Integrating Reliability into the Design of Fault-Tolerant Power Electronics Systems

Alejandro D. Domínguez-García* and Philip T. Krein
Grainger Center for Electric Machinery and Electromechanics
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign
Urbana, IL 61801
USA
*E-mail: aledan@UIUC.EDU

***Abstract*—This paper presents a methodology for integrating reliability considerations into the performance analysis carried out during the design of fault-tolerant power converters. The methodology relies on using a state-space representation of the power converter, based on averaging, similar to the ones used when analyzing linear time-invariant systems, and assumes an unknown-but-bounded uncertainty model for the converter uncontrolled inputs, such as load or variations in input voltage. The converter must be designed such that, for any uncontrolled input, the state variables remain within a region of the state space defined by performance requirements, e.g., output voltage tolerance or switch ratings. In the presence of component faults, and depending on the uncontrolled inputs, the converter may or may not meet performance requirements. Given the uncertain nature of these uncontrolled inputs, and for each particular fault, we introduce an analytical method to compute the probability that the performance requirements are met, which will define the reliability of the converter for each particular fault. By including these probabilities in a Markov reliability model, it is possible to obtain the overall converter reliability. The application of the methodology is illustrated with a case study of a fault-tolerant interleaved buck converter.**

I. Introduction

The safety and mission-critical nature of embedded systems used in aircraft, space, tactical, and automotive applications, mandates that the design functions be performed even in the presence of component faults. These systems are commonly referred to as fault-tolerant systems [1]. In this regard, reliable electric power generation and distribution systems are key to ensure that these safety and mission-critical systems remain operational at all times. This is usually achieved by introducing component and subsystem redundancy and appropriate strategies for managing this redundancy.

Design of effective and reliable fault-tolerant power electronics requires thorough and comprehensive analysis to implement the appropriate level of component and subsystem redundancy; to understand and quantify the potential effects of component faults in the overall system performance; and to design appropriate fault detection, isolation, and reconfiguration (FDIR) mechanisms for redundancy management.

There are well-developed techniques to support the reliability evaluation of conventional systems such as reliability block diagrams, fault trees, failure modes and effect analysis, and Markov models [2]. However, all these techniques can yield ambiguous or incomplete results as they base the analysis on a qualitative description of system functionality, thus relying on expert judgment and previous experience to understand the impact of component failures on the system functionality. The use of these techniques in power electronics has been widely reported; some examples include reliability block diagrams [3], failure modes and effects analysis (FMEA) [4], fault trees [5], and Markov models [6].

In this paper, we introduce a methodology to analyze the behavior of fault-tolerant power electronics systems in the presence of component faults. Rather than using a qualitative description of system functionality, this methodology uses a state-space representation of dynamics based on averaging and linearization. Although power electronics systems are nonlinear, averaged models are generally used to design controls. The issues and limitations of averaged models are well established.

The methodology takes into account the uncertainty associated with the converter uncontrolled inputs such as load input voltage variations. Although these variations can be described in several ways, our model assumes that the values the uncontrolled inputs can take are completely unknown, but the peak values are bounded by some known quantity. This particular way of modeling input uncertainty in an LTI system is known as *unknown but bounded* [7], and it is a reasonable model for describing the uncertainty in the values of converter load and voltage input. Then, by using techniques developed in the context of reachability analysis of LTI systems, the uncertainty in the uncontrolled inputs is propagated to the converter state variables, which also become uncertain. In a non-faulty condition, and given the converter is properly designed, the converter state variables must remain within a region of state space defined by the requirements of the specific application, e.g., output voltage tolerance or maximum current through the switches. In the presence of a component fault, the uncertainty in the uncontrolled variables will propagate differently to the converter state variables, which might result in the state variables being outside the region of the state space defined by the performance requirements. In this context, and for each fault, we analytically compute the probability that the converter will meet the performance requirements, which can

be interpreted as the reliability of the converter for a particular fault. The overall converter reliability is then calculated by including those probabilities into the formulation of a Markov reliability model.

In the context of power electronics, some work using quantitative models of system behavior has been done to determine the effects of variations in component parameters on system performance, and thus on reliability [8], [9]. The work in [9] is based on Monte Carlo analysis, which is computationally intensive. In this regard, if the converter performance (and thus its reliability) is to be evaluated for every possible component fault ρ, and every possible value of the uncontrolled inputs obtained by quantizing the uncontrolled input space, and denoted by $\mu_1 \times \mu_2 \times \cdots \times \mu_k$, where k is the number of uncontrolled inputs, the number of time-domain simulations to be conducted is $\rho \times \mu_1 \times \mu_2 \times \cdots \times \mu_k$. This is necessary to map out the set of reachable states for each possible fault. With the proposed methodology, since the set of reachable states is not mapped through simulation, but through analytical techniques, it is only necessary to conduct ρ simulations to evaluate the overall converter performance. Furthermore, mapping out the set of reachable states under all possible fault conditions with analytically tractable solutions enables the formulation of a tractable model for optimizing dynamic performance and system reliability jointly. The method proposed in [8], called the first-order reliability method (FORM) uses a constrained gradient-based optimization method, where time-domain simulations are also used to check system performance. With respect to Monte Carlo analysis, this method substantially decreases the number of time-domain simulations needed, but this number is still much larger that the number of component faults ρ, which is the number of simulations required in the method proposed in this paper.

The structure of this paper is as follows. Section II presents the mathematical formulation of the methodology, including how to assess the converter performance in the presence of faults; how to compute fault survival probabilities; and how to include these probabilities in the formulation of a Markov reliability model. Section III illustrates the application of the methodology to a fault-tolerant interleaved buck converter. Concluding remarks are presented in Section IV.

