\ 0 & 1/L_2 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}, \; Q = \begin{bmatrix} q_{11} & 0 \\ 0 & q_{22} \end{bmatrix},$$

with the parameters of A, B, and C 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

$$\Phi = \{\tilde{x} : |\pi_i'\tilde{x}| \leq 1, \; i = 1,2,3,4\}, \tag{50}$$

where $\pi_1 = [1.66 \cdot 10^{-2}, 0, 0, 0]'$, $\pi_2 = [0, 1.66 \cdot 10^{-2}, 0, 0]'$, $\pi_3 = [0, 0, 2, 0]'$, and $\pi_4 = [0, 0, 0, 2]'$.

TABLE III

SINGLE FAULT CONDITIONS: EFFECT ON SYSTEM PARAMETERS AND CORRESPONDING FAULT COVERAGE.

Component	*Fault effect*	*Index*	$\det(\Upsilon^{i,1})$	*Fault Coverage*
$\mathrm{R}_{3(4)}$	$\mathrm{R}_{3(4)} = \infty$	[1(2),1]	$1.22 \cdot 10^5$	$c_r = 0.94$
$\mathrm{C}_{1(2)}$	$\mathrm{C}_{1(2)}/2$	[3(4),1]	$7.67 \cdot 10^4$	$c_c = 0.74$
$\mathrm{S}^2_{v_{l1(2)}}$	$k_{14(23)} = 0$	[5(6),1]	$1.23 \cdot 10^5$	$c_v = 0.95$
$\mathrm{S}_{i_{1(2)}}$	$k_{11(22)} = 0$	nil	nil	0
$\mathrm{S}^1_{v_{l1(2)}}$	$k_{13(24)} = 0$	nil	nil	0

By using (6), we can compute the positive definite matrix Υ defining the ellipsoid $\mathcal{E}$ that bounds $\tilde{i}_1,\ \tilde{i}_2,\ \tilde{v}_{l1}$, and $\tilde{v}_{l2}$. In order to solve (6), we consider a minimum volume criterion, which results in $\beta = 1.45 \cdot 10^3$, with the entries of Υ and its determinant taking the values in Table II. In order to visualize this 4-dimensional ellipsoid, we project it on to the subspaces defined by the $\tilde{i}_1, \tilde{i}_2$ axes, and the $\tilde{v}_{l1}, \tilde{v}_{l2}$ axes, and denote these projections as $\Pi_{\tilde{i}}(\mathcal{E})$ and $\Pi_{\tilde{v}}(\mathcal{E})$ respectively. Fig. 8 shows $\Pi_{\tilde{i}}(\mathcal{E})$ and $\Pi_{\tilde{v}}(\mathcal{E})$, where it can be seen that both projections are contained within the corresponding projections $\Pi_{\tilde{i}}(\Phi)$ and $\Pi_{\tilde{v}}(\Phi)$ of Φ defined by (50).

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 the capacitors C_1 and C_2; an output omission in one the current sensors S_{i_1}, S_{i_2}; an output omission in one of the voltage sensors $S^1_{v_{l1}}$, $S^2_{v_{l1}}$, $S^1_{v_{l2}}$, $S^2_{v_{l2}}$. The second column of Table III shows the effects of each fault on the parameters of A and B in (49) which, for each fault will result in a new pair of matrices $\hat{A}$ and $\hat{B}$. We impose the same requirements on variations around nominal values of the state variables, i.e, $\hat{\Phi} \equiv \Phi$. In order to compute fault coverage, we first solve (17), for which we use MATLAB; and then we solve the two convex optimization problems defined by (18-20) and (21-23) respectively. To solve these problems, we use CVX, a package for specifying and solving convex programs in MATLAB [30], [36].

For faults in the current sensors S_{i_1}, S_{i_2} and in the voltage sensors $S^1_{v_{l1}}$ and $S^1_{v_{l2}}$, 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 $\hat{\Phi}$ (equivalent to Φ 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

TABLE IV

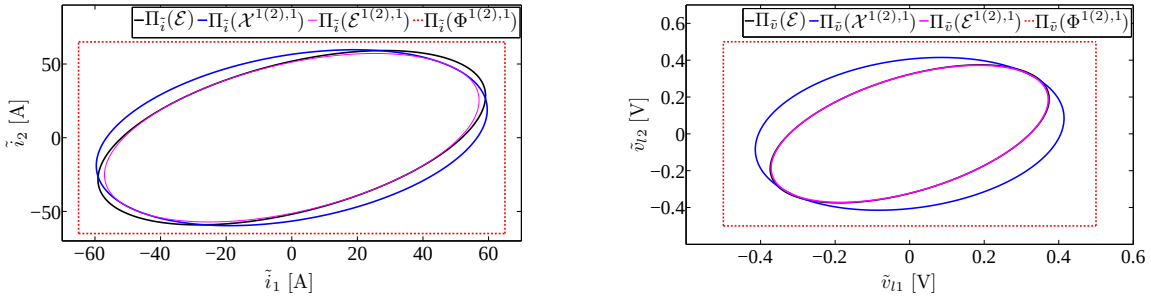
SINGLE FAULT CONDITIONS: ENTRIES OF THE MATRIX $\Xi^{i,1}$, WHERE $i = 1, 2, 3, 4, 5, 6$.

