

Distributed Transient Safety Verification via Robust Control Invariant Sets: A Microgrid Application

Jean-Baptiste Bouvier^{1,2}, Sai Pushpak Nandanoori¹, Melkior Ornik² and Soumya Kundu¹

Abstract—Modern safety-critical energy infrastructures are increasingly operated in a hierarchical and modular control framework which allows for limited data exchange between the modules. In this context, it is important for each module to synthesize and communicate constraints on the values of exchanged information in order to assure system-wide safety. To ensure transient safety in inverter-based microgrids, we develop a set invariance-based distributed safety verification algorithm for each inverter module. Applying Nagumo’s invariance condition, we construct a robust polynomial optimization problem to jointly search for safety-admissible set of control set-points and design parameters, under allowable disturbances from neighbors. We use sum-of-squares (SOS) programming to solve the verification problem and we perform numerical simulations using grid-forming inverters to illustrate the algorithm.

I. INTRODUCTION

The massive failure of the Texas electrical grid in February 2021 [1] gave global coverage to the issue of power network resilience. During these extreme events, time and resources are of essence for the grid operator to assess the situation and take appropriate actions to maintain the operating state of the power network. Hence, to an extent it is imperative on the grid operator to be prepared for extreme events. Microgrids, both grid-connected and stand-alone, have shown promise to enhance resilience and reliability by paving a way of coordinating multiple distributed energy resources (DERs) as a locally operated single controllable entity [2], [3]. However, ensuring operational stability, safety, and reliability of any power network involves a complex multi-timescales problem, spanning sub-seconds to minutes and hours. Traditional power system control operations were largely structured around a temporal decoupling which allows slower-timescale operations (e.g., optimal dispatch) need not directly take into account faster-timescale constraints, and *vice versa*. However, with the emergence of inverter-based DERs and the associated changes in power systems dynamics (e.g., reducing inertia), the timescales separation is expected to continue to shrink [4]. The droop-controlled inverter based microgrids have a lower inertia than conventional generators, which allows large variations of the voltage and frequency

of each inverters [3], [5]. The fluctuations happen during the transient evolution occurring as a result of a fault or due to the transitions between the power set-points, and can lead to violation of safety constraints [6]. It is imperative to develop a mechanism to inform slower-timescale operations (e.g., optimal dispatch of power set-points) of the constraints arising from faster-timescale (transient) dynamics.

Many recent efforts have addressed this need via, for example, stability and security-constrained optimization [3], [5], [7], identification of local and distributed parametric stability conditions [6], [8], [9], etc. The distributed identification of stability conditions are particularly interesting since these fit well into a multi-ownership models of microgrid resources, and facilitate hierarchical and plug-and-play operations [10]. However, most of the related literature, as above, only focus on the stability which concerns with the convergence of power system trajectories (close) to its normal operating point after a disturbance. The concept of safety, on the other hand, relates to avoiding critical operational limits (e.g., on voltages and frequencies), even under large disturbances. Safety is closely tied to resilience, since often in cyber-physical adversarial scenarios, an immediate priority is to contain the system trajectories within some acceptable set, rather than ensuring return to normality.

Safety-constrained control techniques are gaining recent attention in the power systems community [11]–[14]. Model-predictive control [15] remains one of the most commonly used methods for enforcing dynamic constraints over some prediction horizon. However, it suffers from certain limitations in the context of power system dynamics, related to, for example, nonlinearity and associated complexity of the dynamics, information disparity due to communication overheads and/or privacy concerns, and computational burden, especially for longer prediction horizon [13]. To circumvent these issues, distributed safety verification and control methods based on robust forward set-invariance principles have been proposed in [11]–[14]. However, these prior works rely on the existence or the construction of parametric Lyapunov functions and/or barrier functions, thereby often incurring prohibitive computational costs and resulting in conservative safety certificates. The work in [11], for example, proposes a sum-of-squares (SOS) programming based computation algorithm for distributed safety certificates as a super-level set of barrier functions. However, such computational methods result in conservative estimates of the safety-guaranteed set

¹Jean-Baptiste Bouvier, Sai Pushpak Nandanoori and Soumya Kundu are with the Pacific Northwest National Laboratory, Richland, WA, USA. {saipushpak.n, soumya.kundu}@pnnl.gov

²Jean-Baptiste Bouvier and Melkior Ornik are with the Department of Aerospace Engineering and the Coordinated Science Laboratory at the University of Illinois Urbana-Champaign, Urbana, IL, USA. {bouvier3, mornik}@illinois.edu

(e.g., Fig. 1 in [11]), and typically do not scale well.

In this work, we consider a hierarchical and modular microgrid control architecture, [10], [14], [16], which allows system-level dispatch of power set-points to inverter-based resources, accommodating only limited data exchange between the (neighboring) inverter modules. Our objective is to design bounds on dispatched control set-points at the inverter buses, that guarantee, in a distributed sense, the safe excursions of local voltage and frequency within the specified limits while tolerating uncertainty in the neighboring buses. Specifically, the work presented in this paper relies on the *Nagumo's theorem* [17], [18] to build an efficient method for distributed and robust safety verification, without requiring existence or construction of barrier functions. Thus, the proposed approach requires less computation, and relaxes the conservativeness of the barrier-certified safe sets by directly accommodating the original safety specifications. The explicit reference governor [19] relies on the same concept but we focus on establishing safe bounds on control inputs, instead of deriving a specific control law, which is the role of the grid coordinator [14].

The main contributions of this article are threefold. Firstly, we determine the maximal interval (bounds) of the dispatched control set-points guaranteeing the safety of droop-controlled inverters. Secondly, we establish the monotonic relationship between this interval of safety admissible control set-points and the droop coefficients. Finally, we calculate efficiently the maximal droop coefficient for which these safety admissible controls exist. As such, this paper provides novel design guidelines for the droop control parameters, extending the literature on stability-informed droop settings, e.g., [6], [8], [9], and the references therein. We use SOS programming to solve the safety verification problems, and illustrate the algorithm via numerical simulations. The remainder of this article is structured as follows. Section II provides a background of the relevant theory. Section III presents our microgrid problem of interest. Section IV explains the theoretical approach which we illustrate on a numerical example in Section V. We conclude this article with Section VI.