II. Mathematical Formulation

A. Fault-Free System Dynamics

The dynamics of a converter can be described using an averaged model. This averaged model is usually linearized and can be described using a state-space representation of the form

$$\frac{d\tilde{x}}{dt} = A\tilde{x} + B_c\tilde{d} + B_d\tilde{w}, \tag{1}$$

where $\tilde{x}$ represent the small variations of the converter states around the nominal point, $\tilde{d}$ represents the small variations of the converter switch duty ratios (controlled inputs), and $\tilde{w}$ represents the small variations of uncontrolled inputs, such as converter load and input voltage variations. Matrices A, B_c, and B_d are constant and functions of the physical parameters, nominal states and nominal duty ratios [10].

As stated in Section I, we assume the uncertainty in the uncontrolled input $\tilde{w}$ is described using an unknown-but-bounded model, i.e., the values $\tilde{w}$ takes are completely unknown, but the peak values are bounded by some known quantity. In particular, by assuming the inputs are bounded by ellipsoids, it is possible to obtain ellipsoidal approximations bounding the set of reachable states. This has been the subject of extensive research [7], [11], [12]. The values the uncontrolled input $\tilde{w}$ can take will be constrained to some ellipsoid $\Omega_{\tilde{w}}$ described by

$$\tilde{w} \in \Omega_{\tilde{w}} = \{\tilde{w} : \tilde{w}Q^{-1}w \leq 1\}, \tag{2}$$

where Q is a positive definite matrix.

Depending on the application, the converter must meet predefined performance requirements, e..g, the output voltage must be within a certain range of the nominal output voltage, or the current through the switches must not exceed certain limits at all times. These requirements will constrain the state trajectories to some predefined region of the state space denoted by Φ. To meet these requirements in the presence of uncertain variation in the uncontrolled input $\tilde{w}$, a feedback control of the form $\tilde{d} = K\tilde{x}$, where K is a constant matrix, is implemented. Thus, the closed-loop dynamics result in

$$\frac{d\tilde{x}}{dt} = A_c\tilde{x} + B_d\tilde{w}, \tag{3}$$

where $A_c = A + B_cK$, and $\tilde{w} \in \Omega_{\tilde{w}} = \{\tilde{w} : \tilde{w}Q^{-1}w \leq 1\}$.

The values the state variables $\tilde{x}$ can take will be contained in some set $\mathcal{R}$. The exact exact shape of $\mathcal{R}$ is usually not easy to compute. However, it is possible to compute a bounding ellipsoid, denoted by $\Omega_{\tilde{x}}$, such that $\mathcal{R} \subseteq \Omega_{\tilde{x}}$, and defined by

$$\Omega_{\tilde{x}} = \{\tilde{x} : \tilde{x}'\Psi^{-1}\tilde{x} \leq 1\}, \tag{4}$$

where Ψ can be obtained by solving

$$A_c\Psi + \Psi A_c' + \beta\Psi + \frac{1}{\beta}B_dQB_d' = 0, \tag{5}$$

with $\beta > 0$, and Ψ positive definite. The derivation of (5) can be found in [7]. Since $\Omega_{\tilde{x}}$ is an outer bound of the set of reachable states, there can be many different solutions to (5) for different values of β. Thus, when solving (5), it is necessary to find the particular value of β such that the content[1] of $\Omega_{\tilde{x}}$ is minimum, thus ensuring the bound is tight. There are several software packages that can solve this problem, such as CVX [13] or Ellipsoidal Toolbox [14].

As stated before, the predefined performance requirements of the particular application will constrain the state trajectories to some region of the state space Φ. Thus, if the converter is well designed, then the ellipsoid bounding the set of reachable defined in (4) and (5) must be fully contained in Φ.

[1]The notion of content in an n-dimensional Cartesian space is equivalent to the notion of volume in a three-dimensional space, or to the notion of area in a two-dimensional space [15].

As explained in Section I, by quantizing the uncontrolled input space defined by (2) and simulating the system response for each value of the quantized input space, it is possible to map out the set of reachable states $\mathcal{R}$ bounded by the ellipsoid defined in (4) and (5). However, this method is much more computationally expensive than the method used in this paper.

B. System Dynamics After a First Fault

After a fault in one of the converter components occur, one or both matrices A_c, B_d in (3) might be altered, resulting in a new pair $\hat{A}_c, \hat{B}_c$. Examples of faults are a switch failing open or short-circuit, a capacitor failing open circuit, or a sensor failing to send measurements to the controller. The small-signal state-space representation after the fault is defined by

$$\frac{d\tilde{x}}{dt} = \hat{A}_c\tilde{x} + \hat{B}_d\tilde{w}, \tag{6}$$

where $\tilde{w} \in \Omega_{\tilde{w}} = \{\tilde{w} : \tilde{w}Q^{-1}w \leq 1\}$. All possible values the state variables can take will be contained in some set $\hat{\mathcal{R}}$. As before, a bounding ellipsoid $\hat{\Omega}_{\tilde{x}} = \{\tilde{x} : \tilde{x}'\hat{\Psi}^{-1}\tilde{x} \leq 1\}$ such that $\hat{\mathcal{R}} \subseteq \hat{\Omega}_{\tilde{x}}$ can be defined, where $\hat{\Psi}$ is obtained by solving

$$\hat{A}_c\hat{\Psi} + \hat{\Psi}\hat{A}_c' + \hat{\beta}\hat{\Psi} + \frac{1}{\hat{\beta}}\hat{B}_dQ\hat{B}_d' = 0, \tag{7}$$

with $\hat{\beta} > 0$ and $\hat{\Psi}$ positive definite.

