IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 16 September 2026, accepted 26 October 2026. Date of publication 00 xxxx 0000, date of current version 00 xxxx 0000.

Digital Object Identifier 10.1109/ACCESS.2026.3748385

Robust Simulation Functions for Interconnected Systems Under Large Disturbances

BEN WOODING[1], (Member, IEEE), AND SADEGH SOUDJANI[2,3], (Member, IEEE)
[1]Institute for Convergent Software Integrated Systems, Vanderbilt University, Nashville, TN 37212, USA
[2]School of Computer Science, University of Birmingham, B15 2TT Birmingham, U.K.
[3]Max Planck Institute for Software Systems, 67663 Kaiserslautern, Germany

Corresponding author: Ben Wooding (ben.wooding@vanderbilt.edu)

The work of Ben Wooding was supported in part by the Engineering and Physical Sciences Research Council (EPSRC) Studentship under Grant EP/R51309X/1 and in part by the Doctoral Prize Fellowship. The work of Sadegh Soudjani was supported in part by the Horizon Europe European Innovation Council (EIC) Project SymAware under Grant 101070802 and in part the European Research Council (ERC) Project Auto-CyPheR under Grant 101089047.

ABSTRACT This work is concerned with an assume-guarantee approach to compositionally control interconnected systems under large disturbances. The proposed scheme is based on the new notion of *robust simulation functions (RSF) with disturbance refinement* alongside the composition of multiple subsystems to tackle the difficulties associated with scalability of formal control methods, also known as the curse of dimensionality, and with their conservatism under large disturbances. We approximate concrete subsystems with abstractions that have lower dimensions (*a.k.a.* reduced-order models) while providing mathematical guarantees on controller synthesis through the quantification of an upper bound on the closeness between output trajectories of the original system and their abstraction. We employ assume-guarantee contracts to design decentralized controllers for distinct subsystems, composing the per-subsystem invariance guarantees into a global *safety* guarantee over the interconnected network; reachability is established per subsystem. We extend the notion of RSF with disturbance refinement to a class of nonlinear systems with bounded slope (covering, e.g., saturation, sine and cosine functions that arise in power-system models), outline how RSFs can be computed beyond this class for polynomial and general nonlinear systems via sum-of-squares and scenario-based programs, and consider a challenging case study of frequency regulation using a model of the New England 39-Bus Test System (NETS) under large power losses. The disturbance interface tightens the simulation-relation error by 9.4% over the closest existing construction, and the compositional pipeline reduces the abstract state count from 10^{57} to 10^{6}.

INDEX TERMS Simulation relations, formal control synthesis, assume-guarantee contract, power networks.

I. INTRODUCTION

Cyber-physical systems (CPS) combine both cyber and physical components in interconnected models with interactions through feedback loops [1]. They are an important modeling framework for engineering real-life systems such as autonomous vehicles, medical devices and power systems, to name a few. The interconnection of these components in the models often results in high-dimensional systems with complex behavior specifications that are generally safety critical in nature. Providing guarantees on the behavior of these systems is therefore essential but also challenging. To tackle this difficulty, formal methods have been introduced in the relevant literature as a strong mathematical framework to provide guarantees on either verification or controller synthesis of CPS [2], [3].

Power-system operation is a demanding application of CPS that has received considerable attention in the past decade. In particular, as the contribution of renewable energy rises, generation is becoming increasingly variable and intermittent. To ensure stability and functionality of power networks, demand-side control techniques are required [4]. In this respect, smart grid control involves the demand-side of a power grid responding to events in order to reduce the strain on the network, while also optimizing consumer satisfaction and other specialist requirements [5]. Smart grids contain

The associate editor coordinating the review of this manuscript and approving it for publication was Yangmin Li.

© 2026 The Authors. This work is licensed under a Creative Commons Attribution 4.0 License.
For more information, see https://creativecommons.org/licenses/by/4.0/

sensors and information-based technical devices, so it is assumed that the current frequency, power generation or load values applied in different locations of the system can be accurately measured.

There are numerous established control techniques within the power system literature, *e.g.,* loop shaping [6], linear quadratic regulators (LQR) [7], model predictive control (MPC) [8], Lyapunov stability [9], robust control [10]. These methods provide powerful analytical and numerical guarantees — on stability, robustness, and constraint satisfaction — but they do not by themselves establish satisfaction of the discrete temporal-logic specifications considered here over all admissible behaviors, and their validation typically relies on numerical simulations and experiments that may leave a safety-critical scenario untested [11]. In comparison, formal approaches consider a specification that is written using temporal logic [12], and mathematically check whether that specification holds for the system under the designed controller. It is worth noting that formal verification checks mathematically whether the system satisfies a desired specification, while formal control synthesis, which we consider in this work, goes a step further to design a controller that guarantees the specification will hold on the behavior of the system under the designed controller.

Symbolic control is one of the promising techniques for formal control synthesis of CPS [13]. In particular, symbolic models (*a.k.a.* finite abstractions) replace concrete systems to provide an easier medium for synthesis of a formal controller. In abstraction-based techniques, each discrete state and input in the finite abstraction maps to an aggregate collection of continuous states in the original (concrete) model. By establishing a similarity relation between original systems and their symbolic models, one can consider the abstract system as an appropriate substitute in the controller design process with lower computational complexity while still preserving closeness guarantees between the two systems. Simulation and bisimulation functions are powerful techniques to relate output trajectories of abstract systems to those of concrete ones [12], [13]. If a concrete system is (bi)similar to an abstract system, only the abstract system needs to be considered in the formal synthesis process, while guarantees are still provided. For control systems where output trajectories of two systems may not be identical, *approximate* (bi)simulation functions [14] have been developed in which output trajectories of two systems are only required to remain measurably close. In this case, the closeness between output trajectories can be bounded by some maximal ϵ, known as the *simulation relation error*. Given an ϵ-closeness, interface functions can be used to map the synthesized controller from the abstract system back to the concrete one. In [15], this type of relation is extended to *robust* simulation functions (RSF) with small disturbances inside the concrete system, but with an unperturbed abstract system. The works [16], [17] both consider model reduction for power systems, but based on heuristic methods rather than formal approaches.

Abstraction-based techniques often suffer severely from the curse of dimensionality while dealing with high-dimensional systems [18]. To alleviate this computational complexity, one potential approach is to use compositional techniques: decompose a system into multiple subsystems and provide analysis over the high-dimensional system via its smaller subsystems [19]. Assume-guarantee contracts have been explored extensively in the literature to provide control techniques over a network of continuous-time dynamical systems [20], [21], [22], [23]. Compositional approaches have also been used for the construction of (in)finite abstractions for interconnected systems based on abstractions of smaller subsystems [24], [25], [26], [27].

Formal methods play a significant role in power systems to provide formal analysis over this type of demanding systems. In this regard, the work [28] proposes approximate bisimulations in transient power systems and employs differential-algebraic equations (DAEs) to model the New England 39-Bus Test System. In [29], DAEs are utilized as models of the IEEE 14-Bus System and the IEEE 30-Bus System to provide reachability analysis for transient stability without performing any controller synthesis. The work [30] studies formal analysis of power systems via reachable sets of microgrids with distributed energy resources. The results of [31] use contract-based symbolic controller design for voltage stability in DC microgrids. More recently, formal guarantees for power systems with neural networks have been verified in [32]. Formal verification for smart cities is discussed in [33], and Petri nets for smart grid verification are used in [34]. The logical correctness of the modeling topology of a power grid cyber-physical system is formally guaranteed in [35]. Verification of power systems described using graph neural networks are considered in [36] and [37]. Other recent works include formal approaches for reliability analysis [38], [39]. We note here that the majority of these works consider formal verification problems rather than formal design of controllers as in our paper.

Original Contributions. In this work, we design formal controllers for interconnected systems under large measurable disturbances, and we validate the approach on a model of the New England 39-Bus Test System (NETS). The contributions of this work are:

- We equip the notion of robust simulation functions (RSFs) with a disturbance-refinement interface and combine it with assume-guarantee contracts to design formal controllers for interconnected systems under large measurable disturbances, with a global safety guarantee and per-subsystem reachability guarantees.
- We formalize the decentralized design through invariance assume-guarantee contracts and give a composition theorem (Theorem 3), instantiating the framework of [21], that lifts per-subsystem safety guarantees to a global guarantee over the interconnected network.
- We generalize the definition of RSF with disturbance refinement from linear systems to a class

of nonlinear systems with bounded slope, enabling higher-dimensional systems to be controlled by lower-dimensional controllers. The construction reduces to a pair of vertex linear matrix inequalities (LMIs) that can be checked with standard semidefinite programming solvers. Beyond this class, we sketch RSF constructions for polynomial and general nonlinear systems via sum-of-squares and scenario-based programs (Section III-E); these are presented as outlooks rather than formally proven results.

- We show that the compositional pipeline reduces the abstract state space of the symbolic controller from $\mathcal{O}(\boldsymbol{n}^{n_1})$ to $\mathcal{O}(N\,\boldsymbol{n}^{\bar{n}_2})$, where $\boldsymbol{n}$ is the number of partitions per dimension, n_1 the dimension of the original interconnected system, N the number of subsystems, and $\bar{n}_2 := \max_i n_2^i$ the largest reduced subsystem dimension. The synthesis cost thus becomes exponential only in the reduced per-subsystem dimension and linear in the number of subsystems.
- We demonstrate feasibility and quantify the reduction achieved by our results on a model of NETS under a large power loss, as a closely coupled system composed of three 9-dimensional subsystems (27 dimensions in total).

We demonstrate our results for primary frequency control using two scenarios: (i) leveraging the principle of interconnected synchronous machines to control subsystems independently, and (ii) considering power flows between neighboring areas as internal disturbances to relax the assumption that the machines maintain synchronism. We present the developed theory first and bring it together in a single detailed case study at the end of the paper. Throughout, we use *area* and *subsystem* interchangeably.

Relation to prior work. A preliminary version of this work appeared as the technical report [40], and an initial subset of the underlying simulation-function machinery was published as a conference paper [41]. The present manuscript extends the preliminary version in three directions: (i) we generalize the framework from linear systems to a class of nonlinear systems with bounded slope through a vertex-LMI construction (Lemma 1 and Theorem 1); (ii) we give complete proofs of the simulation-relation results (Theorems 1–2) that were previously omitted or only sketched; and (iii) we make the assume-guarantee treatment rigorous through an invariance-contract composition theorem (Theorem 3).

Concretely: [14] assumes an undisturbed concrete system; [15] disturbs the concrete system but leaves the abstraction unperturbed, so $\mathbf{d}_1$ enters ϵ at full magnitude. Our disturbance interface $d_{\mathcal{V}}$ gives the abstraction its own disturbance channel, leaving only the residual $D_1 - PD_2R_1$ in the gain γ_1. Neither work treats interconnections or a state-dependent nonlinearity in the abstraction; we add both. Unlike compositional abstraction [24], [26], we also reduce each subsystem's *order* before abstracting it, which is what yields the state-count reduction.

This yields a large reduction in problem size: a monolithic abstraction of the full 27-dimensional NETS is well beyond reach, whereas the compositional pipeline built on three 3-dimensional reduced-order abstractions requires only about 8.2×10^6 abstract states.

Organization. Section II provides the preliminaries, the class of systems, the linear temporal logic specifications, and the problem formulation. Section III generalizes RSF with disturbance refinement to a class of nonlinear systems with bounded slope. Section IV presents the interconnection of subsystems and the assume-guarantee contracts used to obtain global guarantees. Section V draws these results together in a detailed case study on NETS, covering the proof of concept, the isolated-area controllers, and the compositional design with internal disturbances. Section VI provides concluding remarks and future directions.

II. NOTATIONS AND PRELIMINARIES

We employ the following notation throughout the paper. We denote the set of natural numbers, real, and non-negative real numbers by $\mathbb{N}$, $\mathbb{R}$ and $\mathbb{R}^+$, respectively. The empty set is denoted by $\emptyset$. A function $\gamma : \mathbb{R}^+ \to \mathbb{R}^+$ is a *class-$\mathcal{K}$* function if γ is continuous, strictly increasing and $\gamma(0) = 0$. We write $|\cdot|$ for the absolute value of a scalar and $\|a\|$ for the Euclidean norm of a vector a. For a matrix A, $\|A\|$ denotes the induced Euclidean (spectral) norm and $\|A\|_F$ the Frobenius norm. For a signal $s\colon \mathbb{R}^+ \to \mathbb{R}^n$ we write $\|s\|_\infty := \operatorname{ess\,sup}_{t\geq 0}\|s(t)\|$ for its essential supremum norm; this is the norm used in Theorem 2. $\mathbb{I}^n$ denotes the $n \times n$ identity matrix. For a square matrix A we write $A \succ 0$ ($A \succeq 0$) to mean A is positive (semi-)definite. Throughout, the safe set is the closed interval $\mathcal{B} = [\underline{\mathcal{B}}, \overline{\mathcal{B}}] \subset \mathbb{R}$ and the target set is $\mathcal{T} = [\underline{\mathcal{T}}, \overline{\mathcal{T}}] \subset \mathbb{R}$. All derivatives are taken with respect to time, and we often omit time for simplicity (*e.g.,* write $\mathbf{x}$ instead of $\mathbf{x}(t)$). Given functions $g^i\colon X^i \to Y^i$, $i \in \{1, \ldots, N\}$, their Cartesian product $\Pi_{i=1}^N g^i\colon \Pi_{i=1}^N X^i \to \Pi_{i=1}^N Y^i$ is defined as $(\Pi_{i=1}^N g^i)(x^1, \ldots, x^N) = [g^1(x^1); \ldots; g^N(x^N)]$. We represent systems by Σ, with superscripts labeling subsystems (Σ^i) and subscripts distinguishing concrete and abstract models: Σ_1 is the original system and Σ_2 its reduced-order abstraction.

Definition 1 (Subsystems): Consider a network of N subsystems. Each subsystem $i \in \{1, \ldots, N\}$ at level $z \in \{1, 2\}$ (concrete vs. abstract) is the tuple $\Sigma_z^i = (X_z^i, U_z^i, V_z^i, W_z^i, g_z^i, Y_z^{i,\mathrm{ext}}, Y_z^{i,\mathrm{int}}, h_z^{i,\mathrm{ext}}, h_z^{i,\mathrm{int}})$, where:

- $X_z^i \subseteq \mathbb{R}^{n_z^i}$ is the state set;
- $U_z^i \subseteq \mathbb{R}^{p_z^i}$ is the control input set;
- $V_z^i \subseteq \mathbb{R}^{q_z^i}$ is the external disturbance set;
- $W_z^i \subseteq \mathbb{R}^{r_z^i}$ is the internal disturbance set;
- $g_z^i\colon X_z^i \times U_z^i \times V_z^i \times W_z^i \to X_z^i$ is the transition map;
- $Y_z^{i,\mathrm{ext}} \subseteq \mathbb{R}^{m^{i,\mathrm{ext}}}$ and $Y_z^{i,\mathrm{int}} \subseteq \mathbb{R}^{m^{i,\mathrm{int}}}$ are the external and internal output sets, with possibly distinct dimensions;
- $h_z^{i,\mathrm{ext}}\colon X_z^i \to Y_z^{i,\mathrm{ext}}$ and $h_z^{i,\mathrm{int}}\colon X_z^i \to Y_z^{i,\mathrm{int}}$ are the external and internal output maps.