II. PRELIMINARIES

A. Invariant Sets

Consider a nonlinear dynamical system of the form

$$\dot{x}(t) = f(x(t)), \quad x \in \mathbb{R}^n, \quad (1)$$

with f a Lipschitz continuous function. The objective of our work is to identify safe sets that the state x cannot leave. Such sets are called *invariant* (or *positively invariant*); we define them as in [18].

Definition 1: A set S is *invariant* by the dynamics (1) if $x(0) \in S$ yields $x(t) \in S$ for all $t \geq 0$.

To characterize invariant sets we will be using a theorem first established by Nagumo [17] and then independently rediscovered by Brezis [20]. We state here a more modern formulation of this result from [18].

Theorem 1 (Nagumo 1942): A closed set S is invariant by the dynamics (1) if and only if for all $x \in S$, $f(x) \in \mathcal{C}(x)$, with $\mathcal{C}(x)$ the Bouligand tangent cone to S at x .

A full definition of the Bouligand tangent cone is given in [18], but we will be studying sets S where the Bouligand tangent cone is \mathbb{R}^+ or \mathbb{R}^- . The geometrical interpretation of Nagumo's theorem is that f pointing inside S on its boundary prevents trajectories from leaving S .

B. Network Safety

In a network, the dynamics of node i can be modeled by

$$\dot{x}_i(t) = f_i(x_i(t), u_i(t), w_i(t)), \quad x_i \in \mathbb{R}^n, \quad u_i \in U, \quad w_i \in W, \quad (2)$$

with u_i a control input, w_i an external input, and U and W their respective admissible sets. For such a system we need to adapt our definition of invariant sets following [18].

Definition 2: A set S is *robust control invariant* by the dynamics (2) if there exists a feedback control law $u_i(t)$ such that for all $x_i(0) \in S$ and all time-varying $w_i \in W$, $x_i(t) \in S$ for all $t \geq 0$.

We then want to determine the set of control inputs u ensuring the robust control invariance of a given safe set S despite the fluctuations in the neighboring inverter states. In particular, specific to the example of inverter-based microgrids, i.e., when the safe sets are expressed as box constraints on the states (as in (6)), we define the following:

Definition 3: A 1-dimensional set $S = [\underline{s}, \bar{s}]$ is *upper invariant* (resp. *lower invariant*) for a set of controls U by the dynamics (2) if for all time-varying $w \in W$, $u \in U$ and all $x(0) \in S$, then $x(t) \leq \bar{s}$ (resp. $x(t) \geq \underline{s}$) for $t \geq 0$.

If S is upper invariant (resp. lower invariant), then the state cannot escape by crossing the upper bound (resp. lower bound) of S . Notice that if there are controls making S both upper and lower invariant, then S is a robust control invariant set. We denote such controls as *safety admissible*.

Definition 4: A set of controls U is *safety admissible* for the set S if for all controls $u \in U$, the set S is robust control invariant.

As we will detail later, if the dynamics (2) and the safe set S are polynomial, e.g., $S = \{x \in \mathbb{R}^n : p_j(x) \geq 0, j \in \{1, \dots, m\}\}$ with p_j polynomials, then the invariance condition of Nagumo's theorem can be stated as a polynomial inequality, enabling its fast computation.

III. PROBLEM DESCRIPTION

A microgrid power network is operated by a microgrid coordinator that determines power setpoints for each node of the grid [14], [16]. The transition in between these setpoints, corresponding to a transient regime, might lead the frequency or voltage of some inverters to violate safety constraints. We are thus interested in ensuring the transient safety of microgrid networks, so that they are reliable when operated. Consider the case of droop-controlled inverters [6]:

$$\dot{\theta}_i = \omega_i, \quad (3a)$$

$$\tau_i \dot{\omega}_i = -\omega_i + \lambda_i^p (P_i^{set} - P_i), \quad (3b)$$

$$\tau_i \dot{v}_i = v_i^0 - v_i + \lambda_i^q (Q_i^{set} - Q_i), \quad (3c)$$

where θ_i , ω_i and v_i are, respectively, the phase angle, frequency and voltage magnitude of node i . The droop-coefficients $\lambda_i^p > 0$ and $\lambda_i^q > 0$ are associated with the active power vs. frequency and the reactive power vs. voltage droop curves, respectively. The time-constant of the low-pass filter used for the active and reactive power measurements is τ_i . The nominal voltage magnitude is v_i^0 . The active power and reactive power set-points are P_i^{set} and Q_i^{set} , respectively. Finally, the active and reactive power injected into the network are P_i and Q_i , respectively following the nonlinear coupling equations

$$P_i = v_i \sum_{k \in \mathcal{N}_i} v_k (G_{i,k} \cos \theta_{k,i} - B_{i,k} \sin \theta_{k,i}), \quad (4a)$$

$$Q_i = -v_i \sum_{k \in \mathcal{N}_i} v_k (G_{i,k} \sin \theta_{k,i} + B_{i,k} \cos \theta_{k,i}), \quad (4b)$$

where $\theta_{k,i} = \theta_k - \theta_i$, and \mathcal{N}_i is the set of neighbor nodes with the convention that $i \in \mathcal{N}_i$. The transfer conductance and susceptance of the line connecting nodes i and k are denoted by $G_{i,k}$ and $B_{i,k}$, respectively.

We use the formulation of [11] to model the capability of the inverters to change their control set-points of the active and reactive power output in order to adjust to different operating conditions. More specifically, we write

$$P_i^{set} = P_i^0 + u_i^p, \quad \text{and} \quad Q_i^{set} = Q_i^0 + u_i^q, \quad (5)$$

where P_i^0 and Q_i^0 are the set-points for the nominal operating conditions; and u_i^p and u_i^q are control inputs. We are thus interested in maintaining at all times both voltage and frequency within some pre-specified safety limits. By a usual abuse of notation, instead of considering the actual voltage, we consider its difference from the nominal voltage $v_i^0 = 1$ p.u.. Following [11], [21], [22], we consider the voltage and frequency safe sets to be

$$S_v = [\underline{v}, \bar{v}] = [-0.4, 0.2] \text{ p.u.}, \quad (6a)$$

$$S_\omega = [\underline{\omega}, \bar{\omega}] = [-3, 3] \text{ Hz}. \quad (6b)$$