C. Fault Coverage (or Probability of Surviving a Fault)

Under a fault condition, it becomes necessary to assess whether the converter is still able to meet its performance requirements for all possible values of the uncontrolled input $\tilde{w}$, i.e, the extent to which the new bounding ellipsoid $\hat{\Omega}_{\tilde{x}}$ is contained in the region Φ defined by the performance requirements. This will define a probability measure of the reliability of the converter for a particular fault. This probability measure is commonly referred to as fault coverage [16], and it can be interpreted as the conditional probability that, given a fault has occurred altering the converter dynamics, the converter is still able to meet its performance requirements

As stated before, the time structure of the input $\tilde{w}$ is completely unknown except for its peak value, which results in the state variables $\tilde{x}$ being also completely unknown, except for the bound defined by the ellipsoid $\hat{\Omega}_{\tilde{x}}$. Thus, it is realistic to assume that $\tilde{x}$ is uniformly distributed over $\hat{\Omega}_{\tilde{x}}$.

Let T_i be a random variable representing the time to fault occurrence i. Let X be a random variable representing the values the converter states $\tilde{x}$ can take after the fault occurrence. Then, under the state uniform distribution assumption, and for a particular fault i, its fault coverage, denoted by c_i is obtained by computing

$$c_i = Pr\{X \in \Phi | T_i < t\} = \frac{\text{cont}(\hat{\Omega}_{\tilde{x}} \cap \Phi)}{\text{cont}(\hat{\Omega}_{\tilde{x}})}, \tag{8}$$

where cont$(\hat{\Omega}_{\tilde{x}} \cap \Phi)$ and cont$(\hat{\Omega}_{\tilde{x}})$ are the contents of $\hat{\Omega}_{\tilde{x}} \cap \Phi$ and $\hat{\Omega}_{\tilde{x}}$ respectively.

The result presented in (8) can be generalized to the case in which the converter has survived a sequence of $k-1$ faults, and then an additional fault k occurs [17].

D. Markov Reliability Model

In order to obtain the overall converter reliability, it is necessary to formulate a Markov reliability modeling including the fault coverage for each sequence of component faults, as well as the probability distributions of the time to occurrence of each fault [2].

Let us consider that, at any time $t \geq 0$, the converter 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. 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. Let $c_{j,k-1}^{i,k}$ denote the fault coverage after the k fault occurrence, that leads from the sequence $[j, k-1]$ to the sequence $[i, k]$. Then the stochastic behavior of the converter after the $[i, k]$ sequence of faults is defined by

$$\frac{d}{dt}\begin{bmatrix} p_{2i-1,k} \\ \\ p_{2i,k} \end{bmatrix} = \begin{bmatrix} c_{j,k-1}^{i,k}\lambda_{j,k-1}^{i,k} & -\sum_{N_k}\lambda_{i,k}^{m,k+1} \\ \\ (1-c_{j,k-1}^{i,k})\lambda_{j,k-1}^{i,k} & 0 \end{bmatrix} \begin{bmatrix} p_{2j-1,k-1} \\ \\ p_{2i-1,k} \end{bmatrix}, \tag{9}$$

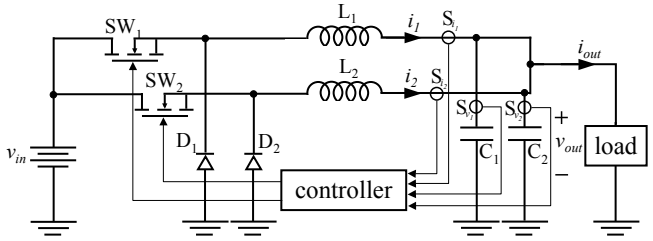
where $\lambda_{j,k-1}^{i,k}$ is the rate at which the last fault occurs in the sequence $[i, k]$, $\lambda_{i,k}^{m,k+1}$ is the rate at which a particular fault will occur next, and N_k is the number of possible faults that can occur after the last fault in the sequence $[i, k]$.

Each sequence of faults will generate a block similar to the one in (9). By assembling all these blocks, it is possible to obtain the state-transition matrix Λ associated with the system Markov reliability model. Let $P(t)$ be the fault sequences' probability vector, which can be obtained by assembling the individual fault sequence probabilities. Then the system Markov reliability model can be expressed in matrix form by

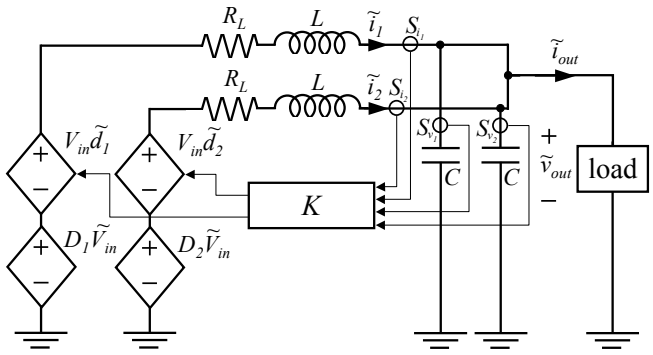
$$\begin{aligned} \tfrac{dP(t)}{dt} &= \Lambda P(t) \\ P(0) &= [1\ 0\ 0\ ...\ 0]'. \end{aligned} \tag{10}$$