The evolution of each subsystem is governed by

$$\Sigma_z^i: \begin{cases} \dot{\mathbf{x}}_z^i = g_z^i(\mathbf{x}_z^i, \mathbf{u}_z^i, \mathbf{v}_z^i, \mathbf{w}_z^i), \\ \mathbf{y}_z^{i,\text{ext}} = h_z^{i,\text{ext}}(\mathbf{x}_z^i), \\ \mathbf{y}_z^{i,\text{int}} = h_z^{i,\text{int}}(\mathbf{x}_z^i), \end{cases} \tag{1}$$

where $\mathbf{v}_z^i \colon \mathbb{R}^+ \to V_z^i$ is measurable and may take arbitrarily large values within the known bounded set V_z^i.

Without loss of generality, we consider Σ_1^i as our original (concrete) subsystem and Σ_2^i as its (possibly) lower-dimensional abstraction (with $n_2^i \leq n_1^i$). In the following, we present the definition of interconnected systems in which subsystems Σ_z^i are connected with each other via internal disturbances $\mathbf{w}_z^i$.

Definition 2 (Interconnected Systems): Consider a network of N subsystems Σ_z^i as in Definition 1, with a coupling matrix $\mathcal{M}$ mapping the stacked internal outputs to the stacked internal disturbances (which requires $r_1^i = r_2^i$ for all i). The interconnection $\mathcal{I}(\Sigma_z^1, \ldots, \Sigma_z^N)$ is the system $\Sigma_z = (X_z, U_z, V_z, g_z, Y_z, h_z)$ with $X_z := \Pi_{i=1}^N X_z^i$, $U_z := \Pi_{i=1}^N U_z^i$, $V_z := \Pi_{i=1}^N V_z^i$, $g_z := \Pi_{i=1}^N g_z^i$, $Y_z := \Pi_{i=1}^N Y_z^{i,\text{ext}}$, and $h_z := \Pi_{i=1}^N h_z^{i,\text{ext}}$, with internal disturbances constrained by

$$[\mathbf{w}_z^1; \ldots; \mathbf{w}_z^N] = \mathcal{M}\,[\mathbf{y}_z^{1,\text{int}}; \ldots; \mathbf{y}_z^{N,\text{int}}].$$

The evolution of the interconnected system is therefore characterized by

$$\Sigma_z: \begin{cases} \dot{\mathbf{x}}_z = g_z(\mathbf{x}_z, \mathbf{u}_z, \mathbf{v}_z), \\ \mathbf{y}_z = h_z(\mathbf{x}_z) \end{cases} \qquad z \in \{1, 2\},$$

where, with a slight abuse of notation, g_z denotes the map obtained by substituting the interconnection constraint $[\mathbf{w}_z^1; \ldots; \mathbf{w}_z^N] = \mathcal{M}\,[\mathbf{y}_z^{1,\text{int}}; \ldots; \mathbf{y}_z^{N,\text{int}}]$ into $\Pi_{i=1}^N g_z^i$. As part of our control approach we use abstraction-based techniques, replacing a continuous-time, infinite-space dynamical system by a discrete-time, finite-space one. We elaborate on this quantization approach here, which has become standard in the hybrid systems literature.

Fix a sampling period $\tau > 0$ and let the controller be implemented so that the input is held constant on each interval $[k\tau, (k+1)\tau)$. Sampling the continuous-time subsystem at these instants yields the discrete-time transition map g_{cl}^i used in (13), whose state is $\mathbf{x}^i(k) := \mathbf{x}^i(k\tau)$. A finite abstraction is then obtained by partitioning the state and input sets into cells: abstract states represent cells of the continuous state space, and abstract inputs represent selected (quantized) concrete inputs. The construction is *sound* in the usual sense that every behavior of the sampled concrete system is matched, up to a state-space quantization parameter $\varepsilon_{\text{grid}}$, by a behavior of the finite abstraction; we use the compositional construction of [42], and refer the reader there for the details and for the choice of τ and grid size that make the relation hold.

Two consequences matter; (i) labels must be robust to the quantization: an atomic proposition is assigned to an abstract state only if it holds on the whole corresponding cell, which is why we will tighten the specifications (cf. (17)). The tightening margin used in synthesis must cover the total error $\epsilon_{\text{total}} = \epsilon + \varepsilon_{\text{grid}}$, combining the RSF bound ϵ of Theorem 2 with the discretization and quantization error; in the case study ϵ dominates and is the quantity we report; (ii) the guarantees obtained by symbolic synthesis, and the composition result of Theorem 3, are statements about the sampled trajectory $\{\mathbf{x}^i(k)\}_{k\in\mathbb{N}}$. Extending them to the inter-sample behavior requires in addition a bound on the reachable set over one sampling interval, which is standard for the Lipschitz dynamics considered here and is likewise absorbed into the over-approximation; we do not repeat that argument, and we state our results at the sampling instants. With a discrete-time abstraction in hand, we can use formal methods to describe the desired behaviors as discrete-time temporal-logic specifications.

Linear Temporal Logic Specifications. For dynamical systems in (1), we consider linear temporal logic (LTL) specifications with syntax [12]

$$\psi := p \mid \neg\psi \mid \psi_1 \wedge \psi_2 \mid \bigcirc\psi \mid \psi_1 \,\mathsf{U}\, \psi_2,$$

where p is an atomic proposition. Let σ be an infinite word, that is, a string composed of letters from the power set of atomic propositions, and σ_k be a subsequence (suffix) of σ. Then the satisfaction relation between σ and a property ψ, expressed as LTL, is denoted by $\sigma \vDash \psi$. Furthermore, $\sigma_k \vDash \neg\psi$ if $\sigma_k \nvDash \psi$ and we say that $\sigma_k \vDash \psi_1 \wedge \psi_2$ if $\sigma_k \vDash \psi_1$ and $\sigma_k \vDash \psi_2$. The next operator $\sigma_k \vDash \bigcirc\psi$ holds if the property holds at the next time instance. The temporal until operator $\sigma_k \vDash \psi_1 \,\mathsf{U}\, \psi_2$ holds if $\exists i \in \mathbb{N} : \sigma_{k+i} \vDash \psi_2$, and $\forall j \in \mathbb{N} : 0 \leq j < i, \sigma_{k+j} \vDash \psi_1$. Disjunction ($\vee$) can be defined by $\psi_1 \vee \psi_2 = \neg(\neg\psi_1 \wedge \neg\psi_2)$, and true $= \neg(\psi \wedge \neg\psi)$. The operator $\sigma_k \vDash \Diamond\psi$ is used to denote that the property will eventually happen at some point in the future. The operator $\sigma_k \vDash \Box\psi$ signifies that ψ must always be true at all times in the future. Additionally, we use a superscript over an operator to indicate the time horizon over a specification, *e.g.,* $\sigma_k \vDash \Diamond^{30}\psi$ would signify the property will eventually hold before 30 units of time.

These temporal logic descriptions are used to describe the desired behavior of a system. A labeling function will give every state in the system some label that is descriptive of that state, *e.g.,* common labels are ''safe states'', ''unsafe states'', ''target states'', etc. A large transition model for the system can then be defined which highlights transitions between states. Using the labels, transitions can then be either prioritized or avoided, such as never choosing transitions that go to a state labeled an ''unsafe state''. Therefore, using the logical properties described, complex specifications of how systems should behave can be defined and checked against. While formal verification approaches use model checking to determine if these specifications are satisfied, formal synthesis designs controllers in order to fulfill these specifications.

We now present the main problem that we aim to solve in this work.

Problem 1: Given a high-dimensional interconnected system $\Sigma_1 = \mathcal{I}(\Sigma_1^1, \ldots, \Sigma_1^N)$ composed of possibly nonlinear subsystems, under large measurable disturbances, and an LTL specification $\psi = \bigwedge_{i=1}^{N} \psi^i$, design decentralized formal controllers such that ψ is satisfied over the original interconnected system for every admissible disturbance.

Due to the high dimensionality of Σ_1, we address Problem 1 compositionally: we construct a reduced-dimension abstraction of each subsystem together with an RSF, design a formal controller on each abstraction, and refine it back to the concrete subsystem, so that the local guarantees combine to yield the satisfaction of ψ over the interconnected system. We assume throughout that: (D1) each $\mathbf{v}_z^i$ is measurable with a *known* bound, $\|\mathbf{d}_1\|_\infty \leq d_{\max}$ — no smallness, smoothness or stochastic model is assumed; (D2) the realized $\mathbf{d}_1(t)$ is available online to $d_\mathcal{V}$, without which the interface cancels nothing and the construction degenerates to [15]; and (D3) $\mathbf{w}^i$ is generated by neighbors through $\mathcal{M}$ and confined to the contract set $\overline{W}^i$. For frequency regulation, $d_{\max}$ is the largest credible infeed loss and $\mathbf{d}_1$ is observable from wide-area measurements. If (D2) holds only approximately, the measurement error is carried as an additional bounded disturbance, increasing ϵ proportionally.

III. SIMULATION FUNCTIONS AND THEIR COMPUTATIONS

In this work, we leverage the notion of robust simulation functions to construct an abstract system which is ϵ-close to the concrete one, where ϵ remains small enough. In the following subsection, we show how incorporating the disturbance of the concrete system into the abstract one, through an interface function $d_\mathcal{V}$, can further reduce the simulation relation error ϵ between Σ_1 and Σ_2. This enables one to perform controller synthesis on the abstract domain and refine it back over potentially high-dimensional original system while improving the scalability of the control scheme.

A. ROBUST SIMULATION FUNCTION WITH DISTURBANCE REFINEMENT

Given the system in (1), we formalize a robust simulation function $\mathcal{V}$ together with two interface functions $u_\mathcal{V}$ and $d_\mathcal{V}$. The definition below concerns a single subsystem pair, so we drop the superscript i; we write $h_z := h_z^{\text{ext}}$ for the output map and $g_z(\mathbf{x}_z, \mathbf{u}_z, \mathbf{d}_z)$ for the dynamics driven by the concatenated disturbance $\mathbf{d}_z = [\mathbf{v}_z; \mathbf{w}_z] \in V_z \times W_z$. Figure 1 illustrates the resulting hierarchical architecture. The abstract system Σ_2 receives the input $\mathbf{u}_2$ from the symbolic controller, while the concrete system Σ_1 is driven by the refined input $\mathbf{u}_1 = u_\mathcal{V}(\mathbf{u}_2, \mathbf{x}_1, \mathbf{x}_2)$ and the external disturbance $\mathbf{d}_1$. The input interface $u_\mathcal{V}$ maps the abstract input back to the concrete system, and the disturbance interface $d_\mathcal{V}$ maps the concrete disturbance $\mathbf{d}_1$ to an abstract disturbance $\mathbf{d}_2 = d_\mathcal{V}(\mathbf{d}_1, \mathbf{x}_1, \mathbf{x}_2)$; both interfaces use the states $\mathbf{x}_1$ and $\mathbf{x}_2$ as feedback.

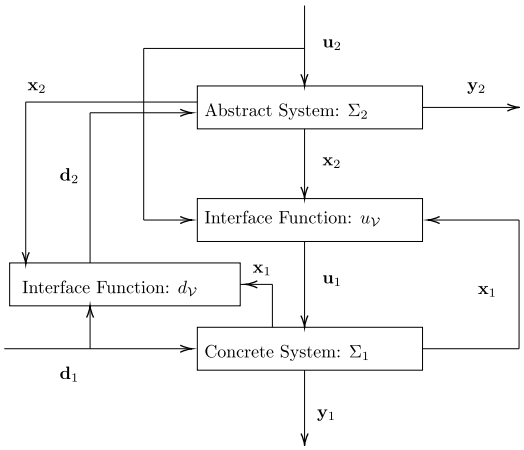


FIGURE 1. Hierarchical control architecture used in this work.

Definition 3 (Robust Simulation Functions): Consider two systems of the form (1). Let $\mathcal{V}\colon X_1 \times X_2 \to \mathbb{R}^+$ be locally Lipschitz and let $u_\mathcal{V}\colon U_2 \times X_1 \times X_2 \to U_1$, $d_\mathcal{V}\colon V_1 \times W_1 \times X_1 \times X_2 \to V_2 \times W_2$ be continuous. Then $\mathcal{V}$ is a *robust simulation function (RSF)* from Σ_2 to Σ_1 with associated interfaces $u_\mathcal{V}, d_\mathcal{V}$, if there exist class-$\mathcal{K}$ functions γ_1, γ_2 such that the following two conditions hold pointwise on $X_1 \times X_2$:

(i) (output-error bound) for all $\mathbf{x}_1 \in X_1, \mathbf{x}_2 \in X_2$,

$$\|h_1(\mathbf{x}_1) - h_2(\mathbf{x}_2)\| \leq \mathcal{V}(\mathbf{x}_1, \mathbf{x}_2); \tag{2}$$

(ii) (gain condition) for all $(\mathbf{x}_1, \mathbf{x}_2) \in X_1 \times X_2$ and all $\mathbf{u}_2 \in U_2$, $\mathbf{d}_1 \in [V_1\ W_1]^T$ with $\gamma_1(\|\mathbf{d}_1\|) + \gamma_2(\|\mathbf{u}_2\|) \leq \mathcal{V}(\mathbf{x}_1, \mathbf{x}_2)$,

$$\nabla_{\mathbf{x}_2}\mathcal{V} \cdot g_2(\mathbf{x}_2, \mathbf{u}_2, d_\mathcal{V}(\mathbf{d}_1, \mathbf{x}_1, \mathbf{x}_2)) + \nabla_{\mathbf{x}_1}\mathcal{V} \cdot g_1(\mathbf{x}_1, u_\mathcal{V}(\mathbf{u}_2, \mathbf{x}_1, \mathbf{x}_2), \mathbf{d}_1) \leq 0, \tag{3}$$

where $\nabla_{\mathbf{x}_z}\mathcal{V}$ denotes the gradient of $\mathcal{V}$ with respect to $\mathbf{x}_z$ and the dot product is contracted with the closed-loop right-hand side.

Where $\mathcal{V}$ is not differentiable, the left-hand side of (3) is understood as the upper right Dini derivative $D^+\mathcal{V}$ of $\mathcal{V}$ along the coupled closed-loop dynamics. We say Σ_1 robustly approximately simulates Σ_2 if there exists an RSF $\mathcal{V}$ from Σ_2 to Σ_1.