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

TABLE V

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

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



(a) Subspace defined by $\tilde{i}_1, \tilde{i}_2$: Projections of ellipsoids $\mathcal{E}$, $\mathcal{E}^{1(2),1}$ and $\mathcal{X}^{1(2),1}$, and projection of performance requirements region $\Phi^{1(2),1}$.

(b) Subspace defined by $\tilde{v}_{l1}, \tilde{v}_{l2}$: Projections of ellipsoids $\mathcal{E}$, $\mathcal{E}^{1(2),1}$ and $\mathcal{X}^{1(2),1}$, and projection of performance requirements region $\Phi^{1(2),1}$.

Fig. 9. DC power system dynamic behavior for an open-circuit fault in R_3 or R_4: projections of the bounding ellipsoid on to the subspaces defined by the $\tilde{i}_1, \tilde{i}_2$ axes, and the $\tilde{v}_{l1}, \tilde{v}_{l2}$ axes.

capacitors C_1 and C_2 and $S^2_{v_{l1}}$ and $S^2_{v_{l2}}$, the solution of (17) yields an ellipsoid fully contained in $\hat{\Phi}$, therefore, there exists a solution to (18-20) and (21-23). For each particular fault, the entries of the matrix $\hat{\Xi}$ obtained from (18-20) take the values in Table IV, and the entries of the corresponding matrix $\hat{\Upsilon}$ 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 $\hat{\Upsilon}$ (fourth column of Table III) and the determinant of Υ (first column of Table II). In all Tables III, IV and V, following the notation

used in Section IV, we replace " ˆ " by a double index when referring to each particular $\hat{\Xi}$ and $\hat{\Upsilon}$. For the case when one of the links between buses 1 and 2 fails, Fig. 9 shows he projections of the ellipsoids $\mathcal{E}$, $\mathcal{E}^{1(2),1}$ and $\mathcal{X}^{1(2),1}$ on to the subspaces defined by the $\tilde{i}_1, \tilde{i}_2$ axes, and the $\tilde{v}_{l1}, \tilde{v}_{l2}$ axes, which we denote by $\Pi_{\tilde{i}}(\mathcal{E})$, $\Pi_{\tilde{i}}(\mathcal{E}^{1(2),1})$, $\Pi_{\tilde{i}}(\mathcal{X}^{1(2),1})$ and $\Pi_{\tilde{v}}(\mathcal{E})$, $\Pi_{\tilde{v}}(\mathcal{E}^{1(2),1})$, $\Pi_{\tilde{v}}(\mathcal{X}^{1(2),1})$ respectively.

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 $S^2_{v_{l1(2)}}$, which are the only first faults with non zero fault coverage. From previous results, any two-fault sequence with a second fault in $S_{i_1(2)}$ or $S^1_{v_{l1(2)}}$ 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.

TABLE VI

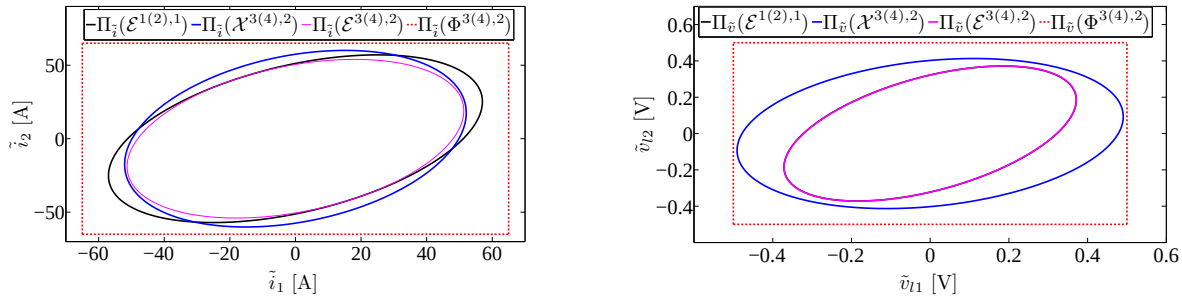
DOUBLE FAULT CONDITIONS: SEQUENCES OF FAULTS WITH NON-ZERO FAULT COVERAGE.