III. Fault-Tolerant Interleaved Buck Converter Case-Study

In this section, we will show how to apply the proposed methodology in the design of a fault-tolerant converter. The goal is to design a buck converter for VRM applications that will withstand any first component fault. For a switching frequency of 250kHZ, a range of load specified by $|i_{load} - I_m| \leq I_m$, where $I_m = 20$A, an input voltage variation specified by $|v_{in} - V_{in}| \leq 0.2V_{in}$, where $V_{in} = 5$V, the converter design must satisfy an output voltage tolerance specified by $|v_{out} - V_{out}| \leq 0.025V_{out}$, where $V_{out} = 1.2$V. Additionally, the switch ratings will impose a requirement on the maximum value of the currents i_1 and i_2, denoted by I_1^{max} and I_2^{max}. The switch rating is defined as 105% of the maximum load.



(a) Converter architecture.



(b) Small-signal equivalent circuit.

Fig. 1. Dual-redundant buck converter

A. Dual-Redundant Architecture

It is clear that by using a single buck converter, the single fault-tolerant requirement will not be met. Thus, let us start with two buck converters arranged in parallel, Fig. 1(a), with full-state feedback of the form $[d_1, d_2]' = K[i_1, i_2, v_{out}]'$, where K is a 2-by-3 constant matrix and d_1 and d_2 are the duty ratios of switches SW_1 and SW_2. The current measurement devices denoted by S_{i_1} and S_{i_2} are just abstractions of possible current measurement techniques used in dc-dc conversion [18]. Although one voltage sensor would be enough to capture the output voltage v_{out}, a second sensor is necessary to fulfill the single fault-tolerance requirement. The controller will use the average of both measurements. In case the controller detects the failure of one sensor (omission), then it will reconfigure and use only the other sensor. It is important to note that this strategy will work for an omission failure mode as they are relatively easy to detect and isolate. If other sensor failure modes are to be considered, e.g., the sensor gets stuck at some value, then detecting which sensor of the two is failed becomes a difficult task. A possible solution to this problem would be to include a third sensor and then use voting strategies for failure detection and isolation as is common in aerospace [19]. This would increase the converter reliability by increasing the coverage to sensor faults, but it would also add more components and increase the cost.

By using common average modeling and linearization techniques, and following the notation used in (2) and (3), the small-signal model of this converter, Fig. 1(b), results in

$$\frac{d}{dt}\begin{bmatrix}\tilde{i}_1\\ \tilde{i}_2\\ \tilde{v}_{out}\end{bmatrix} = A_c\begin{bmatrix}\tilde{i}_1\\ \tilde{i}_2\\ \tilde{v}_{out}\end{bmatrix} + B_d\begin{bmatrix}\tilde{v}_{in}\\ \tilde{i}_{out}\end{bmatrix},$$
$$\tilde{w} = [\tilde{v}_{in}, \tilde{i}_{out}]' \in \Omega_{\tilde{w}} = \{\tilde{w} : \tilde{w}'Q^{-1}\tilde{w} \le 1\} \quad (11)$$

where

$$A_c = \begin{bmatrix} -\frac{R_L}{L} + k_{11}\frac{V_{in}}{L} & k_{12}\frac{V_{in}}{L} & -\frac{1}{L} + k_{13}\frac{V_{in}}{L} \\ k_{21}\frac{V_{in}}{L} & -\frac{R_L}{L} + k_{22}\frac{V_{in}}{L} & -\frac{1}{L} + k_{23}\frac{V_{in}}{L} \\ \frac{1}{2C} & \frac{1}{2C} & 0 \end{bmatrix},$$
$$B_d = \begin{bmatrix} \frac{D_1}{L} & 0 \\ \frac{D_2}{L} & 0 \\ 0 & -\frac{1}{2C} \end{bmatrix}, Q = \begin{bmatrix} 4\cdot 10^{-2}V_{in}^2 & 0 \\ 0 & I_m^2 \end{bmatrix}, \quad (12)$$

with D_1, and D_2 the nominal values of the duty ratios of switches SW_1 and SW_2 respectively; V_{in} the nominal value of the input voltage v_{in}; and $\tilde{i}_1, \tilde{i}_2, \tilde{v}_{out}, \tilde{v}_{in}, \tilde{i}_{out}, \tilde{d}_1$ and $\tilde{d}_2$, the small time-varying components of $i_1, i_2, v_{out}, v_{in}, i_{out}, d_1$ and d_2 respectively.

The design requirements constrain the values of $\tilde{i}_1, \tilde{i}_2$ and $\tilde{v}_{out}$ to a region of the state-space Φ defined by

$$\Phi = [-I_m, I_1^{max}] \times [-I_m, I_2^{max}] \times [-0.025V_{out}, +0.025V_{out}], \quad (13)$$

where $V_{out} = 1.2$V, and $I_1^{max} = I_2^{max} = 1.1I_m = 22$A, for a switch rating of 50%, and $I_1^{max} = I_2^{max} = 2.1I_m = 42$A for a switch rating of 100%.

TABLE I
DUAL-REDUNDANT CONVERTER PARAMETERS.