For the inverters (3), the perturbation w_i from Definition 2 are the neighbor voltage magnitudes (v_k) and phase angle differences ($\theta_{k,i}$) that determine the power transfers, P_i and Q_i . For the purpose of this paper, we assume that the phase angle differences between (any) two neighbor buses are bounded as follows:

$$\theta_{i,k} \in S_\theta = [-\pi/6, \pi/6] \quad \forall k \in \mathcal{N}_i. \quad (7)$$

Note that such range of phase angle differences are typical of distribution feeders, and especially microgrids, that are often characterized by relatively short lines connecting two buses [23]. Furthermore, note that only the difference of phase angles θ_i and θ_k as opposed to their individual values, determine the power-flow connecting the nodes i and k . Thus, for simplicity to notations and without any loss of generality, we set $\theta_i \equiv 0$ as the *reference angle*, and use $\theta_{k,i} \equiv \theta_k$ throughout this text. Then, we want to determine controls $u_i = (u_i^p, u_i^q)$ that maintain $v_i \in S_v$ and $\omega_i \in S_\omega$,

whatever the values of $\theta_k \in S_\theta$ and $v_k \in S_v$ for the neighbors $k \in \mathcal{N}_i$.

Problem 1: (Safety-Admissible Control) What values of control set-points u_i ensure that S_v and S_ω are robust control invariant by the dynamics (3)?

Moreover, note that the impact of neighbor (and network) disturbances on the inverter dynamics (3) are enhanced by larger droop values, a fact which suggests the existence and size of the *safety-admissible* controls depend on the chosen droop coefficients. This motivates the following question:

Problem 2: (Maximal Droop) What values of droop coefficients (λ_i^p, λ_i^q) ensure the existence of a non-empty safety-admissible set of controls, guaranteeing robust control invariance of S_v and S_ω as per dynamics (3)?

IV. THEORETICAL CONSTRUCTION

In this section we establish the theory concerning robust control invariant sets for droop-controlled inverters. Since $\lambda_i^p > 0$ and $\lambda_i^q > 0$ in the inverter dynamics (3), we can define a *minimal lower control* \underline{u} and a *maximal upper control* \bar{u} such that

$$\underline{u} = \inf \{ u_{low} \in \mathbb{R} : S \text{ is lower invariant for all } u \geq u_{low} \},$$

$$\bar{u} = \sup \{ u_{up} \in \mathbb{R} : S \text{ is upper invariant for all } u \leq u_{up} \}.$$

If $\underline{u} \leq \bar{u}$, then the maximal interval of safety admissible controls is $[\underline{u}, \bar{u}]$. To illustrate these definitions and our objective let us study a simplified version of (3).

A. Simple Example

Consider the frequency dynamics equation (3b) when the inverter has a single neighbor. To simplify take $\tau = 1s$, $\lambda^p = 1 \text{ rad/s/p.u.}$, $\theta_2 = 0 \text{ rad}$, $P^0 = 0 \text{ p.u.}$, $G = -2 \text{ p.u.}^{-1}$ and a safe set $S = [-1, 1] \text{ Hz}$. Then, $\dot{\omega} = -\omega + 2\omega\omega_2 + u$.

To make S upper invariant, according to Nagumo's theorem we need $\dot{\omega} \leq 0$ when $\omega = 1$. Thus, we want $2\omega_2 - 1 + u \leq 0$, so $u \leq 1 - 2\omega_2$. We are looking for robust controls u working for all possible $\omega_2 \in S$. Then, the maximal upper control is $\bar{u} = -1$, because for $\omega_2 = 1$, we need $u \leq -1$.

Similarly, to make S lower invariant, we need $\dot{\omega} \geq 0$ when $\omega = -1$. Then, we want $-2\omega_2 + 1 + u \geq 0$, i.e., $u \geq -1 + 2\omega_2$. Thus, the minimal lower control is $\underline{u} = 1$.

In this setting, $\bar{u} < \underline{u}$, there are no safety admissible controls making S robust control invariant. A reason for this failure is that λ^p is too large, making ω unstable. Indeed, for small values of λ^p , (3b) can be approximated by $\tau_i \dot{\omega}_i = -\omega_i$ which is stable. We will elaborate further on this issue in the following subsections.

B. Minimal controls for upper and lower invariance

Let us determine the minimal lower control for S_ω . By definition, $\underline{u}_i^p = \inf_{\theta_k, v_k} \{ u_i^p : \dot{\omega}_i \geq 0, \omega_i = \underline{\omega} \}$. With (3b), $\underline{u}_i^p = \inf \{ u_i^p : u_i^p \geq \frac{1}{\lambda_i^p} \underline{\omega} + P_i - P_i^0, \forall \theta_k, v_k \}$. Then, the minimal u_i^p that is larger than all $[\frac{1}{\lambda_i^p} \underline{\omega} + P_i - P_i^0](\theta_k, v_k)$ is in fact the maximum of this term over all θ_k and v_k , because

P_i is continuous in θ_k, v_k according to (4a) and, S_θ and S_v are compact. Thus,

$$\begin{aligned} \underline{u}_i^p &= \max_{\theta_k, v_k} \frac{1}{\lambda_i^p} \underline{\omega} + P_i - P_i^0, \\ \text{subject to } & \theta_k \in S_\theta, v_k \in S_v, k \in \mathcal{N}_i, \end{aligned} \quad (8)$$

Then, $\dot{\omega}_i \geq 0$ when $\omega_i = \underline{\omega}$ and $u_i^p \geq \underline{u}_i^p$ for all $\theta \in S_\theta$ and $v \in S_v$, which guarantees lower invariance according to Nagumo's theorem. Similarly, the maximal upper control is defined as

$$\begin{aligned} \overline{u}_i^p &= \min_{\theta_k, v_k} \frac{1}{\lambda_i^p} \overline{\omega} + P_i - P_i^0, \\ \text{subject to } & \theta_k \in S_\theta, v_k \in S_v, k \in \mathcal{N}_i, \end{aligned} \quad (9)$$

and makes $\dot{\omega}_i \leq 0$ when $\omega_i = \overline{\omega}$ and $u_i^p \leq \overline{u}_i^p$ for all $\theta \in S_\theta$ and $v \in S_v$. The minimal lower control \underline{u}_i^q and maximal upper control \overline{u}_i^q for the voltage equation are defined similarly.