Sequence	*Second fault effect*	*Index*	$\det(\Upsilon^{i,1})$	$\det(\Upsilon^{j,2})$	*Second fault coverage*
$\mathrm{R}_3 \rightarrow \mathrm{R}_4$, $\mathrm{R}_4 \rightarrow \mathrm{R}_3$	$\mathrm{R}_{4(3)} = \infty$	[1,2], [2,,2]	$1.23 \cdot 10^5$	$1.11 \cdot 10^5$	$c_{rr} = 0.95$
$\mathrm{R}_3 \rightarrow \mathrm{C}_{1(2)}$, $\mathrm{R}_4 \rightarrow \mathrm{C}_{1(2)}$	$\mathrm{C}_{1(2)}/2$	[3(4),2], [5(6),2]	$1.23 \cdot 10^5$	$9.58 \cdot 10^4$	$c_{rc} = 0.88$
$\mathrm{R}_3 \rightarrow \mathrm{S}^2_{v_{l1(2)}}$, $\mathrm{R}_4 \rightarrow \mathrm{S}^2_{v_{l1(2)}}$	$k_{14(23)} = 0$	[7(8),2], [9(10),2]	$1.23 \cdot 10^5$	$1.22 \cdot 10^5$	$c_{rv} = 0.99$
$\mathrm{C}_1 \rightarrow \mathrm{C}_2$, $\mathrm{C}_2 \rightarrow \mathrm{C}_1$	$\mathrm{C}_{2(1)}/2$	[11,2], [12,2]	$7.67 \cdot 10^4$	$4.83 \cdot 10^4$	$c_{cc} = 0.79$
$\mathrm{C}_1 \rightarrow \mathrm{R}_{3(4)}$, $\mathrm{C}_2 \rightarrow \mathrm{R}_{3(4)}$	$\mathrm{R}_{3(4)} = \infty$	[13(14),2], [15(16),2]	$7.67 \cdot 10^4$	$7.49 \cdot 10^4$	$c_{cr} = 0.99$
$\mathrm{C}_1 \rightarrow \mathrm{S}^2_{v_{l1(2)}}$, $\mathrm{C}_2 \rightarrow \mathrm{S}^2_{v_{l1(2)}}$	$k_{14(23)} = 0$	[17(18),2], [19(20),2]	$7.67 \cdot 10^4$	$7.44 \cdot 10^4$	$c_{cv} = 0.98$
$\mathrm{S}^2_{v_{l1}} \rightarrow \mathrm{S}^2_{v_{l2(1)}}$, $\mathrm{S}^2_{v_{l2}} \rightarrow \mathrm{S}^2_{v_{l2(1)}}$	$k_{23(14)} = 0$	[21,2], [22,2]	$1.23 \cdot 10^5$	$1.18 \cdot 10^5$	$c_{vv} = 0.98$
$\mathrm{S}^2_{v_{l1}} \rightarrow \mathrm{R}_{3(4)}$, $\mathrm{S}^2_{v_{l2}} \rightarrow \mathrm{R}_{3(4)}$	$\mathrm{R}_{3(4)} = \infty$	[23(24),2], [25(26),2]	$1.23 \cdot 10^5$	$1.17 \cdot 10^5$	$c_{vr} = 0.97$
$\mathrm{S}^2_{v_{l1}} \rightarrow \mathrm{C}_{1(2)}$, $\mathrm{S}^2_{v_{l2}} \rightarrow \mathrm{C}_{1(2)}$	$\mathrm{C}_{1(2)}/2$	[27(28),2], [29(30),2]	$1.23 \cdot 10^5$	$8.88 \cdot 10^4$	$c_{vc} = 0.85$

TABLE VII

DC DISTRIBUTION SYSTEM: COMPONENT FAILURE RATE EXAMPLE VALUES.

Component	$\mathrm{R}_{3(4)}$	$\mathrm{C}_{1(2)}$	$\mathrm{S}^2_{v_{l1(2)}}$	$\mathrm{S}_{i_{1(2)}}$	$\mathrm{S}^1_{v_{l1(2)}}$
Failure rate (/h)	$\lambda_r = 10^{-7}$	$\lambda_c = 10^{-8}$	$\lambda_v = 10^{-9}$	$\lambda_v = 10^{-9}$	$\lambda_i = 10^{-9}$



(a) Subspace defined by $\tilde{i}_1, \tilde{i}_2$: Projections of ellipsoids $\mathcal{E}$, $\mathcal{E}^{1(2),1}$ and $\mathcal{X}^{1(2),1}$, and projection of performance requirements region $\Phi^{1(2),1}$.

(b) Subspace defined by $\tilde{v}_{l1}, \tilde{v}_{l2}$: Projections of ellipsoids $\mathcal{E}$, $\mathcal{E}^{1(2),1}$ and $\mathcal{X}^{1(2),1}$, and projection of performance requirements region $\Phi^{1(2),1}$.