R_L [Ω]	0.002
L [H]	5×10^{-7}
C [F]	10^{-4}
$k_{11} = k_{21}$ [A^{-1}]	-200
$k_{12} = k_{22}$ [A^{-1}]	-200
$k_{13} = k_{23}$ [V^{-1}]	$-145 \cdot 10^3$
$D_1 = D_2$	0.24

Then, by choosing the parameters displayed in Table I, the design will meet the output voltage requirement; and by choosing a switch rating 50% higher, the requirement on the maximum current flowing through each branch will also be met. This can be shown by computing the ellipsoid that bounds the set of reachable states ($\tilde{i}_1 + \tilde{i}_2, \tilde{v}_{out}$), as explained in Section II-A. Thus, by following the notation of (4) and (5), for $\beta = 1.3 \cdot 10^5$, the entries of the matrix Ψ defining the bounding ellipsoid are $[\Psi]_{1,1} = 3.95 \cdot 10^2$, $[\Psi]_{1,2} = [\Psi]_{2,1} = -5.38 \cdot 10^{-1}$, and $[\Psi]_{2,2} = 7.60 \times 10^{-4}$. This ellipsoid is displayed in Fig. 2, where it can be seen that the region defined by the requirements fully contains it.

Let us turn our attention to the converter behavior in the presence of component faults. The components subject to failure are the inductors, capacitors, switches, diodes and voltage and current measurement devices. Information about components failure modes, associated failure rates and their effect on the overall systems dynamics is collected in Table II.

TABLE II
COMPONENT FAILURE MODES, EXAMPLE FAILURE RATES [20], [21], AND THEIR EFFECT ON THE OVERALL SYSTEM DYNAMICS.

Component	*Failure mode*	*Failure rate* (/h)	*Effect on system dynamics*
$L_{1(2)}$	Open circuit	$\lambda_L = 2 \cdot 10^{-9}$	$[A_c]_{1(2),1} = [A_c]_{1(2),2} = [A_c]_{1(2),3} = 0$,
$C_{1(2)}$	Open circuit	$\lambda_C = 8.7 \cdot 10^{-8}$	$[A_c]_{3,1} = [A_c]_{3,2} = 1/C$, $[B_d]_{3,2} = -1/C$
$SW_{1(2)}$	Open circuit	$\lambda_{SW} = 1.8 \cdot 10^{-9}$	$[A_c]_{1(2),1} = -R_L/L$, $[A_c]_{1(2),2} = 0$, $[A_c]_{1(2),3} = -1/L$, $[B_d]_{1(2),1} = 0$
$D_{1(2)}$	Short circuit	$\lambda_D = 10^{-9}$	$[A_c]_{1(2),1} = -R_L/L$, $[A_c]_{1(2),2} = 0$, $[A_c]_{1(2),3} = -1/L$, $[B_d]_{1(2),1} = 0$
$S_{i_{1(2)}}$	Omission	$\lambda_{S_i} = 10^{-10}$	$[A_c]_{1(2),1(2)} = -R_L/L$, $[A_c]_{2(1),1(2)} = 0$
S_v	Omission	$\lambda_{S_v} = 10^{-10}$	nil

TABLE III
FAULT COVERAGE PARAMETERS FOR DUAL-REDUNDANT CONVERTER WITH 50% SWITCH RATING.

Fault event	*Coverage*
L_1, L_2, D_1, D_2, SW_1, SW_2, S_{i_1}, or S_{i_2}	$c_1 = 0.63$
C_1 or C_2	$c_2 = 0.99$
$\{L_1, L_2, D_1, D_2, SW_1, SW_2, S_{i_1}$, or $S_{i_2}\}$ and $\{C_1$ or $C_1\}$	$c_3 = 0.93$
$\{C_1$ or $C_1\}$ and $\{L_1, L_2, D_1, D_2, SW_1, SW_2, S_{i_1}$, or $S_{i_2}\}$	$c_4 = 0.63$

Although one failure mode per component has been considered, it is possible to include other failure modes. For example, the current and voltage measurement devices could have other failure modes, such as output bias, or gain change.

The matrix $\hat{\Psi}_{SW}$ associated with the new bounding ellipsoid after the switch fault computed using (7) results in $[\hat{\Psi}_{SW}]_{1,1} = 3.90 \cdot 10^2$, $[\hat{\Psi}_{SW}]_{1,2} = [\hat{\Psi}_{SW}]_{2,1} = -5.26 \cdot 10^{-1}$, and $[\hat{\Psi}_{SW}]_{2,2} = 7.61 \times 10^{-4}$, for $\hat{\beta}_{SW} = 1.3 \cdot 10^5$. This ellipsoid, together with the region defined by the performance requirements for a switch rating of 50% is displayed in Fig. 3(a). It can be seen that the right side of the bounding ellipsoid is out of the allowed region, thus by using (8), and denoting by c_1 the coverage for this particular fault, we obtain $c_1 = 0.63$. Identical behavior was observed for single faults in the filter inductors, diodes and current measurement devices. Figure 3(b) shows the converter behavior after a fault in one of the capacitors. For $\hat{\beta}_{SW} = 2.2 \cdot 10^5$, the entries of the matrix associated with the bounding ellipsoid are $[\hat{\Psi}_C]_{1,1} = 5.40 \cdot 10^2$, $[\hat{\Psi}_C]_{1,2} = -7.30 \times 10^{-1}$, and $[\hat{\Psi}_C]_{2,2} = 1.05 \times 10^{-3}$, and the fault coverage results in $c_2 = 0.99$.