A great way to solve the optimization problems (8) and (9) is to use a sum-of-squares (SOS) optimization. A multivariate polynomial $p(x)$, $x \in \mathbb{R}^n$, is an SOS if there exist polynomial functions $h_i(x)$, $i = 1, \dots, s$ such that $p(x) = \sum_{i=1}^s h_i^2(x)$. However, the power-flow equations (4) are not polynomials. Following [11] we choose a third order Taylor expansion of the dynamics (4) to make (3) polynomial. Then, (8) and (9) can be solved with any SOS tool.

C. Maximal droop for robust control invariance

The stability of the voltage and frequency rely on small droop coefficients λ . As in Section IV-A, when λ increases in (3), the perturbations P and Q increase, and we thus have the intuition that the set of safety admissible controls should shrink. We can actually prove a stronger result by using the fact that the optimizations in (8) and (9) only affect P_i .

Proposition 1: The bounds of the interval of safety admissible controls $[\underline{u}, \overline{u}]$ for S_v and S_ω are inversely proportional to the droop coefficient λ .

Proof: We first introduce the maximum and minimum of the active and reactive powers (4) at the lower and upper bounds of S_ω and S_v . More specifically

$$\begin{aligned} P_i^{max} &= \max \{P_i : \omega_i = \underline{\omega}, (\theta_k, v_k) \in S_\theta \times S_v, k \in \mathcal{N}_i\}, \\ P_i^{min} &= \min \{P_i : \omega_i = \overline{\omega}, (\theta_k, v_k) \in S_\theta \times S_v, k \in \mathcal{N}_i\}, \\ Q_i^{max} &= \max \{Q_i : v_i = \underline{v}, (\theta_k, v_k) \in S_\theta \times S_v, k \in \mathcal{N}_i\}, \\ Q_i^{min} &= \min \{Q_i : v_i = \overline{v}, (\theta_k, v_k) \in S_\theta \times S_v, k \in \mathcal{N}_i\}. \end{aligned}$$

Then, (8) and (9) simplify to

$$\underline{u}_i^p(\lambda_i^p) = \frac{1}{\lambda_i^p} \underline{\omega} + P_i^{max} - P_i^0, \quad \overline{u}_i^p(\lambda_i^p) = \frac{1}{\lambda_i^p} \overline{\omega} + P_i^{min} - P_i^0. \quad (10)$$

A similar result holds for the voltage. ■

Building on this result, we can then establish a sufficient condition for the existence of safety admissible controls.

Proposition 2: If the safe set contains 0 in its interior, then safety admissible controls exist for some droop coefficients.

Proof: Note that ω_i does not intervene in P_i (4a), so the constraints for P_i^{min} and P_i^{max} are the same, which leads to $P_i^{min} < P_i^{max}$. Then, based on (10), the condition $\underline{\omega} < 0 < \overline{\omega}$ is necessary and sufficient to make $\underline{u}_i^p(\lambda_i^p) < \overline{u}_i^p(\lambda_i^p)$ for λ_i^p small enough.

On the other hand, since v_i intervenes in Q_i (4b), we cannot order Q_i^{min} and Q_i^{max} without computing them. Thus the condition $\underline{v} < 0 < \overline{v}$ is sufficient but maybe not necessary to make $\underline{u}_i^q(\lambda_i^q) < \overline{u}_i^q(\lambda_i^q)$ for some λ_i^q . ■

Then, the safe sets of (6) guarantee that safety admissible controls exist for some small enough droop coefficients. We now want to find the maximal droop coefficient λ^* for which safety admissible controls exist, i.e.,

$$\lambda^* = \max \{ \lambda \geq 0 : \underline{u}(\lambda) \leq \overline{u}(\lambda) \}. \quad (11)$$

Remark 1: Note that the problem of identifying the maximal droop for stability analysis is relatively well studied in the literature (see, for instance, [6], [8], [9]). However, as a novel contribution of this paper, we propose a method to identify maximal droop values for safety verification.

According to Proposition 1 and 2, if 0 is in the interior of S and $\lambda \leq \lambda^*$, then the interval $[\underline{u}(\lambda), \overline{u}(\lambda)]$ is not empty, is proportional with $1/\lambda$ and makes S robust control invariant.

Proposition 3: The maximal droop coefficient λ^* is

$$\lambda_i^{p*} = \frac{\overline{\omega} - \underline{\omega}}{P_i^{max} - P_i^{min}} \quad \text{and} \quad \lambda_i^{q*} = \frac{\overline{v} - \underline{v}}{Q_i^{max} - Q_i^{min}}. \quad (12)$$

Proof: Since \underline{u}_i^p and \overline{u}_i^p are continuous in λ_i^p according to (10), definition (11) leads to $\underline{u}_i^p(\lambda_i^{p*}) = \overline{u}_i^p(\lambda_i^{p*})$. Using (10) we easily obtain the announced expression for λ_i^{p*} . The calculation of λ_i^{q*} is similar. ■

The term $P^{max} - P^{min}$ in the denominator validates our intuition that increasing the range of possible perturbations decreases λ^{p*} . The larger $\overline{\omega} - \underline{\omega}$ is, the larger ω can be, and thus the stronger the stabilizing term $-\omega$ is in (3b), which increases λ^{p*} . The same analysis holds for λ^{q*} .

Remark 2: There are now two approaches to answer Problem 1 based on the controls \underline{u} and \overline{u} . If $\lambda \leq \lambda^*$, then $\underline{u} \leq \overline{u}$ and any control in between guarantees the robust control invariance of the safe set. On the other hand, if $\lambda > \lambda^*$ we need a state-dependent control law. When the state gets too close from the upper (resp. lower) bound of its safe set, applying \overline{u} (resp. \underline{u}) prevents safety violation. Besides, \underline{u} and \overline{u} can be precomputed, so that the sole real-time action of the controller is to decide which one of the controls to apply.

V. NUMERICAL ANALYSIS

In this section we apply our theory to a modified microgrid model [24], and demonstrate the robust control invariance of the safe sets S_v and S_ω introduced in (6). As per the modifications in [11], [14], four inverters were placed in the network, three of those at buses 1, 4, and 5, and the fourth at bus 0 after disconnecting the utility for islanded operation.