We note here that (2) bounds the outputs of Σ_1 and Σ_2, and (3) prevents $\mathcal{V}$ from increasing whenever it is at or above the threshold $\gamma_1(\|\mathbf{d}_1\|) + \gamma_2(\|\mathbf{u}_2\|)$ set by the disturbance and abstract input. Consequently $\mathcal{V}$ remains bounded by the larger of its initial value and that threshold, which is precisely the bound (12) established in Theorem 2. The output error might not converge to zero, and we consider this error in the resulting controller design. The interface $u_\mathcal{V}$ maps the input chosen on the lower-dimensional abstraction Σ_2 back to the concrete system Σ_1, so that guarantees on Σ_2 refine to Σ_1 at lower controller-design cost. The interface $d_\mathcal{V}$ maps the concrete disturbance $\mathbf{d}_1$ to an abstract disturbance $\mathbf{d}_2$, so that the abstract controller $\mathbf{u}_2$ can be designed robustly against any admissible $\mathbf{d}_1$ in the original system. Neither [14] nor [15] considers a disturbance interface; [15] considers only a small

disturbance on Σ_1 with no abstract counterpart. Without such an interface, the disturbance enters the error bound directly, so the simulation-relation error grows with the disturbance magnitude; under large disturbances the tightened specification can become infeasible and the resulting guarantees vacuous. The disturbance refinement through $d_{\mathcal{V}}$ counteracts precisely this conservatism.

B. NONLINEAR SYSTEM EXAMPLE

Before turning to the constructive results, we illustrate Definition 3 on a small numerical example: we verify that a candidate simulation function and a pair of interface functions satisfy conditions (2) and (3) for a simple nonlinear system and its reduced-order abstraction. Both conditions are established analytically, so the example is a certificate rather than an illustration of a single trajectory.

Consider the nonlinear system

$$\dot{\mathbf{x}}_1 = -\big(1 + \|\mathbf{x}_1\|^2\big)\mathbf{x}_1 + B_1\mathbf{u}_1 + D_1\mathbf{d}_1, \qquad \mathbf{y}_1 = C_1\mathbf{x}_1,$$

where $\mathbf{x}_1 \in \mathbb{R}^4$, $\mathbf{u}_1 \in \mathbb{R}^2$, $\mathbf{d}_1 \in \mathbb{R}^2$, $\mathbf{y}_1 \in \mathbb{R}$, and

$$B_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}^\top,$$
$$D_1 = \tfrac{1}{10}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}^\top,$$

and $C_1 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & 0 & 0 \end{bmatrix}$. We represent this system by the lower dimensional system

$$\dot{\mathbf{x}}_2 = -\big(1 + \|\mathbf{x}_2\|^2\big)\mathbf{x}_2 + B_2\mathbf{u}_2 + D_2\mathbf{d}_2, \qquad \mathbf{y}_2 = C_2\mathbf{x}_2,$$

where $\mathbf{x}_2 \in \mathbb{R}^2$, $\mathbf{u}_2 \in \mathbb{R}^2$, $\mathbf{d}_2 \in \mathbb{R}^2$, and

$$B_2 = \tfrac{1}{\sqrt{2}}\,\mathbb{I}^2, \quad D_2 = \tfrac{1}{10\sqrt{2}}\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}, \quad C_2 = \begin{bmatrix} 1 & 0 \end{bmatrix}.$$

The two models share the same drift; the abstraction aggregates the first two states of Σ_1 into one coordinate and the last two into another, through

$$P = \tfrac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{bmatrix}^\top, \qquad P^\top P = \mathbb{I}^2,$$

so that $B_2 = P^\top B_1$, $D_2 = P^\top D_1$ and $C_2 = C_1 P$. We take the candidate simulation function $\mathcal{V}(\mathbf{x}_1, \mathbf{x}_2) = \|\mathbf{x}_1 - P\mathbf{x}_2\|$, the interface functions

$$\mathbf{u}_1 = u_{\mathcal{V}}(\mathbf{u}_2, \mathbf{x}_1, \mathbf{x}_2) = \mathbf{u}_2 + B_1^\top(P\mathbf{x}_2 - \mathbf{x}_1),$$
$$\mathbf{d}_2 = d_{\mathcal{V}}(\mathbf{d}_1, \mathbf{x}_1, \mathbf{x}_2) = \mathbf{d}_1,$$

and the class-$\mathcal{K}$ functions $\gamma_1(v) = \frac{1}{10\sqrt{2}}v$ and $\gamma_2(v) = \frac{1}{\sqrt{2}}v$.

Both (2) and (3) hold for *all* $\mathbf{x}_1 \in \mathbb{R}^4$, $\mathbf{x}_2 \in \mathbb{R}^2$, $\mathbf{u}_2 \in \mathbb{R}^2$ and $\mathbf{d}_1 \in \mathbb{R}^2$. Condition (2) follows from $C_2 = C_1P$ and $\|C_1\| = 1$. For (3), write $e = \mathbf{x}_1 - P\mathbf{x}_2$: since $P^\top P = \mathbb{I}^2$ the two drifts agree under P, and as $\mathbf{x} \mapsto (1 + \|\mathbf{x}\|^2)\mathbf{x}$ is strongly monotone with modulus 1 the drift contributes at most $-\|e\|^2$ to $e^\top\dot{e}$, while $\mathbf{u}_2$ and $\mathbf{d}_1$ reach e only through $(\mathbb{I}^4 - PP^\top)B_1$ and $(\mathbb{I}^4 - PP^\top)D_1$, of norm $\frac{1}{\sqrt{2}}$ and $\frac{1}{10\sqrt{2}}$. Hence $\dot{\mathcal{V}} \le -\mathcal{V} + \gamma_1(\|\mathbf{d}_1\|) + \gamma_2(\|\mathbf{u}_2\|)$, which is non-positive precisely on the premise of (3). So $\mathcal{V}$ is an RSF from Σ_2 to Σ_1. Figure 2 shows the resulting behavior along one trajectory.

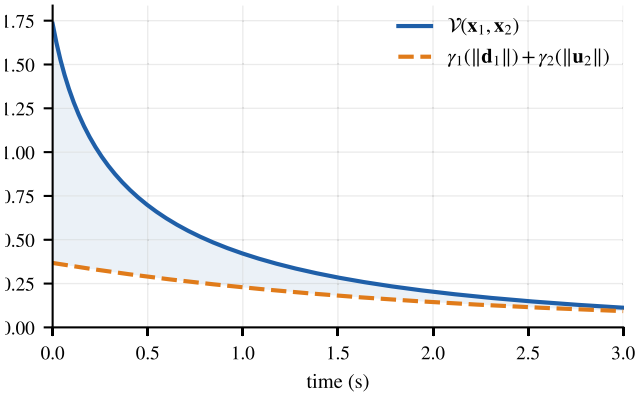


FIGURE 2. One trajectory of the example, from $\mathbf{x}_1(0) = [1, -1, 0.5, 0.5]^\top$ and $\mathbf{x}_2(0) = [0.5, -0.5]^\top$, with input $\mathbf{u}_2(t) = 0.5e^{-t/2}\hat{v}$ for a unit direction $\hat{v}$ and constant disturbance $\mathbf{d}_1$ with $\|\mathbf{d}_1\| = 0.2$. The threshold $\gamma_1(\|\mathbf{d}_1\|) + \gamma_2(\|\mathbf{u}_2\|)$ (dashed) remains below $\mathcal{V}(\mathbf{x}_1, \mathbf{x}_2)$ (solid), so the gain condition (3) is active throughout and $\mathcal{V}$ is decreasing.

C. A CLASS OF NONLINEAR SYSTEMS UNDER LARGE MEASURABLE DISTURBANCE

Here, we focus on a class of nonlinear control systems with (potentially large) measurable disturbances. A model in this class and its abstraction are specified by

$$\Sigma_z: \begin{cases} \dot{\mathbf{x}}_z = A_z\mathbf{x}_z + B_z\mathbf{u}_z + G_z\mathbf{v}_z \\ \quad + S_z\mathbf{w}_z + E_z\phi(F_z\mathbf{x}_z), \\ \mathbf{y}_z = C_z\mathbf{x}_z, \end{cases} \tag{4}$$

where $z \in \{1, 2\}$ represents the model and its abstraction respectively, and where $A_z \in \mathbb{R}^{n_z \times n_z}$, $B_z \in \mathbb{R}^{n_z \times p}$, $C_z \in \mathbb{R}^{m \times n_z}$, $G_z \in \mathbb{R}^{n_z \times q}$, $S_z \in \mathbb{R}^{n_z \times r}$, $E_z \in \mathbb{R}^{n_z \times 1}$, $F_z \in \mathbb{R}^{1 \times n_z}$. In addition, $\phi : \mathbb{R} \to \mathbb{R}$ is a nonlinear term satisfying the following slope restriction:

$$a \le \frac{\phi(c) - \phi(d)}{c - d} \le b, \quad \forall c, d \in \mathbb{R}, c \ne d. \tag{5}$$

Remark 1: Note that if $E_1 = 0$ and/or $F_1 = 0$ in (4), our proposed approach simplifies to the one we provided in [41] for the class of linear control systems with potentially large measurable disturbances.

Remark 2: Examples of nonlinear terms that satisfy the slope restriction property include saturation, sine and cosine functions. These functions are widely used within the power system literature and dynamics, making this extension to a class of nonlinear systems particularly relevant, e.g. see [43].

We define $\mathbf{d}_z = [\mathbf{v}_z\ \mathbf{w}_z]^T \in [V_z\ W_z]^T$ and $D_z = [G_z\ S_z] \in \mathbb{R}^{n_z \times (q+r)}$ as the concatenation of external and internal disturbances. It is assumed $\mathbf{d}_1$ is a measured disturbance having a known bound $d_{\max}$, i.e., $\|\mathbf{d}_1\|_\infty \le d_{\max}$. Moreover, $\mathbf{d}_2$ is derived from $\mathbf{d}_1$ with the interface function $d_{\mathcal{V}}$ (cf. (8b)).

D. RSF CONSTRUCTION FOR THE BOUNDED-SLOPE CLASS

We now construct, for the bounded-slope class (4), a reduced-dimensional abstraction together with an RSF as presented in

Definition 3. We first state a lemma that provides the matrix M and the constant λ used to build the RSF, and then present the main construction theorem. The value of the lemma is the existence of a *common* M feasible at both vertices of δ, which we will later obtain by solving a single semidefinite program containing both constraints; this is stronger than asking that $H(\delta)$ be Hurwitz for each δ separately. A pointwise-stable affine matrix family need not admit a common quadratic Lyapunov function.

Lemma 1: Let $K_1, K_2, P, D_2, Q_1, L_{11}, L_{21}$ be matrices for which the parameterized matrix

$$H(\delta) = (A_1 - PD_2(K_1 + Q_1) + B_1K_2) + \delta\,(E_1 + B_1L_{21} - PD_2L_{11})\,F_1$$

is affine in δ, where $[a, b]$ is the slope interval of (5). Suppose there exist a symmetric positive-definite matrix $M \succ 0$ and a positive constant $\lambda > 0$ such that

$$C_1^T C_1 \preceq M, \tag{6a}$$
$$H(a)^T M + MH(a) \preceq -2\lambda M, \tag{6b}$$
$$H(b)^T M + MH(b) \preceq -2\lambda M. \tag{6c}$$

Then the dissipation inequality $H(\delta)^T M + MH(\delta) \preceq -2\lambda M$ holds for *every* $\delta \in [a, b]$. Moreover, if $M \succ 0$ and $\lambda > 0$ satisfy only the two vertex inequalities (6b)–(6c), then cM satisfies all of (6) with the same λ for every sufficiently large $c > 0$, so that (6a) entails no loss of generality.

Proof: Since H is affine in δ, every $\delta \in [a, b]$ can be written as $\delta = \theta a + (1 - \theta)b$ with $\theta \in [0, 1]$, so $H(\delta) = \theta H(a) + (1 - \theta)H(b)$. The map $H \mapsto H^T M + MH$ is linear, so

$$\begin{aligned} H(\delta)^T M + MH(\delta) &= \theta\,(H(a)^T M + MH(a)) \\ &\quad + (1 - \theta)\,(H(b)^T M + MH(b)) \\ &\preceq -2\lambda(\theta + (1 - \theta))M = -2\lambda M, \end{aligned}$$

which is the claimed inequality. For the final statement, both sides of (6b)–(6c) are homogeneous of degree one in M, so cM satisfies them for every $c > 0$ with λ unchanged, while any $c \geq \lambda_{\max}(M^{-1/2}C_1^T C_1 M^{-1/2})$ gives $C_1^T C_1 \preceq cM$. □

Using Lemma 1, we now propose the next theorem to construct an RSF. Throughout the construction, the matrices that are not fixed by the model order reduction (e.g., B_2, D_2, E_2, and the gains entering the interfaces) are decision variables: they are chosen to satisfy the matrix equalities and LMIs below and to minimize the gains (9)–(10).

Theorem 1: Consider two systems of the form (4). Assume that there exist matrices $P, D_2, K_1, K_2, Q_1, Q_2, L_{11}, L_{12}, L_{21}, L_{22}$, together with $M \succ 0$ and $\lambda > 0$, such that the vertex LMIs (6) of Lemma 1 hold and such that the following matrix equalities hold:

$$C_2 = C_1P, \tag{7a}$$
$$F_2 = F_1P, \tag{7b}$$
$$A_1P + B_1Q_2 = PA_2 + PD_2Q_1P, \tag{7c}$$
$$E_1 = PE_2 - B_1(L_{21} - L_{22}) + PD_2(L_{11} - L_{12}). \tag{7d}$$

Then $\mathcal{V}$ in the form of

$$\mathcal{V}(\mathbf{x}_1, \mathbf{x}_2) = \sqrt{(\mathbf{x}_1 - P\mathbf{x}_2)^T M(\mathbf{x}_1 - P\mathbf{x}_2)}$$

is an RSF from Σ_2 to Σ_1 with its associated interfaces

$$\begin{aligned} u_{\mathcal{V}} &= K_2(\mathbf{x}_1 - P\mathbf{x}_2) + Q_2\mathbf{x}_2 + R_2\mathbf{u}_2 \\ &\quad + L_{21}\phi(F_1\mathbf{x}_1) - L_{22}\phi(F_1P\mathbf{x}_2), \end{aligned} \tag{8a}$$

$$\begin{aligned} d_{\mathcal{V}} &= K_1(\mathbf{x}_1 - P\mathbf{x}_2) + Q_1\mathbf{x}_1 + R_1\mathbf{d}_1 \\ &\quad + L_{11}\phi(F_1\mathbf{x}_1) - L_{12}\phi(F_1P\mathbf{x}_2). \end{aligned} \tag{8b}$$

In addition, the class-$\mathcal{K}$ functions γ_1 and γ_2 are designed as

$$\gamma_1(v) = \frac{\|\sqrt{M}(D_1 - PD_2R_1)\|}{\lambda}v, \tag{9}$$

$$\gamma_2(v) = \frac{\|\sqrt{M}(B_1R_2 - PB_2)\|}{\lambda}v, \tag{10}$$

where R_1 and R_2 are matrices of compatible dimensions and $\|\cdot\|$ denotes the induced Euclidean norm.

Proof: Define the closed-loop right-hand sides

$$f_1^{cl}(\mathbf{x}_1, \mathbf{x}_2, \mathbf{u}_2, \mathbf{d}_1) := A_1\mathbf{x}_1 + B_1u_{\mathcal{V}} + D_1\mathbf{d}_1 + E_1\phi(F_1\mathbf{x}_1),$$
$$f_2^{cl}(\mathbf{x}_1, \mathbf{x}_2, \mathbf{u}_2, \mathbf{d}_1) := A_2\mathbf{x}_2 + B_2\mathbf{u}_2 + D_2d_{\mathcal{V}} + E_2\phi(F_2\mathbf{x}_2),$$

where $u_{\mathcal{V}}$ and $d_{\mathcal{V}}$ are the interfaces in (8). Set $e := \mathbf{x}_1 - P\mathbf{x}_2$.