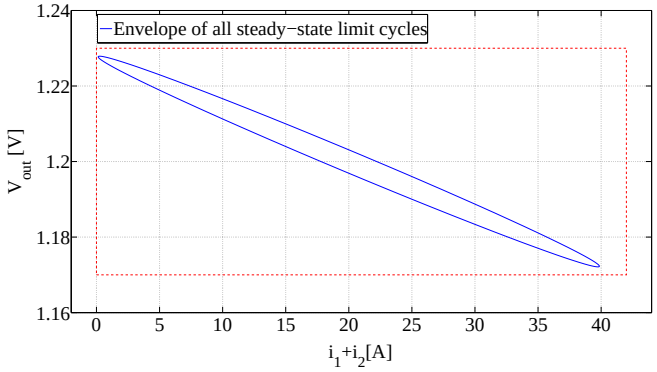
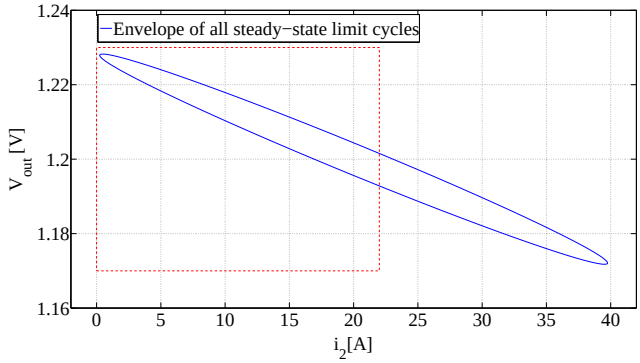
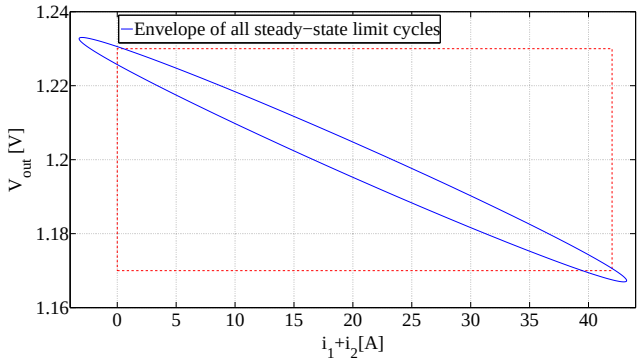


Fig. 2. Ellipsoid bounding the set of reachable states and non-faulty behavior.

The converter is also able to tolerate certain second faults. As displayed in Table III, an additional fault in one of the capacitors after any first fault in one of the inductors, diodes, switches, or current measurement devices will result in a fault coverage of $c_3 = 0.93$, whereas an additional fault in one of the inductors, diodes, switches, or current measurement devices after a fault in one of the capacitors results in a fault coverage of only $c_4 = 0.63$. This result may result counterintuitive as it seems that both fault events are the same (the same components have failed in both cases). However they are not, as the faults are not commutative and the sequence in which they occur is relevant. In this regard, once a certain fault has occur, only the region of the bounding ellipsoid that is left within the performance requirements region can originate an additional fault, thus affecting the coverage calculation.



(a) Behavior after a fault in switch SW_1.



(b) Behavior after capacitor fault.

Fig. 3. Behavior of dual-redundant converter with 50% switch ratings.

TABLE IV
DUAL-REDUNDANT CONVERTER MARKOV RELIABILITY MODEL PROBABILITIES AT THE END OF ITS LIFE-CYCLE (25,000 HOURS).

State	*Description*	*System Status*	*Probability*
1	The system is fault-free	Operational	$9.9571{\cdot}10^{-1}$
2	A covered fault in L_1, L_2, D_1, D_2, SW_1, SW_2, S_{i_1}, S_{i_2}, or a fault in S_{v_1} or S_{v_2}	Operational	$1.5852{\cdot}10^{-4}$
3	A covered fault in C_1 or C_2	Operational	$4.00{\cdot}10^{-3}$
4	An uncovered fault in L_1, L_2, D_1, D_2, SW_1, SW_2, S_{i_1}, or S_{i_2} or an uncovered fault in C_1 or C_2	Operational	$1.3087{\cdot}10^{-4}$
5	Fault event associated with state 2 followed by a covered fault in C_1 or C_2	Failed	$2.9883{\cdot}10^{-7}$
6	Fault event associated with state 2 followed by an uncovered fault in C_1, C_2 or a fault in one of the elements of the remaining non-failed branch	Failed	$1.9321{\cdot}10^{-7}$
7	Fault event associated with state 3 followed by a covered fault in SW_1, SW_2, L_1, L_2, D_1, D_2, S_{i_1}, S_{i_2}, or a fault in S_{v_1} or S_{v_2}	Operational	$3.1874{\cdot}10^{-7}$
8	Fault event associated with state 3 followed by an uncovered fault in SW_1, SW_2, RL_1, RL_2, D_1, D_2, S_{i_1} or S_{i_2} or a fault in the remaining capacitor	Failed	$4.2349{\cdot}10^{-6}$
9	Fault event associated with state 5 followed by an additional fault in any remaining non-faulty component	Failed	$2.1439{\cdot}10^{-10}$
10	Fault event associated with state 7 followed by an additional fault in any remaining non-faulty component	Failed	$2.2856{\cdot}10^{-10}$

TABLE V
NON-ZERO ENTRIES OF THE STATE-TRANSITION MATRIX $\Lambda \in M_{10}$ FOR THE DUAL-REDUNDANT CONVERTER MARKOV RELIABILITY MODEL.