In a microgrid, the distance between inverters is small and thus the states of neighbors are strongly coupled. To account for this physical phenomenon we introduce two constants

Δ_v and Δ_ω measuring the range of allowable uncertainty of neighboring inverters such that $v_k \in [v_i - \Delta_v, v_i + \Delta_v]$ and $\omega_k \in [\omega_i - \Delta_\omega, \omega_i + \Delta_\omega]$ for $k \in \mathcal{N}_i$. For the numerical analysis we choose $\Delta_v = 0.02$ p.u., which is 2% of the nominal voltage v_i^0 , and $\Delta_\omega = 0.12$ Hz, which is 2% of the 6Hz range of S_ω . The nominal droop coefficients of the network are $\lambda^p = 2.51$ rad/s/p.u. and $\lambda^q = 0.2$ p.u./p.u..

The coupling adds a constraint to the calculation of Q_i^{min} and Q_i^{max} . For instance, $Q_i^{max} = \max Q_i(\theta_k, v_k)$ subject to $v_i = \underline{v}$, $\theta_k \in S_\theta$, $v_k \in S_v \cap [v_i - \Delta_v, v_i + \Delta_v] = [\underline{v}, \underline{v} + \Delta_v]$ for $k \in \mathcal{N}_i$. We compute Q_2^{min} , Q_2^{max} with an SOS algorithm and we use the calculations of Proposition 1 to represent \underline{u}_2^q and \overline{u}_2^q on Figure 1.

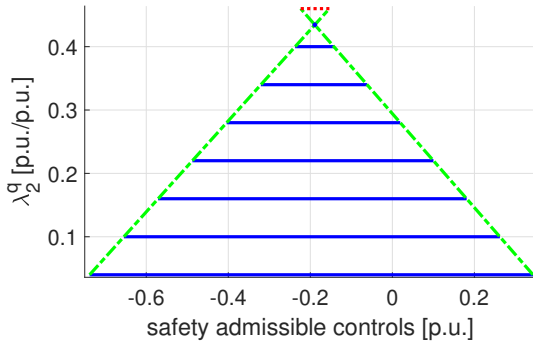


Fig. 1: Evolution of the interval of safety admissible controls in blue for the voltage of node 2. The blue dot corresponds to λ_2^{q*} . The green dash-dot lines correspond to $\underline{u}_2^q(\lambda_2^q)$ and $\overline{u}_2^q(\lambda_2^q)$. The red dotted line indicates that $\underline{u}_2^q > \overline{u}_2^q$.

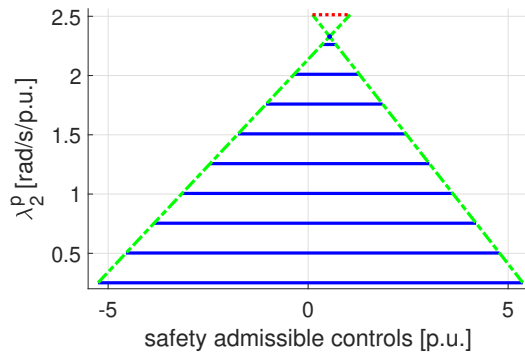


Fig. 2: Evolution of the interval of safety admissible controls in blue for the frequency of node 2. The blue dot corresponds to λ_2^{p*} . The green dash-dot lines correspond to $\underline{u}_2^p(\lambda_2^p)$ and $\overline{u}_2^p(\lambda_2^p)$. The red dotted line indicates that $\underline{u}_2^p > \overline{u}_2^p$.

As proven in Proposition 2, since 0 is in the interior of S_v , we were able to find values of λ_2^q for which safety admissible controls exist. On Figure 1, λ_2^{q*} is located at the intersection of the green dash-dot lines representing $\underline{u}_2^q(\lambda_2^q)$ and $\overline{u}_2^q(\lambda_2^q)$. Figure 2 shows that the same is true for λ_2^p . The computed values of λ^* are gathered in Table I.

Note that for the voltage λ^{q*} ranges from 80% to 217% of

Inverter	1	2	3	4
λ^{p*} [rad/s/p.u.]	1.227	2.329	0.875	1.368
λ^{q*} [p.u./p.u.]	0.228	0.434	0.161	0.241

TABLE I: Maximal droop coefficients λ^* for which safety admissible controls exist.

the nominal λ^q depending on the inverter. For the frequency, λ^{p*} ranges from 35% to 93% of the nominal λ^p .

We now study how the admissible range of states Δ_v , S_θ and S_v impact the maximal droop coefficient λ^{q*} .

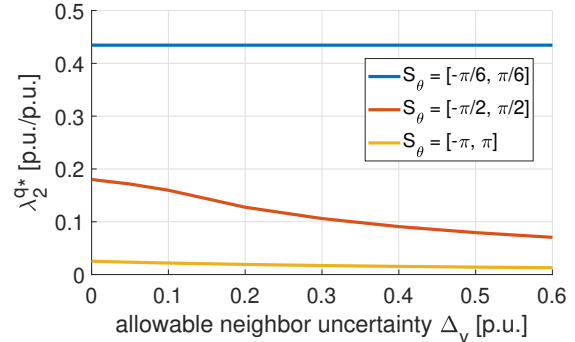


Fig. 3: Evolution of λ_2^{q*} as a function of the allowable neighbor uncertainty Δ_v and of the range of admissible phase angle S_θ .

In Figures 3 and 4, $\Delta_v = 0.6$ p.u. depicts a lack of coupling between inverters, because the length of S_v is at most 0.6 p.u., while for $\Delta_v = 0$ p.u. the coupling is perfect, i.e., $v_k = v_i$ for $k \in \mathcal{N}_i$.

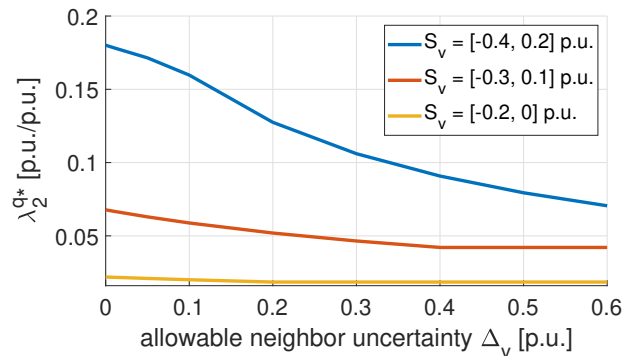


Fig. 4: Evolution of λ_2^{q*} as a function of the allowable neighbor uncertainty Δ_v and of the range of admissible voltage S_v .