Step 1: (2). From (6a) and (7a), $\mathcal{V}(\mathbf{x}_1, \mathbf{x}_2)^2 = e^T Me \geq e^T C_1^T C_1 e = \|C_1\mathbf{x}_1 - C_2\mathbf{x}_2\|^2$, so $\mathcal{V}(\mathbf{x}_1, \mathbf{x}_2) \geq \|h_1(\mathbf{x}_1) - h_2(\mathbf{x}_2)\|$.

Step 2: (3). The directional derivative of $\mathcal{V}$ along the closed-loop dynamics is $\nabla_{\mathbf{x}_2}\mathcal{V} \cdot f_2^{cl} + \nabla_{\mathbf{x}_1}\mathcal{V} \cdot f_1^{cl}$. Using $\mathcal{V}(\mathbf{x}_1, \mathbf{x}_2) = \sqrt{e^T Me}$ and $\nabla_{\mathbf{x}_z}\mathcal{V} = \frac{1}{2\mathcal{V}}(\partial e^T Me/\partial \mathbf{x}_z)$, this reduces to $\frac{1}{\mathcal{V}}\,e^T M\,\dot{e}$ with $\dot{e} = \dot{\mathbf{x}}_1 - P\dot{\mathbf{x}}_2$. Substituting f_1^{cl} and f_2^{cl} and using the equalities (7b)–(7d) gives

$$\dot{e} = H(\delta(\mathbf{x}_1, \mathbf{x}_2))\,e + (D_1 - PD_2R_1)\mathbf{d}_1 + (B_1R_2 - PB_2)\mathbf{u}_2,$$

where $\delta(\mathbf{x}_1, \mathbf{x}_2) \in [a, b]$ is the mean-value coefficient defined by the slope restriction (5), i.e. for which $\phi(F_1\mathbf{x}_1) - \phi(F_1P\mathbf{x}_2) = \delta(\mathbf{x}_1, \mathbf{x}_2)\,F_1\,e$. By Lemma 1 the inequality $H(\delta)^T M + MH(\delta) \preceq -2\lambda M$ holds for *every* $\delta \in [a, b]$, hence for the state-dependent $\delta(\mathbf{x}_1, \mathbf{x}_2)$. Therefore

$$\begin{aligned} e^T M\dot{e} &\leq -\lambda\,e^T Me + e^T M(D_1 - PD_2R_1)\mathbf{d}_1 \\ &\quad + e^T M(B_1R_2 - PB_2)\mathbf{u}_2 \\ &\leq -\lambda\,\mathcal{V}^2 + \|\sqrt{M}e\|\,\big(\|\sqrt{M}(D_1 - PD_2R_1)\|\,\|\mathbf{d}_1\| \\ &\quad + \|\sqrt{M}(B_1R_2 - PB_2)\|\,\|\mathbf{u}_2\|\big), \end{aligned}$$

where we used Cauchy–Schwarz. Consider first the case $\mathcal{V} > 0$. Dividing by $\mathcal{V} = \|\sqrt{M}e\|$,

$$\begin{aligned} \dot{\mathcal{V}} \leq\ & -\lambda\mathcal{V} + \|\sqrt{M}(D_1 - PD_2R_1)\|\,\|\mathbf{d}_1\| \\ & + \|\sqrt{M}(B_1R_2 - PB_2)\|\,\|\mathbf{u}_2\|. \end{aligned} \tag{11}$$

Substituting the definitions of γ_1, γ_2 from (9)–(10), $\dot{\mathcal{V}} \leq -\lambda\mathcal{V} + \lambda\gamma_1(\|\mathbf{d}_1\|) + \lambda\gamma_2(\|\mathbf{u}_2\|)$. Whenever $\gamma_1(\|\mathbf{d}_1\|) + \gamma_2(\|\mathbf{u}_2\|) \leq \mathcal{V}$, the right-hand side is ≤ 0, which is exactly the gain condition (3).

For the case $\mathcal{V} = 0$, i.e. $e = 0$, at which $\mathcal{V}$ is not differentiable and the left-hand side of (3) is read as the upper right Dini derivative $D^+\mathcal{V}$ along the coupled closed-loop dynamics. If the premise of the gain condition holds at such a point, then $\gamma_1(\|\mathbf{d}_1\|) + \gamma_2(\|\mathbf{u}_2\|) \leq \mathcal{V} = 0$. Since γ_1, γ_2 are class-$\mathcal{K}$ and hence non-negative and vanishing only at the origin, this forces $\mathbf{d}_1 = 0$ and $\mathbf{u}_2 = 0$. Substituting into the error dynamics with $e = 0$ gives $\dot{e} = H(\delta)\,0 + (D_1 - PD_2R_1)\,0 + (B_1R_2 - PB_2)\,0 = 0$, so $D^+\mathcal{V} = 0 \leq 0$ and (3) holds at $e = 0$ as well. □

We now leverage the constructed $\mathcal{V}$ in Theorem 1 and quantify the mismatch between output trajectories of Σ_1 and Σ_2 with measurable disturbances, as presented in the next theorem.

Theorem 2: Consider two systems of the form (4). Let $\mathcal{V}$ be an RSF from Σ_2 to Σ_1 with associated interface function $u_{\mathcal{V}}$. Let $\mathbf{u}_2(t)$ be an admissible input of Σ_2 and $\mathbf{x}_1(t)$ a state trajectory of Σ_1 satisfying the closed-loop dynamics under $u_{\mathcal{V}}$. Then

$$\|\mathbf{y}_1(t) - \mathbf{y}_2(t)\| \leq \epsilon = \max\Big\{\mathcal{V}(\mathbf{x}_1(0), \mathbf{x}_2(0)), \gamma_1(\|\mathbf{d}_1\|_\infty) + \gamma_2(\|\mathbf{u}_2\|_\infty)\Big\}. \tag{12}$$

Proof: For brevity, write $\mathcal{V}(t) := \mathcal{V}(\mathbf{x}_1(t), \mathbf{x}_2(t))$. Set $\epsilon = \max\{\mathcal{V}(0),\ \gamma_1(\|\mathbf{d}_1\|_\infty) + \gamma_2(\|\mathbf{u}_2\|_\infty)\}$. We show $\mathcal{V}(t) \leq \epsilon$ for all $t \geq 0$. The case $t = 0$ is immediate. Suppose, for contradiction, that there exists $t_1 > 0$ with $\mathcal{V}(t_1) > \epsilon$. Then there exists $t_0 \in [0, t_1)$ with $\mathcal{V}(t_0) = \epsilon$ and $\mathcal{V}(t) > \epsilon$ for all $t \in (t_0, t_1]$. For every such t, $\gamma_1(\|\mathbf{d}_1(t)\|) + \gamma_2(\|\mathbf{u}_2(t)\|) \leq \gamma_1(\|\mathbf{d}_1\|_\infty) + \gamma_2(\|\mathbf{u}_2\|_\infty) \leq \epsilon < \mathcal{V}(t)$, so the gain condition (3) applies and $\dot{\mathcal{V}}(t) \leq 0$. Integrating, $\mathcal{V}(t_1) - \mathcal{V}(t_0) \leq 0$, contradicting $\mathcal{V}(t_1) > \epsilon = \mathcal{V}(t_0)$. Hence $\mathcal{V}(t) \leq \epsilon$ for all t, and (2) yields $\|\mathbf{y}_1(t) - \mathbf{y}_2(t)\| \leq \epsilon$. □

Remark 3: If either residual matrix ($D_1 - PD_2R_1$ in (9) or $B_1R_2 - PB_2$ in (10)) vanishes, the corresponding coefficient is zero, in which case γ_i is taken as $\gamma_i(\nu) = \eta_i\nu$ for an arbitrary $\eta_i > 0$ so that it remains class-$\mathcal{K}$; the bound (12) is unaffected.

The bound (12) reveals the role of each term. The first argument of the max captures the initial mismatch between concrete and abstract states; it can be made small by aligning the initial conditions. The second argument captures the worst-case contribution of disturbance and abstract input. Including a nonlinearity with bounded slope *inside the dynamics* (as we do via the $E_z\phi(F_z\mathbf{x}_z)$ term) does not add a separate amplitude term to the second argument, whereas folding the same nonlinearity into a disturbance term inflates that argument permanently. The nonlinearity does influence the feasible M and λ, and therefore γ_1 and γ_2; the point is it does not enter (12) as an additional disturbance. This is why our construction gives a smaller ϵ.

Our primary goal of employing the RSF is to construct an abstract system Σ_2 that is ϵ-close to the concrete system Σ_1 with ϵ small enough that, once the specification is tightened by ϵ, a non-empty target set remains for synthesis on the abstract system.

E. BEYOND THE BOUNDED-SLOPE CLASS: POLYNOMIAL AND SCENARIO-BASED CONSTRUCTIONS

The construction above assumes a nonlinearity with bounded slope. We close this section by sketching, for two related but more general classes, how Definition 3 can still be enforced. We present these as outlooks rather than formal contributions of this paper, and we do not exercise them on the case study.

1) POLYNOMIAL VECTOR FIELDS

When g_1, g_2 are polynomial vector fields, an RSF can be searched in the form $\mathcal{V}(\mathbf{x}_1, \mathbf{x}_2) = \sqrt{\theta(\mathbf{x}_1, \mathbf{x}_2)}$ with θ a non-negative polynomial, see [44]. Taking $\gamma_i(\nu) = \alpha_i\nu$, the RSF conditions are implied by the polynomial inequalities

$$\begin{aligned}&\theta(\mathbf{x}_1, \mathbf{x}_2) - (h_1(\mathbf{x}_1) - h_2(\mathbf{x}_2))^\top (h_1(\mathbf{x}_1) - h_2(\mathbf{x}_2)) \geq 0,\\ &\theta(\mathbf{x}_1, \mathbf{x}_2) - 2\alpha_1^2\,\mathbf{d}_1^\top\mathbf{d}_1 - 2\alpha_2^2\,\mathbf{u}_2^\top\mathbf{u}_2 \geq 0,\\ &\quad - \nabla_{\mathbf{x}_2}\theta \cdot g_2 - \nabla_{\mathbf{x}_1}\theta \cdot g_1 \geq 0,\end{aligned}$$

which are sufficient: the second inequality implies the gain premise $\alpha_1\|\mathbf{d}_1\| + \alpha_2\|\mathbf{u}_2\| \leq \sqrt{\theta}$ by Cauchy–Schwarz, and the third enforces the derivative condition unconditionally rather than only when that premise holds. They are linear in the coefficients of θ once the interfaces $u_{\mathcal{V}}, d_{\mathcal{V}}$ are fixed. They are amenable to sum-of-squares (SOS) programming; the interfaces themselves can be searched in an outer loop. SMT solvers [45] provide an alternative validator.

2) SCENARIO APPROACH FOR GENERAL NONLINEAR SYSTEMS

For general nonlinear g_z, the RSF conditions can be enforced approximately via the wait-and-judge scenario theory of Campi and Garatti [46], [47]. One fixes a parameterized template $\mathcal{V}(\mathbf{x}_1, \mathbf{x}_2, \theta_{\mathcal{V}})$, $u_{\mathcal{V}}(\mathbf{u}_2, \mathbf{x}_1, \mathbf{x}_2, \theta_u)$, $d_{\mathcal{V}}(\mathbf{d}_1, \mathbf{x}_1, \mathbf{x}_2, \theta_d)$ with fixed class-$\mathcal{K}$ gains γ_1, γ_2 (e.g., linear as in (a)), draws N_s i.i.d. samples $(\mathbf{x}_1^{(i)}, \mathbf{x}_2^{(i)}, \mathbf{u}_2^{(i)}, \mathbf{d}_1^{(i)})$ from the operating envelope, and solves the convex program

$$\begin{aligned}\max_{\theta_{\mathcal{V}}, \theta_u, \theta_d, \eta}\quad & \eta\\ \text{s.t. } & \|h_1(\mathbf{x}_1^{(i)}) - h_2(\mathbf{x}_2^{(i)})\| \leq \mathcal{V}(\mathbf{x}_1^{(i)}, \mathbf{x}_2^{(i)}, \theta_{\mathcal{V}}),\\ & \gamma_1(\|\mathbf{d}_1^{(i)}\|) + \gamma_2(\|\mathbf{u}_2^{(i)}\|) \leq \mathcal{V}(\mathbf{x}_1^{(i)}, \mathbf{x}_2^{(i)}, \theta_{\mathcal{V}}),\\ & \nabla_{\mathbf{x}_2}\mathcal{V} \cdot g_2\big(\cdot, d_{\mathcal{V}}(\cdot, \theta_d)\big)\\ & \quad + \nabla_{\mathbf{x}_1}\mathcal{V} \cdot g_1\big(\cdot, u_{\mathcal{V}}(\cdot, \theta_u), \mathbf{d}_1^{(i)}\big) + \eta \leq 0,\\ & \eta \geq 0, \quad i = 1, \ldots, N_s.\end{aligned}$$

The wait-and-judge bound of [46] then gives, for any confidence $\beta \in (0, 1)$, an a-posteriori risk $\rho(s^\star_{N_s})$ as a function of the support cardinality $s^\star_{N_s} \leq N_s$ of the optimal solution, such that

$$\mathbb{P}\{\text{RSF violated on a fresh sample}\} \leq \rho(s^\star_{N_s})$$

with probability at least $1 - \beta$. The polynomial determining $\rho(s^\star_{N_s})$ is the standard Campi and Garatti expression [46, Theorem 1] and we refer the reader to that source for the explicit formula. Because the resulting RSF is only a

probabilistic certificate, we do not use this construction in the case study; we mention it as a tool for fully nonlinear extensions.

IV. ASSUME-GUARANTEE CONTRACTS FOR INTERCONNECTED SYSTEMS

The RSF with disturbance refinement of the previous section mitigates the *curse of dimensionality* by replacing a high-dimensional system with a lower-dimensional abstraction. The trade-off is the buffer ϵ, which is carried through the synthesis to keep the controller robust to the information lost in the reduction. The more the system is reduced, the larger ϵ becomes, and the harder it is to synthesize a robust controller.

This approach is conservative for large-scale systems. To improve it, we combine the RSF with disturbance refinement with assume-guarantee contracts: the large-scale system is treated as an interconnected network of smaller subsystems, a reduced-order abstraction is constructed for each subsystem, and the per-subsystem guarantees are lifted to the interconnected system. The LTL properties useful for this composition are conjunction ($\wedge$) and disjunction ($\vee$): local specifications defined on the subsystems combine through conjunction into a global specification for the overall network.