$[\Lambda]_{1,1}$	$-2(\lambda_{SW}+\lambda_L+\lambda_C+\lambda_D+\lambda_{S_i}+\lambda_{S_v})$
$[\Lambda]_{2,1}$	$2c_1(\lambda_{SW}+\lambda_L+\lambda_D+\lambda_{S_i})$ +$2\lambda_{S_v}$
$[\Lambda]_{3,1}$	$2c_2\lambda_C$
$[\Lambda]_{4,1}$	$2(1-c_1)(\lambda_{SW}+\lambda_L+\lambda_D+\lambda_{S_i})+(1-2c_2)\lambda_C$
$[\Lambda]_{2,2}$	$-(\lambda_{SW}+\lambda_L+\lambda_C+\lambda_D+\lambda_{S_i}+\lambda_{S_v})-2\lambda_C$
$[\Lambda]_{5,2}$	$2c_3\lambda_C$
$[\Lambda]_{6,2}$	$2(1-c_3)\lambda_C+(\lambda_{SW}+\lambda_L+\lambda_C+\lambda_D+\lambda_{S_i}+\lambda_{S_v})$
$[\Lambda]_{3,3}$	$-2(\lambda_{SW}+\lambda_L+\lambda_D+\lambda_{S_i})$
$[\Lambda]_{7,3}$	$2c_4(\lambda_{SW}+\lambda_L+\lambda_D+\lambda_{S_i})+2\lambda_{S_v}$
$[\Lambda]_{8,3}$	$2(1-c_4)(\lambda_{SW}+\lambda_L+\lambda_D+\lambda_{S_i})+\lambda_C$
$[\Lambda]_{5,5}$	$-(\lambda_{SW}+\lambda_L+\lambda_D+\lambda_{S_i}+\lambda_C+\lambda_{S_v})$
$[\Lambda]_{9,5}$	$\lambda_{SW}+\lambda_L+\lambda_D+\lambda_{S_i}+\lambda_C+\lambda_{S_v}$
$[\Lambda]_{7,7}$	$-(\lambda_{SW}+\lambda_L+\lambda_D+\lambda_{S_i}+\lambda_C+\lambda_{S_v})$
$[\Lambda]_{10,7}$	$\lambda_{SW}+\lambda_L+\lambda_D+\lambda_{S_i}+\lambda_C+\lambda_{S_v}$

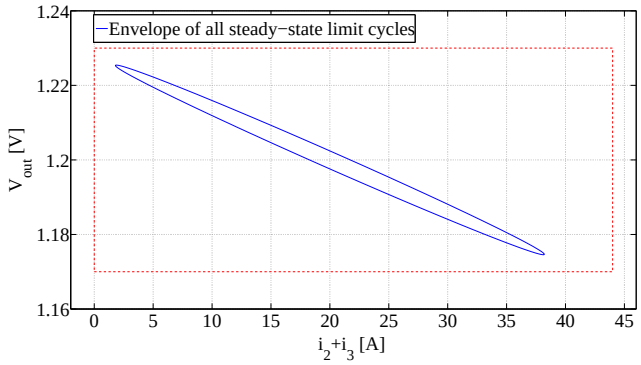
The converter overall reliability can be estimated by formulating a Markov reliability model as explained in Section II-D. Table IV describes the fault events associated with each state of the Markov reliability model, as well as the status of the system resulting from each fault event, i.e., whether or not the system still meets performance requirements after the fault event. The state probabilities can be obtained by solving (10), where the state-transition matrix Λ is obtained by substituting the fault coverage estimates displayed in Table III, and the failure rates displayed in Table II into the expressions displayed in Table V. For a life cycle of 25,000 hours, the resulting state probabilities are collected in the fourth column of Table IV. The overall converter reliability R can be obtained by adding up the probabilities of the Markov model operational states, resulting in $R = p_1 + p_2 + p_3 + p_4 + p_7 = 9.9987 \cdot 10^{-1}$ (unreliability $Q = p_5 + p_6 + p_8 + p_9 + p_{10} = 1.3122 \cdot 10^{-4}$).

B. Dual-Redundant Converter Improved Design

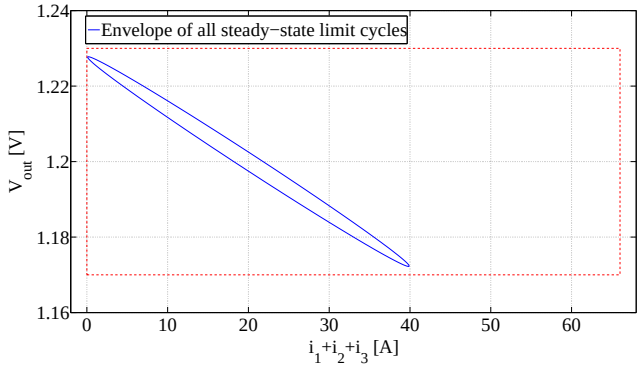
One of the dual-redundant converter design goals was to achieve single fault-tolerance. The design presented did not achieve this goal as the coverage of certain first faults is not complete, e.g., a fault in a switch or in one of the inductors is only covered with probability 0.63, whereas the coverage for a capacitor fault is 0.99. However, it is possible to make slightly modifications in the design to achieve fault coverage in all first faults. For example, by increasing the capacitance of the output filter by 20%, i.e., $C = 1.2 \cdot 10^{-4}$F, the coverage of any fault involving a capacitor increases to 1, i.e., $c_2 = c_3 = 1$. Additionally, by increasing the switch rating to 95%, the coverage of any fault involving a switch, a diode, an inductor, or a current measuring devices also increases to 1, i.e., $c_1 = c_4 = 1$. With this new fault coverage parameters, the converter reliability results in $R = 9.999997 \cdot 10^{-1}$ ($Q = 2.5843 \cdot 10^{-7}$). The improved design not only meets the single fault-tolerance requirement, but it is three orders of magnitude more reliable than the original design.