As predicted with (12) and illustrated on Figures 3 and 4, as the uncertainty ranges Δ_v and S_θ increase, the value of λ^{q*} decreases. The impact of the length of S_v on λ^{q*} is more difficult to predict as it affects both the numerator and denominator of λ^{q*} in (12). However, the verdict of Figure 4 is clear: enlarging S_v increases λ^{q*} , the voltage has more wiggle room inside its safe set, it is thus easier to maintain $v \in S_v$.

We compute the controls u_1^p and $\overline{u_1^p}$ on an Intel Core i7-4770S with a CPU at 3.1GHz and 8GB of RAM. Previous works [8], [11] relied on the widely used MATLAB toolbox SOSTOOLS [25] and the semi-definite programming (SDP) solver SeDuMi [26]. However, the computation times were often excessive for nodes with more than two neighbors. We thus consider the Julia language [27], its SOS toolbox [28] and the SDP solvers SDPA [29] and Mosek [30]. As expected, Julia is faster and the computation times can be reduced by two orders of magnitude as shown on Table II.

Language	MATLAB	Julia	Julia
SDP solver	SeDuMi	SDPA	Mosek
Run-time for u_1^p and $\overline{u_1^p}$	4295s	343s	33s

TABLE II: Run-time comparison between implementations.

In order to illustrate the invariance of the safe sets with the safety admissible controls calculated, we simulate the evolution of the voltage and the frequency of node 1. We use the original non-polynomial dynamics of the system. We choose λ_1^p and λ_1^q at respectively 40% and 100% of their nominal values, so that $\lambda_1^p < \lambda_1^{p*}$ and $\lambda_1^q < \lambda_1^{q*}$. Then, the intervals of safety admissible controls are $U_\omega = [-0.724, 1.571]$ p.u. and $U_v = [-0.25, -0.0937]$ p.u.

Every second we randomly choose a control value $u_1^q \in U_v$ and $u_1^p \in U_\omega$ as shown on Figures 5(a) and 5(b). Similarly, the states $\omega_k \in S_\omega \cap [\omega_1 - \Delta_\omega, \omega_1 + \Delta_\omega]$ and $v_k \in S_v \cap [v_1 - \Delta_v, v_1 + \Delta_v]$ of the neighboring nodes are stochastically updated every 10ms as depicted on Figures 5(c) and 5(d). The evolution of the voltage and frequency of node 1 are then pictured on Figures 5(e) and 5(f).

We can see that even randomly chosen controls, as long as they are within the safety admissible interval, enforce the safety of the system as $v_1 \in S_v$ and $\omega_1 \in S_\omega$ despite the stochastic variations of the neighbor states.

One could rightfully object that the stochastic nature of the variations of the neighbor states ω_k and v_k prevent significant changes in v_1 and ω_1 that could lead to safety violations. To overcome this limitation, we run a similar simulation where the neighbor states take their worst case values. To keep a constant phase angle $\theta_k = -\frac{\pi}{6}$ rad, we need a constant frequency $\omega_k = 0$ Hz and thus the frequency coupling must be removed by taking $\Delta_\omega = \infty$. We set the voltage at its lowest admissible bound, i.e., $v_k = \max\{\underline{v}, v_i - \Delta_v\}$. We keep the same stochastic controls and same values of droop coefficients.

Figure 6(a) shows how the voltage of a neighboring inverter v_3 follows its admissible lower bound. As illustrated on Figure 6(b) and 6(c) the voltage v_1 is maintained in S_v and the frequency ω_1 is maintained in S_ω despite the stochastic safety admissible controls and the lower bound neighbor states. Similar results are obtained when choosing θ_k at its upper bound $\frac{\pi}{6}$ and/or v_k at its upper bound $\min\{\overline{v}, v_i + \Delta_v\}$.

VI. CONCLUSION AND FUTURE WORK

In this paper we considered the problem of transient safety in inverter-based microgrids. Relying on Nagumo's theorem, we developed two approaches to enforce the invariance of frequency and voltage sets of droop-controlled inverters. We solved the resulting optimization problems with SOS algorithms and successfully illustrated the safety methods on a microgrid model.

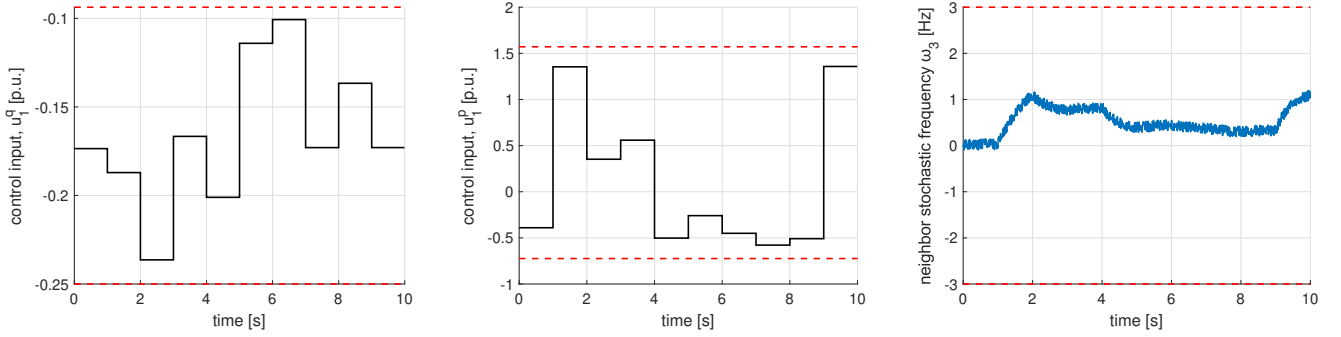
There are three promising avenues of future work. We first want to compare the efficiency of our approach in terms of size of invariant set and of computation times with barrier function and explicit governor approaches. We believe that a similar method can be used to handle safe energy storage, with only adding a state of charge constraint to the problem. Finally, we want to demonstrate our approach in conjunction with system level optimal dispatch problem.