A. SPECIFICATION COMPOSITION

The most important requirement in our setting is safety (invariance): each subsystem output (for NETS, the frequency deviation Δf^i) must remain inside a safe interval $\mathcal{B}^i = [\underline{\mathcal{B}}^i, \overline{\mathcal{B}}^i]$; per-subsystem target sets $\mathcal{T}^i$ are defined analogously. We write the safety part of the global LTL specification as the conjunction of local specifications ψ^i:

$$\psi^i = \square\big[\Delta f^i \in \mathcal{B}^i\big], \quad \forall i \in \{1, \dots, N\},$$
$$\psi_{\text{safe}} = \bigwedge_{i=1}^{N} \psi^i,$$

so that guaranteeing every ψ^i guarantees ψ_{safe}. The assume-guarantee composition of Theorem 3 delivers exactly ψ_{safe}, while reachability targets are treated per subsystem. Because subsystems exchange information through the coupling matrix $\mathcal{M}$, the worst-case behavior of a subsystem's neighbors must be accounted for when synthesizing its local controller. We do this in two ways in the following: either we assume that all subsystem frequencies coincide, so that the internal disturbance vanishes (*isolated subsystems*), or we treat the neighbors' frequencies as an internal disturbance to the local subsystem (*compositionality with internal disturbances*).

B. INVARIANCE CONTRACTS AND THEIR COMPOSITION

Following [48], we use assume-guarantee contracts to control subsystems independently while providing global guarantees on the interconnected system. A contract for a subsystem consists of an *assumption*, which describes the behavior the subsystem expects from its environment—here, from its neighbors through the internal disturbance—and a *guarantee*, which describes the behavior the subsystem promises in return. When every subsystem's guarantee discharges the assumptions of its neighbors, the local guarantees hold simultaneously across the network, and controllers can be designed for each subsystem in isolation. In this section we formalize this principle for safety (invariance) specifications. We claim no new contract theory: the composition result below is an instance of the invariance assume-guarantee framework of [21] and [49], stated for the interconnection of Definition 2.

We work with the closed-loop subsystems produced by the synthesis step: the subsystem Σ^i of Definition 1 under its controller, abstracted as in Section II, has the transition map

$$\mathbf{x}^i(k+1) = g^i_{\text{cl}}\big(\mathbf{x}^i(k), \mathbf{v}^i(k), \mathbf{w}^i(k)\big), \tag{13}$$

with internal outputs $\mathbf{y}^{i,\text{int}}(k) = h^{i,\text{int}}(\mathbf{x}^i(k))$ and the interconnection constraint of Definition 2 imposed at each step, $[\mathbf{w}^1(k); \dots; \mathbf{w}^N(k)] = \mathcal{M}\,[\mathbf{y}^{1,\text{int}}(k); \dots; \mathbf{y}^{N,\text{int}}(k)]$. Since all contracts in this section concern closed loops of the concrete subsystems under the refined controllers, we drop the level subscript z.

Definition 4 (Invariance Contracts): An *invariance contract* for the closed-loop subsystem (13) is a pair $\mathcal{C}^i = (\overline{W}^i, \mathcal{S}^i)$, where the *assumption set* $\overline{W}^i \subseteq W^i$ collects internal disturbances and the *guarantee set* $\mathcal{S}^i \subseteq X^i$ collects states. The closed-loop subsystem *satisfies* $\mathcal{C}^i$ if

$$g^i_{\text{cl}}(\mathbf{x}^i, \mathbf{v}^i, \mathbf{w}^i) \in \mathcal{S}^i \quad \forall \mathbf{x}^i \in \mathcal{S}^i,\ \forall \mathbf{w}^i \in \overline{W}^i,\ \forall \mathbf{v}^i \in V^i, \tag{14}$$

i.e., if $\mathcal{S}^i$ is robustly invariant under all internal disturbances in the assumption set and all admissible external disturbances.

Condition (14) is precisely what a safety controller delivers: the winning set of the symbolic synthesis is a controlled-invariant set that is robust against the declared disturbance sets. In the terminology of [21] and [49], (14) together with a safe initialization gives *strong* satisfaction of the contract—the guarantee extends one step beyond the horizon on which the assumption has been discharged.

Theorem 3 (Composition of Invariance Contracts): Consider N closed-loop subsystems (13) interconnected through the coupling matrix $\mathcal{M}$ as in Definition 2, with invariance contracts $\mathcal{C}^i = (\overline{W}^i, \mathcal{S}^i)$, $i \in \{1, \dots, N\}$, whose assumptions are consistent with the guarantees:

$$\Big(\mathcal{M}\,\big[h^{1,\text{int}}(\mathbf{x}^1); \dots; h^{N,\text{int}}(\mathbf{x}^N)\big]\Big)_i \in \overline{W}^i \tag{15}$$

for all $\mathbf{x}^j \in \mathcal{S}^j$, $j \in \{1, \dots, N\}$, and all i. If every closed-loop subsystem satisfies its contract $\mathcal{C}^i$, then every trajectory of the interconnected closed loop with $\mathbf{x}^i(0) \in \mathcal{S}^i$ for all i remains in $\prod_{i=1}^N \mathcal{S}^i$ for all $k \in \mathbb{N}$. In particular, if $\mathcal{S}^i \subseteq \{\mathbf{x}^i : \Delta f^i(\mathbf{x}^i) \in \mathcal{B}^i\}$ for the safe intervals of Section IV-A, the interconnection satisfies the global safety specification $\psi_{\text{safe}} = \bigwedge_{i=1}^N \square\big[\Delta f^i \in \mathcal{B}^i\big]$ on the trajectory.

Proof: By induction on k: $\mathbf{x}^j(0) \in \mathcal{S}^j$ for all j by hypothesis; if $\mathbf{x}^j(k) \in \mathcal{S}^j$ for all j, then by (15) the internal disturbance generated by the interconnection satisfies $\mathbf{w}^i(k) \in \overline{W}^i$, and (14) yields $\mathbf{x}^i(k+1) \in \mathcal{S}^i$ for every i. The result

is an instance of the composition theorems for invariance assume-guarantee contracts of [21, Thm. 2] and [49, Thm. 2]: satisfaction in the sense of Definition 4 implies strong satisfaction of every contract, so the strong-satisfier condition required on every cycle of the interconnection graph holds trivially. □

Remark 4 (Relation to the Contract Algebra): In the contract algebra of [48], composition absorbs the mutual dependence between assumptions and guarantees; discharging those assumptions along the trajectories of a feedback interconnection is a separate step, and Theorem 3 is exactly that step for invariance contracts. Conditioning each contract on the neighbors' *global* invariance would be circular—the network-wide invariant is what the composition is meant to establish. The one-step margin in (14) (strong satisfaction in the sense of [21]) is what breaks this circularity; the parametric small-gain theorem of [50] offers an alternative mechanism, which the invariance setting lets us avoid.

Remark 5 (Reachability): Theorem 3 composes safety only. The specification we consider also includes a reachability subformula $\Diamond\mathcal{T}$, and local liveness $\Sigma^i \models \Diamond\mathcal{T}^i$ does not in general compose to global liveness without a fairness assumption on the disturbance sequence, since an adversarial disturbance could re-perturb a different subsystem indefinitely. In our case study the disturbance is a single power-loss event: after the event, each local reach-avoid controller certifies reaching $\mathcal{T}^i$ within a bounded horizon inside its winning set, and the finite conjunction of these bounded-horizon eventualities yields the global reachability guarantee. Composing liveness in general remains open; the dynamic contracts of [51] are a natural starting point.

Remark 6 (Isolated Subsystems): If the interconnection vanishes—for NETS, the principle of interconnected synchronous machines gives $f^i = f^j$ for all i, j, which zeroes the tie-line coupling—then $\overline{W}^i = \{0\}$, the consistency condition (15) is trivial, and Theorem 3 reduces to the conjunction of N decoupled invariance guarantees: $\mathbf{x}^i(0) \in \mathcal{S}^i$ implies $\square[\mathbf{x}^i \in \mathcal{S}^i]$ for each i separately.

V. CASE STUDY: NEW ENGLAND 39-BUS TEST SYSTEM

We now bring the developed theory together in a detailed case study on a model of the New England 39-Bus Test System (NETS), a standard benchmark model for interconnected power-system dynamics. The model is similar to the three-control-area power system of [52]. NETS has 10 machines, 39 buses, 46 lines, and three areas; one of the generators represents the connection between NETS and the wider American power network.

NETS decomposes into three areas (subsystems) Σ_1^1, Σ_1^2, Σ_1^3, each containing a specific generator for frequency regulation. The interconnected system Σ_1 has 27 states (9 per subsystem Σ_1^i). External disturbances $\mathbf{v}_1^1$, $\mathbf{v}_1^2$, $\mathbf{v}_1^3$ represent measurable load/generation perturbations, control inputs $\mathbf{u}_1^1$, $\mathbf{u}_1^2$, $\mathbf{u}_1^3$ are realized by Energy Storage Systems (ESSs) or Plug-in Electric Vehicles (EVs), and internal disturbances $\mathbf{w}_1^1$, $\mathbf{w}_1^2$, $\mathbf{w}_1^3$ capture the influence of neighboring areas on each local area.

Our goal is to formally control NETS. Given that formal control approaches often struggle with scalability, we employ model order reduction techniques together with RSF with disturbance refinement to reduce the number of states while providing mathematical guarantees for the system behavior. Reducing NETS from 27 states to lower dimensions introduces a reduction error ϵ which is generally very large. Hence, we employ a compositional technique to first decompose the NETS into three 9-dimensional areas and then reduce the dimension of each area via constructing reduced-order abstractions.

The need for this decomposition is concrete: a direct model reduction of the full 27-dimensional NETS to a 9-dimensional abstraction gives $\epsilon = 0.5288$, for which the tightened target set $\hat{\mathcal{T}}$ of (17) below is empty and no controller can be designed. Note that $\epsilon = 0.5288$ is not selected: it is the value Theorem 2 *returns* for the monolithic $27 \to 9$ reduction, reported because it is too large to use. The target range has half-width 0.4 Hz, so tightening by 0.5288 empties $\hat{\mathcal{T}}$ and synthesis is infeasible before reaching the solver. This motivates the compositional route, which yields $\epsilon^i \approx 0.10$. The interconnection between the three areas, shown in Fig. 3, is captured through the tie-line frequency coupling.

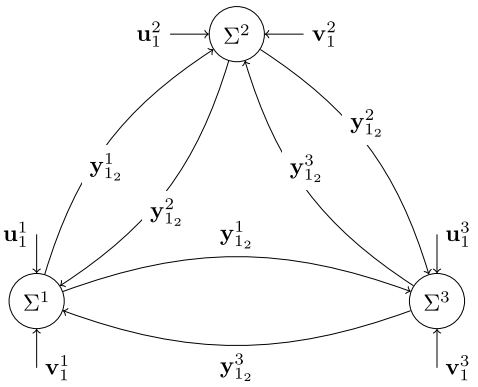


FIGURE 3. Graphical representation of NETS as a composition of three subsystems (vertices) with interconnections to neighbors (edges).

The abstract state space of the symbolic controller for NETS scales as $\boldsymbol{n}^{n_1}$, with $\boldsymbol{n}$ partitions per dimension and n_1 the dimension of the interconnected system. The compositional pipeline reduces this to $N\,\boldsymbol{n}^{\bar{n}_2}$, where N is the number of subsystems and $\bar{n}_2 = \max_i n_2^i$ the largest per-subsystem reduced order. With $\boldsymbol{n} = 140$, $n_1 = 27$, $N = 3$, and $\bar{n}_2 = 3$, the abstract state count drops from $\boldsymbol{n}^{27} \approx 8.82 \times 10^{57}$ to $3\,\boldsymbol{n}^3 = 8.23 \times 10^6$, a reduction of more than 10^{50}. The corresponding wall-clock and peak-memory figures are reported below.

Although each decomposed area of NETS has 9 states, the synthesis is still intractable for a direct grid-based abstraction because of the curse of dimensionality. We therefore build a 3-state reduced-order abstraction for each area and construct

an RSF with disturbance refinement as the relation between each concrete area and its abstraction. To preserve the interconnection of areas, we use the frequencies of neighboring areas as internal disturbances of the local area. In the frequency domain, the tie-line power interchange between area i and its neighbors is

$$\Delta P^i_{\text{tie}}(\jmath\omega) \;=\; \frac{2\pi}{\jmath\omega}\sum_{j=1}^{N} T^{ij}\left(f^i(\jmath\omega) - f^j(\jmath\omega)\right), \tag{16}$$

where f^i is the local area frequency, f^j is the neighbor's frequency, and T^{ij} is the synchronizing torque coefficient between areas i and j. Under the principle of interconnected synchronous machines [5], $f^i = f^j$ for all neighbors and the right-hand side of (16) vanishes; each area then collapses to a 9-state model with no internal disturbance.

Remark 7 (Linear vs. Nonlinear Case-Study Model): Power systems are inherently nonlinear, but for frequency regulation under load disturbances a low-order linear model around the synchronous operating point is an accurate representation, see [4, Section 2.2]. We therefore obtain a linear core for each area through Simulink Model Linearizer applied to the closed-loop system, and we append a saturation, satisfying the slope restriction (5), that captures the ESS power-output limit. Because the saturation is the only nonlinearity in the proof of concept, the case study exercises the bounded-slope class rather than a fully nonlinear swing-equation model. The framework itself, developed in Theorem 1, applies whenever the system fits the form (4) (e.g., it covers $\sin(\delta_i - \delta_j)$ swing-equation couplings restricted to a bounded operating region [43]). To strengthen confidence that the linearized model is faithful, one can add a disturbance term that bounds the linearization residual, tune the model parameters from data, or apply runtime verification to the synthesized controller.

A. SPECIFICATIONS

In this section, we define the requirements on frequency regulation based on the GB power grid using LTL specifications. A detailed description of power system frequency regulation requirements converted from natural language to LTL specifications can be found in [53]. The nominal frequency of the GB power grid is $f_0 = 50\ Hz$. The frequency f should in general remain between statutory limits for all losses up to a maximum *normal infeed loss*. Taking advantage of the fast response capabilities of *energy storage systems* (ESSs), control approaches can leverage the ESSs to respond within 1 second of the frequency crossing the limits of a deadband threshold.