C. Triple-Redundant Architecture

If the converter reliability were to be improved further, then a possibility would be to decrease the component failure rates by using higher quality components. Although not always clear, adding more redundancy might increase reliability. However, including more redundancy for reliability seems to also increase the cost, but it is not clear either that this effect is multiplicative. In this regard, if we choose to add a third buck converter in parallel, using the same design parameters displayed in Table I, with a switch rating of only 50% (as opposed to the 95 % rating switches used in the improved dual-redundant buck converter), it is possible to achieve full coverage to all single faults as displayed in Figs. 4(a) and 4(b). As it can be seen, in both cases, the ellipsoids bounding the set of all steady-state limit cycles are fully contained within the region defined by the performance requirements, which means that the coverage to both fault is complete. The reliability of this triple-redundant architecture is $R = 9.999996 \cdot 10^{-1}$ ($Q = 6.6121 \cdot 10^{-7}$), which is slightly worse but in the same order of magnitude that the reliability of the dual-redundant converter improved design. The triple architecture is only 50% oversized (in terms of current rating), whereas the dual architecture is 100% oversized, which might make the cost of the dual architecture higher than the cost of the triple architecture. Under these circumstances, it is possible



(a) Behavior after a fault in switch SW_1.



(b) Behavior after capacitor fault.

Fig. 4. Behavior of triple-redundant converter with 50% switch ratings.

to set up an optimization problem which would help to determine which architecture is optimal when the cost function includes reliability and cost. Furthermore, by introducing three measurement devices for current and voltage, and by using voting strategies and reconfigurable control, it is possible to detect and isolate other than omission faults.

IV. Concluding Remarks

In this paper, we proposed a methodology for integrating reliability considerations into the the design of fault-tolerant power converters. The methodology integrates techniques used in the reachability analysis of LTI systems with techniques used in system reliability analysis. One of the advantages of the methodology is that system reliability is obtained using analytically tractable models, which alleviates the computational burden of other techniques based on simulating the system behavior for each possible fault event and every possible uncontrolled input. Furthermore, by obtaining analytically tractable solutions, it is possible to get a better understanding of the influence of design parameters on the overall system reliability and performance.

In the fault-tolerant buck converter example, we showed how to improve the overall reliability of a given topology by modifying some design parameters. We also showed that there are certain trade-off between adding more redundancy for reliability purposes and the associated cost, but we showed that component rating can play an important role in these trade-off studies. In further work, we will use this methodology in the formulation of an optimization problem for fault-tolerant power converters design, that will address these trade-off issues between reliability, cost, and other metrics of interest.

References

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

[2] A. Høyland and M. Rausand, *System Reliability Theory*. New York, NY: John Wiley and Sons, 1994.

[3] V. Fazio, P. Firpo, and S. Savio, "An innovative procedure for reliability assessment of power electronic equipped s ystems: a real case study," in *Proc. IEEE International Symposium on Industrial Electronics*, December 2000, pp. 511–516.

[4] K. Macken, I. Wallace, and M. Bollen, "Reliability assessment of motor drives," in *Proc. IEEE Power Electronics Specialists Conference*, June 2006.

[5] R. Kulkarni and V. Agarwal, "Reliability analysis of a modern power supply under nuclear radiation effects," in *Proc. International Conference on Power Electronics and Drive Systems*, November 2003, pp. 71–76.

[6] A. Dominguez-Garcia, J. Kassakian, and J. Schindall, "Reliability evaluation of the power supply of an electrical power net for safety-relevant applications," *Journal of Reliability Engineering and System Safety*, vol. 91, no. 5, pp. 505–514, May 2006.

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

[8] L. Kamas and S. Sanders, "Power electronic circuit reliability analysis incorporating parallel simulations," in *Proc. IEEE Workshop on Computers in Power Electronics*, August 1996, pp. 45–51.

[9] W. Huang, D. Clafette, G. Shcuelling, M. Crowther, and J. Wallace, "System accuracy analysis of multiphase voltage regulator module," *IEEE Transactions on Power Electronics*, vol. 22, no. 3, pp. 1019–1026, May 2007.

[10] P. Krein, *Elements of Power Electronics*. New York, NY: Oxford University Press, 1997.

[11] 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.

[12] 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 2000.

[13] M. Grant and S. Boyd, *Matlab software for disciplined convex programming, http://stanford.edu/ boyd/cvx (web page and software)*, 2002.

[14] A. Kurzhanskiy and P. Varaiya, *Ellipsoidal Toolbox, http://www.eecs.berkeley.edu/ akurzhan/ellipsoids/ (web page and software)*, 2006.

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

[16] 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.

[17] A. Domínguez-García, "An integrated methodology for the performance and reliability evaluation of fault-tolerant systems," Ph.D. dissertation, Massachusetts Institute of Technology, Cambridge, MA, 2007.

[18] H. Forghani-zadeh and G. Rincon-Mora, "Current-sensing techniques for dc-dc converters," in *Proc. Midwest Symposium on Circuits and Systems*, August 2002, pp. 4–7.

[19] B. Pahami, "Voting algorithms," *IEEE Transactions on Reliability*, vol. 43, no. 4, pp. 617–629, December 1994.

[20] *Reliability Prediction of Electronic Equipment*. Department of Defense, MIL-HDBK-217F, January 1990.

[21] S. Clemente and K. Teasdale, "Understanding and using power mosfet reliability data," International Rectifier, El Segundo, CA, Tech. Rep. AN-976, 1986.