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: projections of the bounding ellipsoid on to the subspaces defined by the $\tilde{i}_1, \tilde{i}_2$ axes, and the $\tilde{v}_{l1}, \tilde{v}_{l2}$ axes (for simplicity, the legend for projections $\mathcal{E}^{5(6),2}$ was omitted since these projections are equivalent to $\mathcal{E}^{3(4),2}$).

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 considere 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. In order to complete the numerical analysis, in Table VII we provide a reasonable order of magnitude for each component failure rate.

Table IX of the Appendix collects the parametrical expressions of the non-zero entries of the Markov reliability model generator matrix, collecting also the corresponding numerical values when the model parameters (component failure rates and fault coverage for first and second faults) take the values in Tables III, VI and VII. 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 following information: 1) the fault events associated to each state of the Markov model; 2) the resulting outcome, i.e., whether or not the system is still operational after each fault event; and 3) the associated probabilities for the considered evaluation time. A lower bound $\hat{R}$ 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 $\hat{R} = 0.99952$. As explained in [39], the probability of the final absorbing state 18 is the upper bound on the reliability estimate error $e_R = 2.66 \cdot 10^{-9}$. Thus, the true reliability estimate R is bounded as follows: $\hat{R} \leq R \leq \hat{R} + e_r$, from where we conclude that truncating the analysis after sequences of two faults yields an accurate reliability estimate.

VII. Concluding Remarks

In this paper, we proposed a fault coverage model for LTI systems where the system input is considered to be unknown but bounded, where the bound is described by an ellipsoid; the performance requirements constrain the system trajectories to regions of the state-space defined by a symmetrical polytope; and behavioral decomposition holds, i.e, the time constants

TABLE VIII

DC distribution system: Markov reliability model probabilities at the end of the evaluation period (23,000 hours).