We consider a stricter primary frequency specification than the GB power grid, in which the frequency f can deviate away from its steady state value f_0, the deviation is denoted by $\Delta f = f - f_0$. Since the specification is stated on the deviation Δf rather than on the frequency itself, adopting these GB-derived limits for NETS, whose nominal frequency is 60 Hz, is simply a choice of illustrative thresholds; the nominal value f_0 does not enter the analysis. We bound two regions that the frequency deviation should never transition into, $\mathcal{A}_{ub} = (\overline{\mathcal{B}}, +\infty)$ and $\mathcal{A}_{lb} = (-\infty, \underline{\mathcal{B}})$. Additionally, whenever there are deviations, the frequency should return to the target range $\mathcal{T} = [\underline{\mathcal{T}}, \overline{\mathcal{T}}]$. The desired system behavior can be described by the following LTL formulae:

$$\begin{aligned}&\psi = \square(\psi_{\text{reach}} \wedge \psi_{\text{avoid}})\\ &\text{with } \psi_{\text{reach}} = \lozenge\mathcal{T},\ \psi_{\text{avoid}} = \neg(\mathcal{A}_{ub} \vee \mathcal{A}_{lb}).\end{aligned}$$

Here $\mathcal{T}$, $\mathcal{A}_{ub}$ and $\mathcal{A}_{lb}$ are used as shorthand for the atomic propositions labeling the states whose frequency deviation lies in the respective set, via a labeling function $L\colon X \to 2^{AP}$. Since $\square(\varphi_1 \wedge \varphi_2) \equiv \square\varphi_1 \wedge \square\varphi_2$, the formula ψ is equivalent to $\square\lozenge\mathcal{T} \;\wedge\; \square\psi_{\text{avoid}}$, i.e. a *recurrence* requirement that the frequency returns to the target range infinitely often, conjoined with a safety requirement. After each deviation the frequency must return, rather than reaching $\mathcal{T}$ only once. The composition result of Section IV applies to the safety conjunct $\square\psi_{\text{avoid}}$. We modify this specification appropriately with the simulation relation error ϵ where $\mathcal{V}(\mathbf{x}_1, \mathbf{x}_2) \le \epsilon$, to acquire a conservative specification $\hat{\psi}$ over Σ_2 as:

$$\begin{aligned}&\hat{\psi} = \square(\hat{\psi}_{\text{reach}} \wedge \hat{\psi}_{\text{avoid}})\\ &\text{with } \hat{\psi}_{\text{reach}} = \lozenge\hat{\mathcal{T}},\ \hat{\psi}_{\text{avoid}} = \neg(\hat{\mathcal{A}}_{ub} \vee \hat{\mathcal{A}}_{lb}),\end{aligned} \tag{17}$$

with $\hat{\mathcal{T}} = [\underline{\mathcal{T}} + \epsilon, \overline{\mathcal{T}} - \epsilon]$, $\hat{\mathcal{A}}_{ub} = (\overline{\mathcal{B}} - \epsilon, +\infty)$ and $\hat{\mathcal{A}}_{lb} = (-\infty, \underline{\mathcal{B}} + \epsilon)$. This modification ensures that whenever the abstract system Σ_2 satisfies $\hat{\psi}$, the concrete system Σ_1 satisfies the original specification ψ by applying appropriate input and disturbance interface functions for refining the controller.

B. PROOF OF CONCEPT

We consider Σ_1 as the interconnected NETS, Σ_1^i as the 9-state decomposed subsystem i, and Σ_2^i as the 3-state reduced-order abstraction of subsystem i. In all scenarios of this case study, the default external disturbance is a power-loss event of $\mathbf{v}_1^i = 1$ per unit (100 MW, equivalent to a typical generator or about 35,000 households). The abstract systems Σ_2^i are built with MATLAB's `balreal` function by truncating to reduced-state order 3. We solve the LMIs of Lemma 1 and the matrix equalities of Theorem 1 with YALMIP [54] and MOSEK [55] on a workstation (macOS, Intel Core i5, 8 GB RAM); the LMI solve takes under 30 s per area. We synthesize the symbolic controller with SCOTS [56] on a single HPC node (Intel Xeon Gold 6248R, 48 cores, 192 GB RAM); the 3-D abstraction synthesis for Area 1 takes 77 min 34 s with peak RSS of approximately 9.1 GB. A direct 9-D synthesis attempt exhausted memory at $\boldsymbol{n} = 20$. Simulations are run over 6 seconds with a time step of 0.005 seconds. Table 1 summarizes the parameters of the symbolic synthesis. The Appendix provides the system, certificate and interface matrices for the nonlinear Area 1 proof of concept, for the linear isolated Area 1 model, and for the fully interconnected 27-state NETS model; the Area 2 and Area 3 matrices are obtained from the interconnected model by the extraction procedure described.

TABLE 1. Parameters of the symbolic synthesis in the proof of concept. The simulation time step is the integration step used for the plots, not the abstraction sampling period.

Parameter	Value
Reduced order per area (n_2^i)	3
Partitions per dimension ($\boldsymbol{n}$)	140
Abstract input bound ($\|\mathbf{u}_2\|_\infty$)	0.5
External disturbance ($\mathbf{v}_1^1$)	1 p.u.
Disturbance bound ($d_{\max}$)	1 p.u.
Simulation horizon / time step	6 s / 0.005 s

To demonstrate the proposed RSF with disturbance refinement, we consider just one area of NETS, containing 9 states with one input, one external disturbance and no internal disturbance. For the remainder of this subsection we drop the area superscript, writing Σ_1 and Σ_2 for Area 1 and its abstraction Σ_1^1 and Σ_2^1. A linear model for Area 1 of NETS is acquired using the Simulink Model Linearizer on the closed-loop system.

To add nonlinear parts to this model, we consider a collection of energy storage systems (ESSs) which provide feedback control to the system depending on the current frequency. The power output of these ESSs is limited by a saturation function. We assume to have knowledge of dynamics of this feedback but no control over its power output. The dynamics of this output are adapted and simplified from aggregate battery charger models appeared in [57] and [58]:

$$\Delta P_{ESS} = N_{ESS} \times \mathsf{sat}(\frac{k_{ESS}}{R_{ESS}} \Delta f),$$

where P_{ESS} is the power contribution of EVs, f is the system frequency, N_{ESS} is the number of participating ESSs, k_{ESS} is the average participation factor, and R_{ESS} is the droop constant. The saturation function $\mathsf{sat}(x)$ is also defined as

$$\mathsf{sat}(x) := \begin{cases} ESS_{max}, & x \geq ESS_{max}, \\ x, & ESS_{min} \leq x \leq ESS_{max}, \\ ESS_{min}, & x \leq ESS_{min}. \end{cases}$$

The saturation satisfies the slope restriction (5) with $[a, b] = [0, 1]$, so the LMI vertices of Lemma 1 are $H(0)$ and $H(1)$. We assume that $\mathbf{v}_1$ is measurable given that the disturbance may represent changes in the behavior of generation and load components, e.g., generators, plug-in electric vehicles (EVs) and ESSs. The generation or load values of these components may be known to operators and the connection/disconnection of these components could be tracked through sensors in a smart grid. We assume we have access to a fleet of EVs which can connect/disconnect from the power grid almost instantaneously. Such responsive loads are flexible and can be used for load shedding [59] and frequency regulation of smart grids [60]. The dynamics of the model are therefore a nonlinear system Σ_1^1 equivalent to (4).

1) SIMULATION RELATION ERROR

Uncontrolled system. If the response of EVs is not included in the system ($\mathbf{u}_1 = 0$), the open-loop nonlinear system Σ_1 has the maximum frequency deviation of $\Delta f = -0.6872$ Hz, which violates the specification ψ. Therefore, the contribution of EVs is essential to satisfy the specification on the frequency.

Abstraction with disturbance refinement. We apply Theorems 1–2 with the disturbance interface. The safe and target sets are $\underline{\mathcal{B}} = -0.35$, $\overline{\mathcal{B}} = 0.5$, $\underline{\mathcal{T}} = -0.3$, $\overline{\mathcal{T}} = 0.5$ (Hz). We fix $\lambda = 1.7$, $\|\mathbf{u}_2\|_\infty = 0.5$, and impose $0.01\,\mathbb{I}^9 \preceq M \preceq 120\,\mathbb{I}^9$ on the matrix M of Lemma 1, together with $L_{22} = 1$, $L_{21} = 0$, $D_2 = E_2$, $Q_1 = K_1 = 0$. These constraints linearize the otherwise bilinear product terms in the LMI feasibility problem; we picked them by a small grid search over $\lambda \in \{1.0, 1.3, 1.7, 2.0\}$ and the upper M bound $\in \{60, 120, 240\}$, which covers the regime where the LMI remains feasible. The residual of the matrix equality (7c) for the resulting P is $\|A_1P + B_1Q_2 - PA_2 - PD_2Q_1P\|_F = 4.1 \times 10^{-4}$, within numerical tolerance this can be considered equality. The residual can be accommodated rigorously by treating the leftover term $r(\mathbf{x}_2) := (A_1P + B_1Q_2 - PA_2 - PD_2Q_1P)\mathbf{x}_2$ as an additional bounded disturbance acting on the error dynamics: over the bounded operating region used for synthesis it contributes an extra additive term to (11), and hence an increment of the same order to ϵ, which is three orders of magnitude below the reported $\epsilon = 0.1019$ and does not affect any conclusion drawn below. We optimize R_1, R_2, B_2 to minimize (9)–(10), obtaining $\epsilon = 0.1019$.

Remark 8 (Disturbance Refinement vs. Disturbance Absorption): If the nonlinear terms were absorbed into an enlarged disturbance on a purely linear abstraction (the construction of [15]), ϵ rises to 0.1125 for the same operating point, an increase of 9.4%.

2) CONTROLLER SYNTHESIS

Baseline controller. As can be seen in Fig. 1, the input $\mathbf{u}_1$ for the original system is derived from the interface function which considers both system states $\mathbf{x}_1$ and $\mathbf{x}_2$ as well as the control input selected for the abstract system $\mathbf{u}_2$. Even when $\mathbf{u}_2 = 0$, the interface function may select an input $u_{\mathcal{V}} > 0$, in order to maintain $\|\mathbf{y}_1 - \mathbf{y}_2\| \leq \epsilon$. In this way, the interface function acts like a closed loop controller and so we consider the case when $\mathbf{u}_2 = 0$ as our baseline controller for this system. This way we demonstrate most clearly that the specification is guaranteed via the design of a formal controller over the abstract system $\mathbf{u}_2$ and the specification would otherwise not be satisfied.

To elaborate, we consider our RSF with the constructed abstract system Σ_2 and the interface functions (8) but with $\mathbf{u}_2 = 0$ in (8a). As Q_2 and K_2 are non-zero in (8a), control inputs are chosen automatically based on the current states of Σ_1 and Σ_2 to maintain outputs of the two systems within distance ϵ. When the power system frequency moves away from its steady-state value, the input interface function $u_{\mathcal{V}}$ generates a control input for Σ_1, which is considered here as a *baseline controller*. Although the baseline controller reduces the frequency deviations, it is still unable to satisfy

the required specification ψ. We intend to demonstrate most clearly that it is due to the formal controller we synthesize that the specification holds over the system, and that mathematical guarantees are provided.

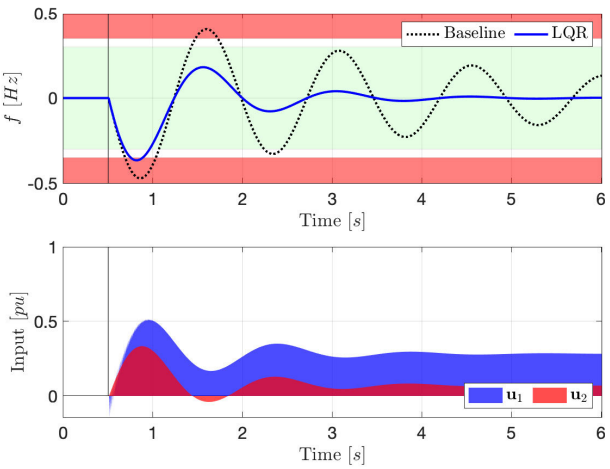


FIGURE 4. Area 1 of the linear NETS system with an LQR control strategy. Despite finding the optimal controller for system Σ_2, the controller does not satisfy the specification of Σ_1 as it enters the unsafe region (red).

To visualize this point, we provide Fig. 4. We design an LQR controller for the linear part of Area 1 of NETS, the same system as in [41]. The LQR finds the optimal cost-minimizing gain $K = [0.9648, -1.0131, 0.0524]$ for Σ_2, but the specification of Σ_1 is violated because the simulation-relation error ϵ is not accounted for during synthesis. This illustrates the value of explicitly carrying ϵ through the synthesis pipeline, as our framework does. For reproducibility: the LQR gain is $\texttt{lqr}(A_2, B_2, \mathbb{I}^3, 1)$, with $\|\mathbf{u}_2\|_\infty$ capped at 0.5, the same bound imposed on the symbolic controller in Table 1. Both are designed on the same abstraction and evaluated on the same concrete system under the same disturbance, so the comparison isolates the treatment of ϵ. The symbolic controller has no gains to tune: its parameters are the grid resolution, input bound and tightening ϵ of Table 1, and we select the minimum-energy admissible input at each state. Changing Q, R changes the LQR trajectory but not the conclusion, since no choice makes LQR aware of the abstraction error.

Controller using RSF. We employ the constructed abstraction Σ_2 as an appropriate substitute in the controller synthesis process. In particular, by knowing ϵ as the maximum error between outputs of Σ_1 and Σ_2, a symbolic controller can be first designed for the reduced-order model Σ_2 to satisfy $\hat{\psi}$ and then be refined back to Σ_1 while providing a guarantee on the satisfaction of ψ. The controller does not have a closed-form solution, but instead is a piecewise constant controller as a lookup table in the binary decision diagram (BDD) format, where for each state in the system all inputs that satisfy the specification are listed. In our simulation the smallest input is chosen, *i.e.* the input with lowest energy cost. We visualize the controller by fixing the second coordinate of the abstract state

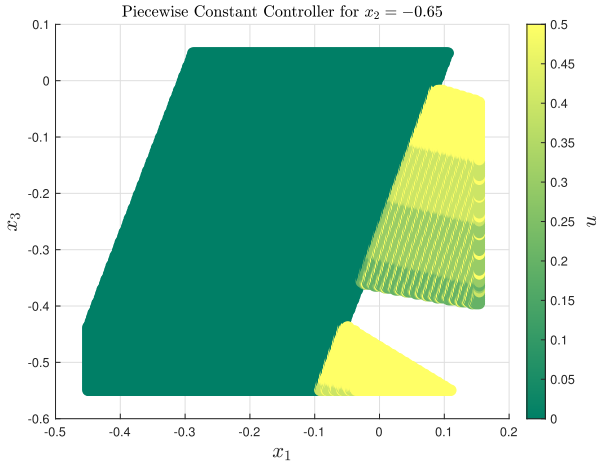


FIGURE 5. Slice of the piecewise-constant symbolic controller (BDD lookup table) at the second abstract-state coordinate fixed to -0.65. The color map shows the minimal-energy admissible input at each abstract state. White cells correspond to states from which no input satisfies $\hat{\psi}$ and are pruned during synthesis.

at -0.65 in Fig. 5 and using a color map to show the minimal input for each state. States with no color cannot satisfy the specification and so are omitted.