ACKNOWLEDGMENT

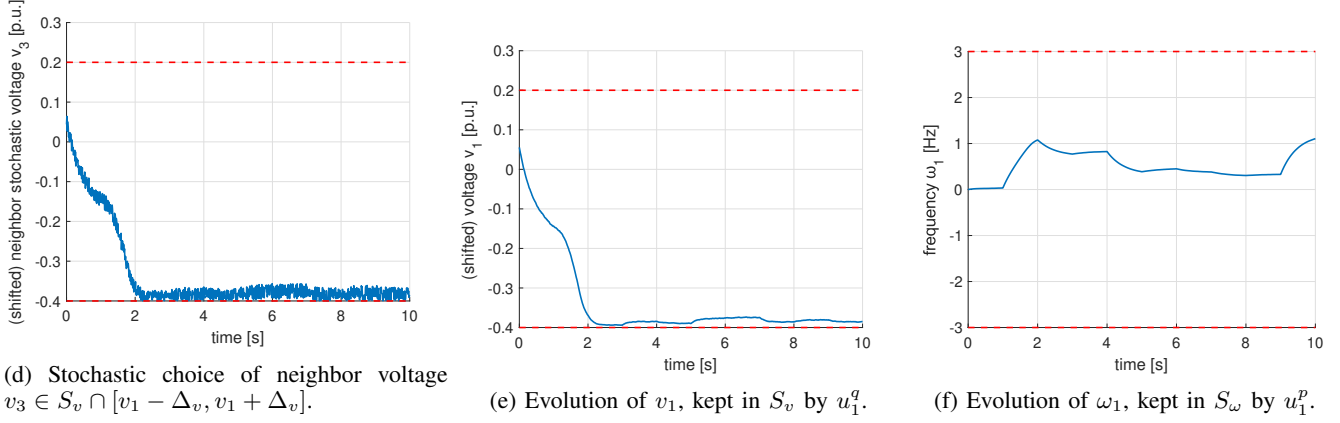
This research was supported by the Resilience through Data-driven Intelligently-Designed Control (RD2C) Initiative, under the Laboratory Directed Research and Development (LDRD) Program at Pacific Northwest National Laboratory (PNNL). PNNL is a multi-program national laboratory operated for the U.S. Department of Energy (DOE) by Battelle Memorial Institute under Contract No. DE-AC05-76RL01830.

REFERENCES

- [1] J. W. Busby, K. Baker, M. D. Bazilian, A. Q. Gilbert, E. Grubert, V. Rai, J. D. Rhodes, S. Shidore, C. A. Smith, and M. E. Webber, "Cascading risks: Understanding the 2021 winter blackout in Texas," *Energy Research & Social Science*, vol. 77, pp. 1 – 10, 2021.
- [2] M. Farrokhabadi, C. A. Cañizares, J. W. Simpson-Porco, E. Nasr, L. Fan, P. A. Mendoza-Araya, R. Tonkoski, U. Tamrakar, N. Hatziaargyriou, D. Lagos *et al.*, "Microgrid stability definitions, analysis, and examples," *IEEE Transactions on Power Systems*, vol. 35, no. 1, pp. 13–29, 2019.
- [3] Y. Xu, C.-C. Liu, K. P. Schneider, F. K. Tuffner, and D. T. Ton, "Microgrids for service restoration to critical load in a resilient distribution system," *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 426 – 437, 2016.
- [4] J. A. Taylor, S. V. Dhople, and D. S. Callaway, "Power systems without fuel," *Renewable and Sustainable Energy Reviews*, vol. 57, pp. 1322 – 1336, 2016.
- [5] A. Maulik and D. Das, "Stability constrained economic operation of islanded droop-controlled DC microgrids," *IEEE Transactions on Sustainable Energy*, vol. 10, no. 2, pp. 569 – 578, 2018.
- [6] J. Schiffer, R. Ortega, A. Astolfi, J. Raisch, and T. Sezi, "Conditions for stability of droop-controlled inverter-based microgrids," *Automatica*, vol. 50, no. 10, pp. 2457 – 2469, 2014.
- [7] E. Barklund, N. Pogaku, M. Prodanovic, C. Hernandez-Aramburo, and T. C. Green, "Energy management in autonomous microgrid using stability-constrained droop control of inverters," *IEEE Transactions on Power Electronics*, vol. 23, no. 5, pp. 2346 – 2352, 2008.
- [8] S. Kundu, W. Du, S. P. Nandanoori, F. Tuffner, and K. Schneider, "Identifying parameter space for robust stability in nonlinear networks: A microgrid application," in *American Control Conference*. IEEE, 2019, pp. 3111 – 3116.
- [9] S. P. Nandanoori, S. Kundu, W. Du, F. K. Tuffner, and K. P. Schneider, "Distributed small-signal stability conditions for inverter-based unbalanced microgrids," *IEEE Transactions on Power Systems*, vol. 35, no. 5, pp. 3981 – 3990, 2020.
- [10] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. De Vicuña, and M. Castilla, "Hierarchical control of droop-controlled ac and dc microgrids—a general approach toward standardization," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 1, pp. 158–172, 2010.

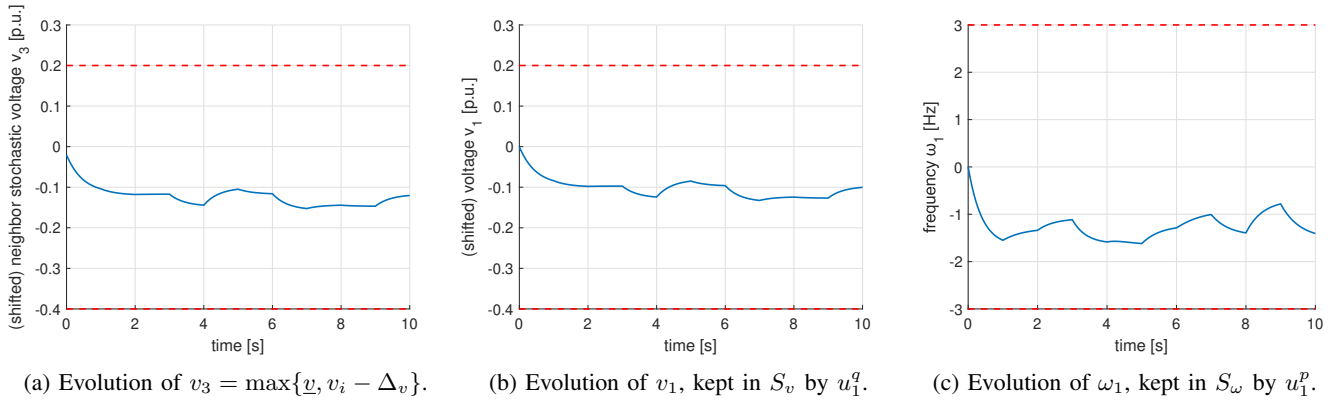


(a) Stochastic choice of $u_1^q \in U_v$, where U_v is the interval of safety admissible controls. (b) Stochastic choice of $u_1^p \in U_\omega$, where U_ω is the interval of safety admissible controls. (c) Stochastic choice of neighbor frequency $\omega_3 \in S_\omega \cap [\omega_1 - \Delta_\omega, \omega_1 + \Delta_\omega]$.