Markov State	*Fault event*	*Outcome*	*Probability*
1	nil	Operational	0.99482
2	$\{R_{3(4)}$ covered$\}$	Operational	$4.31 \cdot 10^{-3}$
3	$\{C_{1(2)}$ covered $\}$	Operational	$3.39 \cdot 10^{-4}$
4	$\{S^2_{v_{l1(2)}}$ covered $\}$	Operational	$4.35 \cdot 10^{-5}$
5	$\{R_{3(4)}$ uncovered$\}$ or $\{C_{1(2)}$ uncovered$\}$ or $\{S^1_{v_{l1(2)}}$ uncovered$\}$ or $\{S^2_{v_{l1(2)}}$ uncovered$\}$ or $\{S_{i_{1(2)}}$ uncovered$\}$	Failed	$4.88 \cdot 10^{-4}$
6	$\{R_3$ covered$\rightarrow R_4$ covered$\}$ or $\{R_4$ covered$\rightarrow R_3$ covered$\}$	operational	$4.71 \cdot 10^{-6}$
7	$\{R_3$ covered $\rightarrow C_{1(2)}$ covered$\}$ or $\{R_4$ covered $\rightarrow C_{1(2)}$ covered$\}$	operational	$8.72 \cdot 10^{-7}$
8	$\{R_3$ covered $\rightarrow S^2_{v_{l1(2)}}$ covered$\}$ or $\{R_4$ covered $\rightarrow S^2_{v_{l1(2)}}$ covered$\}$	operational	$9.81 \cdot 10^{-8}$
9	$\{R_3$ covered $\rightarrow R_4$ uncovered$\}$ or $\{R_4$ covered $\rightarrow R_3$ uncovered$\}$ or $\{R_3$ covered $\rightarrow C_{1(2)}$ uncovered$\}$ or $\{R_4$ covered$\rightarrow C_{1(2)}$ uncovered$\}$ or $\{R_3$ covered$\rightarrow S^1_{v_{l1(2)}}$ uncovered$\}$ or $\{R_4$ covered$\rightarrow S^1_{v_{l1(2)}}$ uncovered$\}$ or $\{R_3$ covered$\rightarrow S^2_{v_{l1(2)}}$ uncovered$\}$ or $\{R_4$ covered$\rightarrow S^2_{v_{l1(2)}}$ uncovered$\}$ or $\{R_3$covered$\rightarrow S_{i_{1(2)}}$uncovered$\}$ or $\{R_4$ covered$\rightarrow S_{i_{1(2)}}$uncovered$\}$	failed	$5.66 \cdot 10^{-7}$
10	$\{C_1$ covered$\rightarrow C_2$ covered$\}$ or $\{C_2$ covered$\rightarrow C_1$ covered$\}$	operational	$3.08 \cdot 10^{-8}$
11	$\{C_1$ covered$\rightarrow R_{3(4)}$ covered$\}$ or $\{C_2$ covered$\rightarrow R_{(3)4}$ covered$\}$	operational	$7.72 \cdot 10^{-7}$
12	$\{C_1$ covered$\rightarrow S^2_{v_{l1(2)}}$ covered$\}$ or $\{C_2$ covered$\rightarrow S^2_{v_{l1(2)}}$ covered$\}$	operational	$7.63 \cdot 10^{-9}$
13	$\{C_1$ covered $\rightarrow C_2$ uncovered$\}$ or $\{C_2$ covered $\rightarrow C_1$ uncovered$\}$ or $\{C_1$ covered $\rightarrow R_{3(4)}$uncovered$\}$ or $\{C_2$ covered$\rightarrow R_{3(4)}$ uncovered$\}$ or $\{C_1$ covered$\rightarrow S^1_{v_{l1(2)}}$ uncovered$\}$ or $\{C_2$ covered$\rightarrow S^1_{v_{l1(2)}}$uncovered$\}$ or $\{C_1$ covered$\rightarrow S^2_{v_{l1(2)}}$ uncovered$\}$ or $\{C_2$ covered$\rightarrow S^2_{v_{l1(2)}}$ uncovered$\}$ or $\{C_1$covered$\rightarrow S_{i_{1(2)}}$ uncovered$\}$ or $\{C_2$ covered$\rightarrow S_{i_{1(2)}}$ uncovered$\}$	failed	$3.18 \cdot 10^{-8}$
14	$\{S^2_{v_{l1}}$ covered$\rightarrow S^2_{v_{l2}}$ covered$\}$ or $\{S^2_{v_{l2}}$ covered$\rightarrow S^2_{v_{l1}}$ covered$\}$	operational	$4.90 \cdot 10^{-10}$
15	$\{S^2_{v_{l1}}$ covered $\rightarrow R_{3(4)}$ covered$\}$ or $\{S^2_{v_{l2}}$ covered $\rightarrow R_{3(4)}$ covered$\}$	operational	$9.71 \cdot 10^{-8}$
16	$\{S^2_{v_{l1}}$ covered$\rightarrow C_{1(2)}$ covered$\}$ or $\{S^2_{v_{l2}}$ covered$\rightarrow C_{1(2)}$ covered$\}$	operational	$8.50 \cdot 10^{-9}$
17	$\{S^2_{v_{l1}}$ covered$\rightarrow S^2_{v_{l2}}$ uncovered$\}$ or $\{S^2_{v_{l2}}$ covered$\rightarrow S^2_{v_{l1}}$ uncovered$\}$ or $\{S^2_{v_{l1}}$covered$\rightarrow R_{3(4)}$ uncovered$\}$ or $\{S^2_{v_{l2}}$ covered$\rightarrow R_{3(4)}$ uncovered$\}$ or $\{S^2_{v_{l1}}$covered $\rightarrow C_{1(2)}$ uncovered$\}$ or $\{S^2_{v_{l2}}$ covered $\rightarrow C_{1(2)}$ uncovered$\}$ or $\{S^2_{v_{l1}}$ covered$\rightarrow S^1_{v_{l1(2)}}$ uncovered$\}$ or $\{S^2_{v_{l2}}$ covered$\rightarrow S^1_{v_{l1(2)}}$ uncovered$\}$ or $\{S^2_{v_{l1}}$covered$\rightarrow S_{i_{1(2)}}$ uncovered$\}$ or $\{S^2_{v_{l2}}$ covered$\rightarrow S_{i_{1(2)}}$ uncovered$\}$	failed	$6.52 \cdot 10^{-9}$
18	Any additional transition out of Markov states 6, 7, 8, 10. 11, 12, 14, 15, and 16	nil	$2.66 \cdot 10^{-9}$

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, since our fault coverage model is formulated in terms of the system physical and performance parameters, it enables an integrated framework for analyzing 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.

In order to calculate fault coverage it is necessary to obtain 1) the system reach set before the fault occurrence, 2) the largest set contained in the pre-fault reach set, and 3) 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: 1) obtaining ellipsoidal bounds to the reach set, and 2) 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 n-dimensional case. We also discussed an important class of systems where the time 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.

It is important to 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, in order 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].

APPENDIX

TABLE IX

DC DISTRIBUTION SYSTEM MARKOV RELIABILITY MODEL: NON-ZERO ENTRIES OF THE STATE-TRANSITION MATRIX $\Lambda \in \mathbb{M}^{18\times 18}$.