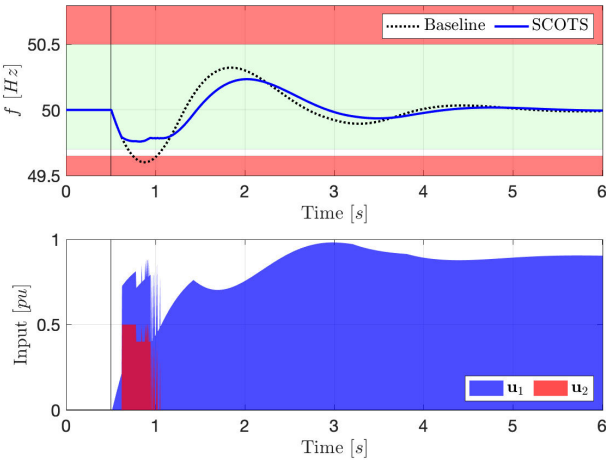


FIGURE 6. *Proof of concept (Area 1, $\mathbf{v}_1^1 = 1$ p.u., $\epsilon = 0.1019$, horizon 6 s). Top:* target range $\mathcal{T} = [-0.3, 0.5]$ Hz in green, unsafe regions $\mathcal{A}_{ub} = (0.5, \infty)$ and $\mathcal{A}_{lb} = (-\infty, -0.35)$ in red. Over the plotted horizon the SCOTS controller composed with the RSF with disturbance refinement stays within the safe and target regions required by ψ, whereas the baseline (interface-only, $\mathbf{u}_2^1$=0) controller leaves them; satisfaction of ψ itself is certified by the synthesis, not by this trace. *Bottom:* abstract control input $\mathbf{u}_2^1$ designed for Σ_2^1 and refined control input $\mathbf{u}_1^1$ delivered to Σ_1^1.

A comparison between the baseline controller and the synthesized one is provided in Fig. 6. The input $\mathbf{u}_2$, synthesized by SCOTS, is chosen to be the minimum $\mathbf{u}_2$ that guarantees satisfaction of the specification ψ. Successful synthesis of the controller over Σ_2 formally shows that ψ also holds on Σ_1. Fig. 6 (bottom) shows that over the time interval $t \in [0.5, 1]$, the synthesized controller over Σ_2 takes non-zero values to

bring back the frequency to the intended target region, thus enabling Σ_1 to satisfy ψ.

As it can be observed, we provided formal guarantees using symbolic control over a 9-dimensional system while only requiring the computational load of a 3-dimensional system. To illustrate Theorem 2, we quantify the maximum mismatch between output trajectories of Σ_1 and Σ_2 from simulations as

$$\max_t \|\mathbf{y}_1(t) - \mathbf{y}_2(t)\| = 0.0541.$$

This observed mismatch is consistent with the certified bound $\epsilon = 0.1019$. The formal robustness itself follows from the certificate of Theorem 1 and the soundness of the finite abstraction, not from this single trajectory.

C. ISOLATED CONTROLLERS

Here, we isolate the subsystems using the assumption that the frequency of NETS is the same for all subsystems, *i.e.,* $f^1 = f^2 = f^3$, following the principle of interconnected synchronous machines. Under this assumption the internal disturbance from neighboring subsystems is removed, and (16) equates to zero. Fig. 7(a) depicts this isolated design.

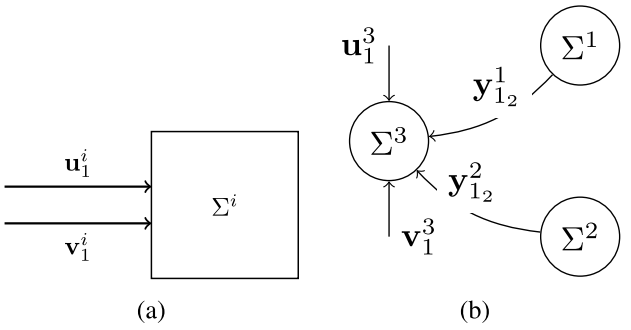


FIGURE 7. (a) Design of NETS using isolated subsystems under the principle of interconnected synchronous machines, where $i \in \{1, 2, 3\}$. (b) The NETS subsystem Σ^3 as the focal vertex of a graph in which other subsystems are neighbors and edges are interconnections; $\mathbf{u}_1^3$ is the local input, $\mathbf{v}_1^3$ the external disturbance, and $\mathbf{y}_1^{1,\text{int}}$, $\mathbf{y}_1^{2,\text{int}}$ internal disturbances acting on Σ^3.

We synthesize a controller for each area separately and obtain the global guarantee from Section IV: under isolation the internal disturbance vanishes, so each area satisfies its invariance contract with $\overline{W}^i = \{0\}$, and by Remark 6 the per-area guarantees conjoin to the specification of the interconnected power network.

1) DECENTRALIZED NETS CONTROL

Using the construction of Section V-B restricted to the linear case ($E_1^i = F_1^i = 0$ in (4)), each area's controller can be synthesized independently because isolation removes the internal disturbances. In this linear setting the per-area simulation-relation error ϵ^i (the bound of Theorem 2 applied to the pair (Σ_1^i, Σ_2^i)) is 0.1016, marginally below the $\epsilon = 0.1019$ of the nonlinear proof of concept because the saturation term is absent. The linear restriction here is intentional: the multi-area compositional pipeline is more sensitive to the conservatism of ϵ than the single-area proof of concept, and in the nonlinear setting only Area 1 yielded a non-empty winning region in our experiments. We therefore present the multi-area results in the linear setting and report the nonlinear extension as future work in Section VI. By combining the per-area guarantees through Theorem 3, in the decoupled form of Remark 6, we obtain the global safety specification on NETS. Under isolation each subsystem can be disturbed independently by $\mathbf{v}_1^i$ without any area violating its specification.

We define the global specification as

$$\psi_{\text{ra}} = \psi_{\text{ra}}^1 \wedge \psi_{\text{ra}}^2 \wedge \psi_{\text{ra}}^3,$$

where ψ_{ra}^i is the reach-avoid specification of subsystem i, the per-area analogue of ψ from Section V-A. Isolating the areas also uncouples the reachability specifications providing a higher likelihood of formal guarantees over the interconnected system. For the safety guarantees, if a system can guarantee Δf^i never falls below a bound $\underline{\mathcal{B}}'$, then it implicitly guarantees Δf^i never falls below any $\underline{\mathcal{B}}''$ with $\underline{\mathcal{B}}' > \underline{\mathcal{B}}''$. So the overall guarantee provided for all areas would match the weakest guarantee of a single area (*i.e.,* worst-case scenario). When each uncontrolled subsystem ($\mathbf{u}_2^i = 0$) is disturbed by $\mathbf{v}_1^i = 1$ per unit the frequency of multiple areas violates the safety specification.

By deploying the formally synthesized controllers with $\mathbf{u}_2^i = 0.5$, the safety conjunct of ψ_{ra} holds over the network by Theorem 3. The reachability conjunct is delivered separately, per area, by the local reach-avoid synthesis; this is sound here only because the isolation assumption $f^1 = f^2 = f^3$ makes the areas genuinely decoupled, so that the conjunction of the per-area guarantees is a guarantee for the network. Theorem 3 composes safety only, and that we do not claim a composed reachability result for the coupled model. The frequency of each area also remains close to the neighboring regions, see Fig. 8.

2) SINGLE AREA CONTROL

We consider Area 3 of NETS. When designing the controller, we consider a large measurable disturbance $\mathbf{v}_1^3$ of 1 per unit. In addition, $\mathbf{v}_1^1 = \mathbf{v}_1^2 = 0$. $\underline{\mathcal{B}} = -0.6$, $\underline{\mathcal{T}} = -0.35$, $\overline{\mathcal{B}} = \overline{\mathcal{T}} = \infty$, $\mathbf{u}_2^3 = 0.5$, and ϵ^3 is calculated as 0.1016. The synthesized controller is depicted in Fig. 9. It is worth remarking that for Area 3, it was not possible to find as tight of a reach-avoid bound as in Σ^1 and Σ^2, see extended version [40], where $\underline{\mathcal{B}} = -0.35$, $\underline{\mathcal{T}} = -0.3$, $\overline{\mathcal{B}} = \overline{\mathcal{T}} = \infty$.

D. COMPOSITIONALITY WITH INTERNAL DISTURBANCES

We now employ compositional techniques exclusively to capture internal disturbances from neighboring subsystems. Under assume-guarantee contracts, we aim to strengthen the guarantees on the behavior of the system using shared information.

For NETS, we consider additional knowledge of the frequency of neighboring regions which impacts the frequency

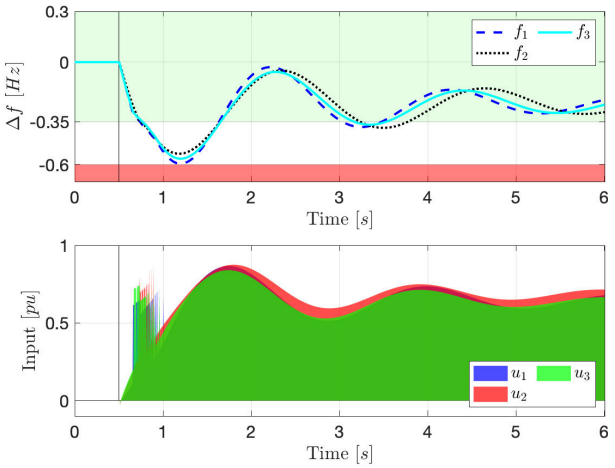


FIGURE 8. *Three-area interconnected NETS, isolated AGC controllers,* $\mathbf{v}_1^i = 1$ *p.u.,* $\mathbf{u}_2^i = 0.5$*,* $\epsilon^i = 0.1016$ *(per area). Top:* target $\mathcal{T}$ in green, unsafe $\mathcal{A}$ in red; over the plotted horizon all three frequency deviations remain within the regions required by ψ. *Bottom:* abstract input $\mathbf{u}_2^i$ from SCOTS and refined input $\mathbf{u}_1^i$ from the RSF interface, combined to deliver the global guarantee.

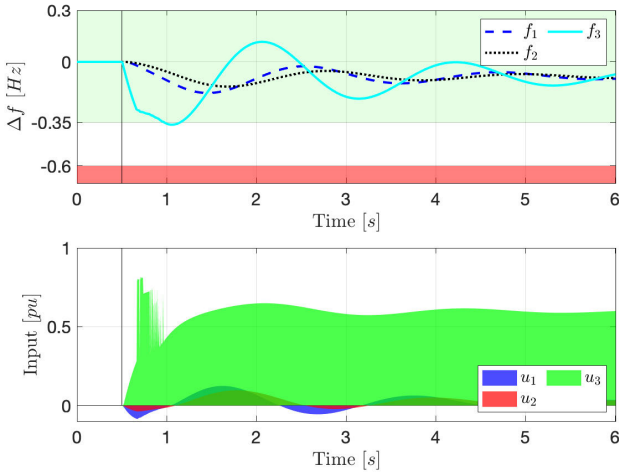


FIGURE 9. *Single-area control of NETS Area 3,* $\mathbf{v}_1^3 = 1$ *p.u.,* $\mathbf{v}_1^1 = \mathbf{v}_1^2 = 0$*,* $\mathbf{u}_2^3 = 0.5$*,* $\epsilon^3 = 0.1016$*. Top:* target $\mathcal{T}$ in green, unsafe $\mathcal{A}$ in red; over the plotted horizon the area remains within the regions required by ψ. *Bottom:* abstract input $\mathbf{u}_2^3$ from SCOTS and refined input $\mathbf{u}_1^3$ delivered to Σ_1^3.

of the local subsystem. We consider the frequency of neighboring subsystems as internal disturbances defined in (16).

When synthesizing a controller, it is important to include the neighboring frequency information in the synthesis procedure. Here, we consider a reach-avoid specification where each subsystem should avoid a region of the state space while trying to return a safe region after being disturbed. The disturbance of a neighboring area should never cause the local area to violate the specification. Therefore, in the control synthesis problem, the controller should be robust to the worst-case neighbors' frequencies. Given the reach-avoid specification for each area, the boundary of the avoid region can be used to define the worst-case disturbance acting on a local subsystem from its neighbor. Fig. 7(b) shows how this looks for Σ^3 with input $\mathbf{u}_1^3$, external disturbance $\mathbf{v}_1^3$, and internal disturbances $\mathbf{w}_1^3 = [\mathbf{y}_1^{1,\text{int}}\ \mathbf{y}_1^{2,\text{int}}]^T$.

In the framework of Section IV, the internal output of each area is its frequency deviation, $h^{i,\text{int}}(\mathbf{x}^i) = \Delta f^i$, and the coupling matrix $\mathcal{M}$ routes the neighbors' frequency deviations into the local area, where they act through the tie-line dynamics (16). The assumption set consistent with the neighbors' guarantees is therefore the box

$$\overline{W}^i = \prod_{j \neq i} [\underline{\mathcal{B}}^j, \overline{\mathcal{B}}^j], \tag{18}$$

which is what we encode as the internal-disturbance set during synthesis. Since each winning set satisfies $\mathcal{S}^j \subseteq \{\mathbf{x}^j : \Delta f^j \in \mathcal{B}^j\}$, the consistency condition (15) holds by construction, and Theorem 3 lifts the per-area safety guarantees to the interconnected NETS.

TABLE 2. Per-area simulation-relation error ϵ^i in the case study. The compositional column accounts for two internal disturbances from neighbors, and covers both the areas exposed to the loss event and the area where the loss occurs.

Subsystem	Isolated ϵ^i	Compositional ϵ^i	Abstract input $\mathbf{u}_2^i$
Σ^1	0.1016	0.1896	0.5
Σ^2	0.1016	0.1428	0.5
Σ^3	0.1016	0.1992	1.0

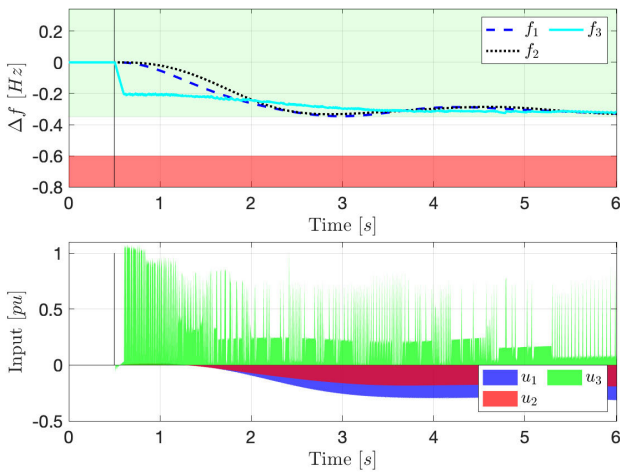


FIGURE 10. *Compositional control with internal disturbances; Area 3,* $\mathbf{v}_1^3 \leq 1$ *p.u.,* $\mathbf{u}_2^3 = 1$*,* $\epsilon^3 = 0.1992$*. Top:* target $\mathcal{T}$ in green, unsafe $\mathcal{A}$ in red; the plotted realization stays within the regions required by the specification for all three areas. The guarantee for every admissible disturbance in $\mathbf{v}_1^3 \leq 1$ p.u. comes from the contract check of Theorem 3, not from this realization. *Bottom:* abstract input $\mathbf{u}_2^3$ from SCOTS and refined input $\mathbf{u}_1^3$.

Under the compositional approach each subsystem receives two internal disturbances from its neighbors, and these inflate the simulation-relation error ϵ relative to the isolated case; the per-area values are summarized in Table 2. We define the global specification: if a disturbance

$\mathbf{v}_1^3 \leq 1$ p.u. is present in Σ^3, no area frequency may fall below $\Delta f^i \leq -0.6$ Hz. With $\mathbf{u}_2^3 = 1$ we obtain $\epsilon^3 = 0.1992$ and the controller satisfies the specification (Fig. 10). When the EV input is removed ($\mathbf{u}_2^3 = 0$), the frequency deviation violates the specification, confirming that the ESS/EV input is essential.