(d) Stochastic choice of neighbor voltage $v_3 \in S_v \cap [v_1 - \Delta_v, v_1 + \Delta_v]$. (e) Evolution of v_1 , kept in S_v by u_1^q . (f) Evolution of ω_1 , kept in S_ω by u_1^p .

Fig. 5: Simulation of the voltage v_1 and frequency ω_1 under stochastic safety admissible controls u_1^q and u_1^p , and stochastic variations of neighbor states θ_2 , θ_3 , v_2 and v_3 .



(a) Evolution of $v_3 = \max\{\underline{v}, v_i - \Delta_v\}$. (b) Evolution of v_1 , kept in S_v by u_1^q . (c) Evolution of ω_1 , kept in S_ω by u_1^p .

Fig. 6: Simulation of the voltage v_1 and frequency ω_1 under stochastic safety admissible controls u_1^q and u_1^p , and lower bound choice of neighbor states θ_2 , θ_3 , v_2 and v_3 .

[11] S. Kundu, S. Geng, S. P. Nandanoori, I. A. Hiskens, and K. Kalsi, "Distributed barrier certificates for safe operation of inverter-based microgrids," in *American Control Conference*. IEEE, 2019, pp. 1042–1047.

[12] Y. Chen, J. Anderson, K. Kalsi, S. H. Low, and A. D. Ames, "Compositional set invariance in network systems with assume-guarantee contracts," in *American Control Conference*. IEEE, 2019, pp. 1027–1034.

[13] Y. Zhang and J. Cortés, "Distributed bilayered control for transient frequency safety and system stability in power grids," *IEEE Transactions on Control of Network Systems*, vol. 7, no. 3, pp. 1476–1488, 2020.

[14] S. Kundu and K. Kalsi, "Transient safety filter design for grid-forming inverters," in *American Control Conference*. IEEE, 2020, pp. 1299–1304.

[15] D. Q. Mayne, J. B. Rawlings, C. V. Rao, and P. O. Scokaert, "Constrained model predictive control: Stability and optimality," *Automatica*, vol. 36, no. 6, pp. 789–814, 2000.

[16] M. Almassalkhi, S. Brahma, N. Nazir, H. Ossareh, P. Racherla, S. Kundu, S. P. Nandanoori, T. Ramachandran, A. Singhal, D. Gayme *et al.*, "Hierarchical, grid-aware, and economically optimal coordination of distributed energy resources in realistic distribution systems," *Energies*, vol. 13, no. 23, p. 6399, 2020.

[17] M. Nagumo, "Über die lage der integralkurven gewöhnlicher differ-

- entialgleichungen,” *Proceedings of the Physico-Mathematical Society of Japan. 3rd Series*, vol. 24, pp. 551 – 559, 1942.
- [18] F. Blanchini, “Set invariance in control,” *Automatica*, vol. 35, no. 11, pp. 1747 – 1767, 1999.
- [19] M. M. Nicotra and E. Garone, “The explicit reference governor: A general framework for the closed-form control of constrained nonlinear systems,” *IEEE Control Systems Magazine*, vol. 38, no. 4, pp. 89–107, 2018.
- [20] H. Brezis, “On a characterization of flow-invariant sets,” *Communications on Pure and Applied Mathematics*, vol. 23, no. 2, pp. 261 – 263, 1970.
- [21] K. P. Schneider, N. Radhakrishnan, Y. Tang, F. K. Tuffner, C.-C. Liu, J. Xie, and D. Ton, “Improving primary frequency response to support networked microgrid operations,” *IEEE Transactions on Power Systems*, vol. 34, no. 1, pp. 659 – 667, 2018.
- [22] J. Elizondo, R. Y. Zhang, P.-H. Huang, J. K. White, and J. L. Kirtley, “Inertial and frequency response of microgrids with induction motors,” in *17th Workshop on Control and Modeling for Power Electronics*. IEEE, 2016, pp. 1 – 6.
- [23] W. H. Kersting, “Radial distribution test feeders,” *IEEE Transactions on Power Systems*, vol. 6, no. 3, pp. 975–985, 1991.
- [24] T. Ersal, C. Ahn, I. A. Hiskens, H. Peng, and J. L. Stein, “Impact of controlled plug-in evs on microgrids: A military microgrid example,” in *Power and Energy Society General Meeting*. IEEE, 2011, pp. 1–7.
- [25] A. Papachristodoulou, J. Anderson, G. Valmorbida, S. Prajna, P. Seiler, and P. A. Parrilo, *SOSTOOLS: Sum of squares optimization toolbox for MATLAB*, 2013, available from <http://www.cds.caltech.edu/sostools>.
- [26] J. F. Sturm, “Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones,” *Optimization Methods and Software*, vol. 11, pp. 625 – 653, 1999, software available at <http://fewcal.kub.nl/sturm/software/sedumi.html>.
- [27] J. Bezanson, S. Karpinski, V. B. Shah, and A. Edelman, “Julia: A fast dynamic language for technical computing,” *arXiv preprint arXiv:1209.5145*, 2012.
- [28] B. Legat, C. Coey, R. Deits, J. Huchette, and A. Perry, “Sum-of-squares optimization in Julia,” in *First Annual JuMP-dev Workshop*, 2017.
- [29] M. Yamashita, K. Fujisawa, M. Fukuda, K. Kobayashi, K. Nakata, and M. Nakata, “Latest developments in the SDPA family for solving large-scale SDPs,” in *Handbook on semidefinite, conic and polynomial optimization*. Springer, 2012, pp. 687 – 713.
- [30] J. Dahl, “Semidefinite optimization using MOSEK,” in *International Symposium on Mathematical Programming*, 2012.