Symbolic expression	*Numerical value (/h)*
$[\Lambda]_{1,1} = -2(\lambda_r + \lambda_c + 2\lambda_v + \lambda_i)$	$-2.26 \cdot 10^{-7}$
$[\Lambda]_{1,2} = 2c_r\lambda_r$	$1.88 \cdot 10^{-7}$
$[\Lambda]_{1,3} = 2c_c\lambda_c$	$1.48 \cdot 10^{-8}$
$[\Lambda]_{1,4} = 2c_v\lambda_v$	$1.9 \cdot 10^{-9}$
$[\Lambda]_{1,5} = 2(1-c_r)\lambda_r + 2(1-c_c)\lambda_c + 2(1-c_v)\lambda_v + 2\lambda_v + 2\lambda_i$	$2.13 \cdot 10^{-8}$
$[\Lambda]_{2,2} = -(\lambda_r + 2\lambda_c + 4\lambda_v + 2\lambda_i)$	$-1.26 \cdot 10^{-7}$
$[\Lambda]_{2,6} = c_{rr}\lambda_r$	$9.5 \cdot 10^{-8}$
$[\Lambda]_{2,7} = 2c_{rc}\lambda_c$	$1.76 \cdot 10^{-8}$
$[\Lambda]_{2,8} = 2c_{rv}\lambda_v$	$1.98 \cdot 10^{-9}$
$[\Lambda]_{2,9} = (1-c_{rr})\lambda_r + 2(1-c_{rc})\lambda_c + 2(1-c_{rv})\lambda_v + 2\lambda_v + 2\lambda_i$	$1.14 \cdot 10^{-8}$
$[\Lambda]_{3,3} = -(2\lambda_r + \lambda_c + 4\lambda_v + 2\lambda_i)$	$-2.16 \cdot 10^{-7}$
$[\Lambda]_{3,10} = c_{cc}\lambda_c$	$7.9 \cdot 10^{-9}$
$[\Lambda]_{3,11} = 2c_{cr}\lambda_r$	$1.98 \cdot 10^{-7}$
$[\Lambda]_{3,12} = 2c_{cv}\lambda_v$	$1.96 \cdot 10^{-9}$
$[\Lambda]_{3,13} = 2(1-c_{cr})\lambda_r + (1-c_{cc})\lambda_c + 2(1-c_{cv})\lambda_v + 2\lambda_v + 2\lambda_i$	$8.14 \cdot 10^{-9}$
$[\Lambda]_{4,4} = -(2\lambda_r + 2\lambda_c + 3\lambda_v + 2\lambda_i)$	$-2.25 \cdot 10^{-7}$
$[\Lambda]_{4,14} = c_{vv}\lambda_v$	$9.8 \cdot 10^{-10}$
$[\Lambda]_{4,15} = 2c_{vr}\lambda_r$	$1.94 \cdot 10^{-7}$
$[\Lambda]_{4,16} = 2c_{vc}\lambda_c$	$1.7 \cdot 10^{-8}$
$[\Lambda]_{4,17} = 2(1-c_{vr})\lambda_r + 2(1-c_{vc})\lambda_c + (1-c_{vv})\lambda_v + 2\lambda_v + 2\lambda_i$	$1.302 \cdot 10^{-8}$
$[\Lambda]_{6,6} = -2(\lambda_c + 2\lambda_v + \lambda_i)$	$-2.6 \cdot 10^{-8}$
$[\Lambda]_{6,18} = 2(\lambda_c + 2\lambda_v + \lambda_i)$	$2.6 \cdot 10^{-8}$
$[\Lambda]_{7,7} = -(\lambda_r + \lambda_c + 4\lambda_v + 2\lambda_i)$	$-1.16 \cdot 10^{-7}$
$[\Lambda]_{7,18} = \lambda_r + \lambda_c + 4\lambda_v + 2\lambda_i$	$1.16 \cdot 10^{-7}$
$[\Lambda]_{8,8} = -(\lambda_r + 2\lambda_c + 3\lambda_v + 2\lambda_i)$	$-1.25 \cdot 10^{-7}$
$[\Lambda]_{8,18} = \lambda_r + 2\lambda_c + 3\lambda_v + 2\lambda_i$	$1.25 \cdot 10^{-7}$
$[\Lambda]_{10,10} = -2(\lambda_r + 2\lambda_v + \lambda_i)$	$-2.06 \cdot 10^{-7}$
$[\Lambda]_{10,18} = 2(\lambda_r + 2\lambda_v + \lambda_i)$	$2.06 \cdot 10^{-7}$
$[\Lambda]_{11,11} = -(\lambda_r + \lambda_c + 4\lambda_v + 2\lambda_i)$	$-1.15 \cdot 10^{-7}$
$[\Lambda]_{11,18} = \lambda_r + \lambda_c + 4\lambda_v + 2\lambda_i$	$1.15 \cdot 10^{-7}$
$[\Lambda]_{12,12} = -(2\lambda_r + 3\lambda_v + \lambda_c + 2\lambda_i)$	$-2.15 \cdot 10^{-7}$
$[\Lambda]_{12,18} = 2\lambda_r + 3\lambda_v + \lambda_c + 2\lambda_i$	$2.15 \cdot 10^{-7}$
$[\Lambda]_{14,14} = -2(\lambda_r + \lambda_c + \lambda_v + \lambda_i)$	$-2.24 \cdot 10^{-7}$
$[\Lambda]_{14,18} = 2(\lambda_r + \lambda_c + \lambda_v + \lambda_i)$	$2.24 \cdot 10^{-7}$
$[\Lambda]_{15,15} = -(\lambda_r + 2\lambda_c + 3\lambda_v + 2\lambda_i)$	$-1.25 \cdot 10^{-7}$
$[\Lambda]_{15,18} = \lambda_r + 2\lambda_c + 3\lambda_v + 3\lambda_v + 2\lambda_i$	$1.25 \cdot 10^{-7}$
$[\Lambda]_{16,16} = -(2\lambda_r + \lambda_c + 3\lambda_v + 2\lambda_i)$	$-2.15 \cdot 10^{-7}$
$[\Lambda]_{16,18} = 2\lambda_r + \lambda_c + 3\lambda_v + 2\lambda_i$	$2.15 \cdot 10^{-7}$

TABLE X

DC DISTRIBUTION SYSTEM MARKOV RELIABILITY MODEL: STATE-TRANSITION MATRIX PARAMETER VALUES.

λ_r (/h)	λ_c (/h)	λ_v (/h)	λ_i (/h)	c_r	c_c	c_v	c_{rr}	c_{rc}	c_{rv}	c_{cc}	c_{cr}	c_{cv}	c_{vv}	c_{vr}	c_{vc}
10^{-7}	10^{-8}	10^{-9}	10^{-9}	0.94	0.74	0.95	0.95	0.88	0.99	0.79	0.99	0.98	0.98	0.97	0.85

REFERENCES

[1] J. Laprie, Ed., *Dependability: Basic Concepts and Terminology*. New York, NY: Springer-Verlag, 1991.

[2] W. Bouricius, W. Carter, and P. Schneider, "Reliability modeling techniques for self-repairing computer systems," in *Proceedings of the* 24^{th} *National ACM Conference*. New York, NY: ACM Press, 1969.

[3] T. Arnold, "The concept of coverage and its effect on the reliability model a repairable system," *IEEE Transactions on Computers*, vol. C-22, no. 3, pp. 251–254, March 1973.

[4] J. Dugan and K. Trivedi, "Coverage modeling for dependability analysis of fault-tolerant systems," *IEEE Transactions on Computers*, vol. 38, no. 6, pp. 775–787, June 1989.

[5] J. Stiffler and L. Bryant, "Care III phase II report –mathematical description," National Aeronautics and Space Administration, Tech. Rep. NASA-CR-3566, November 1982.

[6] K. Trivedi and R. Geist, "Decomposition in reliability analysis of fault-tolerant systems," *IEEE Transactions on Reliability*, vol. R-32, pp. 463–468, December 1983.

[7] D. Pradhan, Ed., *Fault-Tolerant Computer System Design*. New Jersey, NJ: Prentice Hall, 1995.

[8] M.-C. Hsueh, T. Tsai, and R. Iyer, "Fault injection techniques and tools," *Computer*, vol. 40, no. 4, pp. 75–82, April 1997.

[9] J. Arlat, A. Costes, Y. Crouzet, J.-C. Laprie, and D. Power, "Fault injection and dependability evaluation of fault-tolerant systems," *IEEE Transactions on Computers*, vol. 42, no. 8, pp. 913–923, August 1993.

[10] D. Powell, E. Martins, and J. Arlat, "Estimators for fault tolerance coverage evaluation," *IEEE Transactions on Computers*, vol. 44, no. 2, pp. 261–274, February 1995.

[11] M. Cukier, D. Powell, and J. Arlat, "Coverage estimation methods for stratified fault-injection," *IEEE Transactions on Computers*, vol. 48, no. 7, pp. 707–723, July 1999.

[12] L. Kaufman, B. Johnson, and J. Dugan, "Coverage estimation using statistics of the extremes for when testing reveals no failures," *IEEE Transactions on Computers*, vol. 51, no. 1, pp. 3–12, January 2002.

[13] C. Constantinescu, "Estimation of coverage probabilities for dependability validation of fault-tolerant computing systems," in *Proceedings of the* 9^{th} *Annual Conference on Computer Assurance*, June 1994, pp. 101–106.

[14] ——, "Using multi-stage and stratified sampling for inferring fault-coverage probabilities," *IEEE Transactions on Reliability*, vol. 44, no. 4, pp. 632–639, December 1995.

[15] D. Luenberger, Ed., *Introduction to Dynamic Systems*. New York, NY: John Wiley, 1979.

[16] A. Amendola, "Event sequences and consequence spectrum: A methodology for probabilistic transient analysis," *Nuclear Science An Engineering*, vol. 77, no. 3, pp. 297–315, March 1981.

[17] T. Aldemir, "Computer-assisted markov failure modeling of process control systems," *IEEE Transactions on Reliability*, vol. R-36, no. 1, pp. 133–144, Apr. 1987.

[18] J. Devooght and C. Smidts, "Probabilistic reactor dynamics-I: The theory of continuos event trees," *Nuclear Science and Engineering*, vol. 111, no. a, pp. 229–240, a 1992.

[19] ——, "Probabilistic dynamics as a tool for dynamic PSA," *Reliability Engineering and System Safety*, vol. 52, no. 3, pp. 185–196, June 1996.

[20] P. Labeau, C. Smidts, and S. Swaminathan, "Dynamic reliability: Towards an integrated platform for probabilistic risk assessment," *Journal of Reliability Engineering and System Safety*, vol. 68, no. 3, pp. 219–254, June 2000.

[21] A. Kurzhanski and P. Varaiya, "Ellipsoidal techniques for reachability analysis. parts I & II," *Optimization Methods and Software*, vol. 17, pp. 177–206 and 207–237, February 2002.

[22] F. Schweppe, *Uncertain Dynamic Systems*. Englewood Cliffs, NJ: Prentice-Hall Inc., 1973.

[23] A. Kurzhanski and I. Vályi, *Ellipsoidal Calculus for Estimation and Control*. Boston, MA: Birkhauser, 1997.

[24] F. Chernousko, "What is ellipsoidal modelling and how to use it for control and state estimation," in *Whys and Hows in Uncertainty Modelling: Probability, Fuzziness, and Anti-Optimization*, ser. CISM Courses and Lectures, I. Elishakoff, Ed. Vienna, Austria: Springer, 1999, ch. 3, pp. 127–188.

[25] F. Chernousko and A. Ovseevich, "Properties of the optimal ellipsoids approximating the reachable sets of uncertain systems," *Optimization Theory and Applications*, vol. 120, no. 2, pp. 223–246, February 2004.

[26] F. Blanchini, "Set invariance in control," *Automatica*, vol. 35, pp. 1747–1767, 1999.

[27] M. Kendall, *A course in the Geometry of n Dimensions*. New York, NY: Hafner, 1961.

[28] S. Boyd, L. E. Ghaoui, E. Feron, and V. Balakrishnan, *Linear Matrix Inequalities in System and Control Theory*. Philadelphia, PA: Society for Industrial and Applied Mathematics, 1994.

[29] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, UK: Cambridge University Press, 2004.

[30] M. Grant and S. Boyd. (October, 2008) Matlab software for disciplined convex programming. [Online]. Available: http://stanford.edu/ boyd/cvx.

[31] G. Grimmett and D. Stirzaker, *Probability and Random Processes*, 3rd ed. Oxford, UK: Oxford University Press, 2001.

[32] K. Åström, *Introduction to Stochastic Control Theory*. New York, NY: Academic Press, 1970.

[33] D. Bertsimas and J. Sethuraman, "Moment problems and semidefinite optimization," in *Handbook of semidefinite programming*, ser. Internat. Ser. Oper. Res. Management Sci. Boston, MA: Kluwer Acad. Publ., 2000, vol. 27, pp. 469–509.

[34] L. Vandenberghe, Boyd, and K. Comanor, "Generalized Chebyshev bounds via semidefinite programming," *SIAM Review*, vol. 49, no. 1, pp. 52–64, May 2007.

[35] K. Mistry, E. Silverman, T. Taylor, and R. Willis, "Telecommunications power architectures: Distributed or centralized," in *Proceedings of the 11^{th} Telecommunications Energy Conference*, October 1989.

[36] M. Grant and S. Boyd, "Graph implementations for nonsmooth convex programs," in *Recent Advances in Learning and Control (a tribute to M. Vidyasagar)*, ser. Lecture Notes in Control and Information Sciences, V. Blondel, S. Boyd, and H. Kimura, Eds. Berlin, Germany: Springer, 2008, pp. 95–100.

[37] M. Rausand and A. Høyland, *System Reliability Theory*, 2nd ed. New York, NY: John Wiley and Sons, 2004.

[38] P. Babcock, "An introduction to reliability modeling of fault-tolerant systems," The Charles Stark Draper Laboratory, Cambridge, MA, Tech. Rep. CSDL-R-1899, 1986.

[39] P. Babcock, G. Rosch, and J. Zinchuk, "An automated environment for optimizing fault-tolerant systems design," in *Proceedings of the Reliability and Maintainability Symposium*, Orlando, FL, 1991, pp. 360–367.

[40] D. Bertsimas and I. Popescu, "Optimal inequalities in probability theory: A convex optimization approach," *SIAM J. on Optimization*, vol. 15, no. 3, pp. 780–804, 2005.