Table 2 shows two effects. First, the isolated ϵ^i are identical because each isolated area uses the same operating-point matrices and the same LMI parameter envelope; the ordering between areas only emerges once internal disturbances are turned on. Second, in the compositional column $\epsilon^2 < \epsilon^1 < \epsilon^3$: Area 2 has the smallest disturbance gain because its reduced-order projection P^2 gives the smallest $\|\sqrt{M}(D_1 - PD_2R_1)\|$ among the three areas, which through (9) yields the smallest γ_1, whereas Area 3, where the loss occurs, is subject to both the disturbance and an amplified input, so its ϵ^3 is largest.

E. COMPUTATIONAL COST, ROBUSTNESS AND PRACTICAL LIMITATIONS

Computational cost. For a subsystem of reduced order n_2 with $\boldsymbol{n}$ partitions per dimension and $\boldsymbol{m}$ quantized inputs, the transition relation has $\mathcal{O}(\boldsymbol{n}^{n_2}\boldsymbol{m})$ entries and the reach-avoid fixed point converges in $\mathcal{O}(\boldsymbol{n}^{n_2})$ sweeps, giving $\mathcal{O}(\boldsymbol{n}^{2n_2}\boldsymbol{m})$ operations; monolithically, n_2 is replaced by n_1. The N subsystems are independent, so their wall-clock cost is that of one area in parallel. For Area 1 this is 77 min 34 s at 9.1 GB peak, against a monolithic problem that is infeasible at any resolution and a direct 9-dimensional attempt that exhausted 192 GB at $\boldsymbol{n} = 20$. The offline LMI solve is under 30 s per area. Online, the controller is a BDD lookup plus two $\mathcal{O}(n_1 n_2)$ matrix–vector products, which is not the bottleneck at primary-response timescales.

Scope of the robustness claim. What is certified is robustness to the *disturbance and input signals*: the specification holds for every measurable $\mathbf{d}_1$ with $\|\mathbf{d}_1\|_\infty \leq d_{\max}$, not a sampled subset. It is not a guarantee against *model-parameter* variation, since perturbing $A_z, \ldots, F_z$ changes $H(\delta)$ and hence feasibility of (6). Two mitigations apply. The vertex LMIs hold with a strict margin, so a perturbation Δ preserves feasibility while $\|\Delta^\top M + M\Delta\|$ stays below it — checkable for a given uncertainty radius without re-synthesis. And any uncertainty expressible as an additive bounded signal, as linearization residuals are, is absorbed by the disturbance channel at the cost of a larger $d_{\max}$ and hence ϵ. Solving the LMIs over a polytope of plant matrices is left to future work.

Limitations. (i) Guarantees are statements about the chosen model — a linearized core per area plus one saturation (Remark 7). (ii) The disturbance must be measured online per (D2); estimation error must be carried as additional bounded disturbance. (iii) Actuation is modelled as instantaneous and rate-unconstrained, so delays and the switching activity in Figs. 6 and 8 would need dwell-time constraints in practice. (iv) Theorem 3 certifies the sampled trajectory; intersample behavior is covered only by over-approximation. (v) The bounded-slope class admits one scalar nonlinearity per subsystem, so multi-channel swing-equation models are not covered. (vi) The nonlinear multi-area synthesis gave a non-empty winning region only for Area 1, hence the linear three-area results.

VI. CONCLUSION

We presented a compositional control approach for large-scale interconnected systems under large measurable disturbances. The framework couples (i) robust simulation functions with a new disturbance-refinement interface $d_{\mathcal{V}}$, (ii) a vertex-LMI construction (Lemma 1, Theorem 1) that delivers the extension to nonlinear systems with bounded slope whenever the common vertex LMIs, the matching equalities and the interface conditions are jointly feasible, (iii) a constant-envelope simulation-relation error bound (Theorem 2), and (iv) an invariance assume-guarantee composition (Theorem 3), instantiating the framework of [21], that lifts per-subsystem safety to global safety.

Case study results. On the NETS case study, the disturbance-refinement interface reduces the simulation-relation error from $\epsilon = 0.1125$ (no disturbance interface, [15]) to $\epsilon = 0.1019$ for Area 1 in isolation, a 9.4% reduction. The compositional pipeline reduces the abstract state space from $\boldsymbol{n}^{27} \approx 8.82 \times 10^{57}$ to $3\boldsymbol{n}^3 \approx 8.23 \times 10^6$, and the abstraction is synthesized in 77 min 34 s with peak memory of 9.1 GB, whereas a direct synthesis of the original system with SCOTS exhausts memory.

Outlook. The results in this paper open several promising avenues. The bounded-slope class admits the saturation already exercised in the case study and naturally extends to the swing-equation $\sin(\delta_i - \delta_j)$ coupling (Remark 7); a follow-up exercising this end-to-end would lift the framework from primary frequency control to wide-area angle stability. Theorem 3 composes safety, and a natural next step is to compose reachability under bounded-fairness assumptions on the disturbance. On the application side, replacing the assumed instantaneous neighbor-frequency feedback with a delay-aware tightening of ϵ would let the framework target real PMU/SCADA deployments; the scenario-based extension sketched in Section III-E is a natural companion for fully nonlinear models, and integration with abstraction-free synthesis [61] promises further scalability gains.

Applicability beyond power networks. Nothing in Definitions 1–2 or Theorems 1–3 is specific to power systems: the framework applies to any network of continuous-time subsystems coupled through measurable internal signals whose subsystems admit reduced-order models satisfying (7) and (6). Networks of mobile robots are a natural candidate, with two caveats. First, the guarantee differs in kind: distributed control of such systems typically certifies tracking performance or a disturbance attenuation level, whereas we certify a temporal-logic specification over all admissible behaviors, so the two are not directly comparable without first agreeing a common specification. Second, unicycle and nonholonomic models fall outside the bounded-slope

class (4), since the heading–translation coupling is bilinear rather than slope-restricted; they would require the polynomial construction of Section III-E or feedback linearization first. Identifying which robotic interconnections admit a useful reduced-order RSF is future work rather than a corollary of these results.

APPENDIX
MATRICES OF NEW ENGLAND 39-BUS TEST SYSTEM

We denote n consecutive zero elements in a matrix by 0^n for the sake of space, e.g. $\begin{bmatrix}0^2 & 1 & 0^3\end{bmatrix} = \begin{bmatrix}0 & 0 & 1 & 0 & 0 & 0\end{bmatrix}$.

Proof of Concept - Nonlinear Area 1

$A_1, M, B_1, D_1, C_1, E_1, F_1, Q_1, Q_2, R_1, A_2, B_2, D_2, C_2, E_2, F_2, P, K_2, L_{11}, L_{12}, L_{22}, ESS_{max}, ESS_{min}$, and $[a, b]$, as shown in the equation at the bottom of the page.

Fully Interconnected New England 39-Bus System

B, C, D, and A, as shown in the equation at the top of the next page.

Linear Area 1 - Isolated

The matrices A_1, B_1, D_1, C_1, A_2, M, K_2, $Q_1 = K_1$, and $R_1 = R_2$ coincide with those of the nonlinear case above (the terms E_z, F_z, and $L_{11}, \ldots, L_{22}$ are absent in the linear case); the remaining matrices are, B_2, D_2, C_2, Q_2, and P, as shown in the equation at the top of the next page.

Area 1 is formed from rows and columns $1-8$ and 25 from A in the fully interconnected system.

Linear Area 1 - with Internal Disturbance

The internal disturbances can be derived from column 13 and column 21 of A returning the following disturbance matrix.

$$D_1 = \begin{bmatrix}0\,0\,0 & 0 & -1\,0\,0\,0\,0 \\ 0\,0\,0 & -0.37 & 0\,0\,0\,0\,0 \\ 0\,0\,0 & -0.52 & 0\,0\,0\,0\,0\end{bmatrix}^T$$

Linear Area 2 and Area 3

Area 2 and Area 3 are extracted from the fully interconnected New England 39-Bus System above in the same way

$$A_1 = \begin{bmatrix}-12.5 & 0 & 0 & 0.09 & -0.65 & 0^3 & -0.09 \\ 0 & -16.67 & 0 & 0.09 & -0.65 & 0^3 & -0.09 \\ 0 & 0 & -14.29 & 0.05 & -0.61 & 0^3 & -0.05 \\ 0 & 0 & 0 & 0 & 0.93 & 0^3 & 0 \\ 0^3 & -6.28 & -0.09 & 2.5 & 2.78 & 2.38 & 0 \\ 12.5 & 0^3 & 0 & -2.5 & 0 & 0 & 0 \\ 0 & 16.67 & 0^3 & 0 & -2.78 & 0 & 0 \\ 0 & 0 & 14.29 & 0^3 & 0 & -2.38 & 0 \\ 0 & 0 & 0 & 6.28 & 2.08 & 0^3 & 0\end{bmatrix}$$

$$M = \begin{bmatrix}0.22 & 0 & 0 & 0 & 0.01 & -0.01 & 0 & 0 & 0 \\ 0 & 0.26 & 0 & 0 & 0.01 & 0 & -0.01 & 0 & 0 \\ 0 & 0 & 0.26 & 0 & 0.01 & 0 & 0 & -0.01 & 0 \\ 0 & 0 & 0 & 82.14 & 20.22 & 0 & 0 & 0 & 16.80 \\ 0.01 & 0.01 & 0.01 & 20.22 & 11.62 & 0 & 0 & 0 & 11.68 \\ -0.01 & 0 & 0 & 0.01 & 0 & 0.02 & 0 & 0 & 0 \\ 0 & -0.01 & 0 & 0.01 & 0 & 0 & 0.02 & 0 & 0 \\ 0 & 0 & -0.01 & 0.01 & 0 & 0 & 0 & 0.02 & 0 \\ 0 & 0 & 0 & 16.80 & 11.68 & 0 & 0 & 0 & 29.44\end{bmatrix}$$

$$B_1 = \begin{bmatrix}0^4 & 1 & 0^4\end{bmatrix}^T, \quad D_1 = \begin{bmatrix}0^4 & -1 & 0^4\end{bmatrix}^T, \quad C_1 = \begin{bmatrix}0^4 & 2.05 & 0^4\end{bmatrix}$$

$$E_1 = \begin{bmatrix}0^4 & 0.0285 & 0^4\end{bmatrix}^T$$

$$F_1 = \begin{bmatrix}0^4 & 2 & 0^4\end{bmatrix}, \quad Q_1 = K_1 = \begin{bmatrix}0^9\end{bmatrix}, \quad Q_2 = \begin{bmatrix}0.02 & -0.0343 & 0.2860\end{bmatrix}, \quad R_1 = R_2 = 1$$

$$A_2 = \begin{bmatrix}-0.6333 & 3.0028 & 0.4428 \\ -3.0028 & -0.0026 & -0.0263 \\ -0.4428 & -0.0263 & -1.5159\end{bmatrix}, \quad B_2 = \begin{bmatrix}-1.0204 & 0.6395 & 0.8273\end{bmatrix}^T, \quad D_2 = \begin{bmatrix}1.0204 & -0.6395 & -0.8273\end{bmatrix}^T$$

$$C_2 = \begin{bmatrix}-1.5128 & 0.096 & 0.5044\end{bmatrix}, \quad E_2 = \begin{bmatrix}1.0204 & -0.6395 & -0.8273\end{bmatrix}^T, \quad F_2 = \begin{bmatrix}-1.4726 & 0.0934 & 0.4910\end{bmatrix}$$

$$P = \begin{bmatrix}0.03 & 0.025 & 0.03 & 0.01 & -0.74 & 0.02 & 0.04 & 0.025 & 0.55 \\ -0.01 & -0.01 & -0.01 & 0.25 & 0.05 & -0.08 & -0.08 & -0.08 & 0.3 \\ -0.02 & -0.015 & -0.015 & -0.15 & 0.25 & -0.28 & -0.21 & -0.26 & 0.44\end{bmatrix}^T$$

$$K_2 = \begin{bmatrix}-0.2 & -0.2 & -0.2 & -482.5 & -278.9 & -2.5 & -2.8 & -2.4 & -279.9\end{bmatrix}$$

$$L_{11} = L_{21} = 0, \quad L_{12} = 0.0285, \quad L_{22} = 1, \quad ESS_{max} = 0.5454, \quad ESS_{min} = 0, \quad [a, b] = [0, 1].$$

$$B = \begin{bmatrix} 0^4 & 1 & 0^{22} \\ 0^{12} & 1 & 0^{14} \\ 0^{20} & 1 & 0^6 \end{bmatrix}^T, \quad C = \begin{bmatrix} 0^4 & 2.05 & 0^{22} \\ 0^{12} & 1.83 & 0^{14} \\ 0^{20} & 2.09 & 0^6 \end{bmatrix}, \quad D = \begin{bmatrix} 0^4 & -1 & 0^{22} \\ 0^{12} & -1 & 0^{14} \\ 0^{20} & -1 & 0^6 \end{bmatrix}^T$$

$$A = \begin{bmatrix}
-12.5 & 0^2 & 0.09 & -0.65 & 0 & 0 & 0 & 0^{16} & -0.11 & 0^2 \\
0 & -16.67 & 0 & 0.09 & -0.65 & 0^2 & 0 & 0^{16} & -0.11 & 0^2 \\
0 & 0 & -14.29 & 0.05 & -0.61 & 0^2 & 0 & 0^{16} & -0.05 & 0^2 \\
0^2 & 0 & 0 & 0.92 & 0^2 & 0^5 & -0.37 & 0^7 & -0.52 & 0^6 \\
0^2 & 0 & -6.28 & -0.09 & 2.5 & 2.78 & 2.38 & 0^{16} & 0 & 0^2 \\
12.5 & 0^2 & 0 & 0 & -2.5 & 0 & 0 & 0^{16} & 0 & 0^2 \\
0 & 16.67 & 0^2 & 0 & 0 & -2.78 & 0 & 0^{16} & 0 & 0^2 \\
0^2 & 14.29 & 0 & 0 & 0 & 0 & -2.38 & 0^{16} & 0 & 0^2 \\
0^8 & -16.67 & 0^2 & 0.18 & -0.61 & 0^3 & 0^8 & 0 & -0.19 & 0 \\
0^8 & 0 & -16.67 & 0 & 0 & -0.68 & 0^3 & 0^8 & 0 & 0^2 \\
0^8 & 0^2 & -12.5 & 0.12 & -0.69 & 0^3 & 0^8 & 0 & -0.13 & 0 \\
0^4 & -0.41 & 0^3 & 0^4 & 0.58 & 0^3 & 0^4 & -0.25 & 0^3 & 0^3 \\
0^8 & 0^2 & 0 & -6.28 & -0.08 & 2.27 & 3.13 & 2.5 & 0^8 & 0^3 \\
0^8 & 16.67 & 0 & 0^2 & 0 & -2.27 & 0 & 0 & 0^8 & 0^3 \\
0^8 & 0 & 16.67 & 0^2 & 0 & 0 & -3.13 & 0 & 0^8 & 0^3 \\
0^8 & 0 & 0 & 12.5 & 0^2 & 0 & 0 & -2.5 & 0^8 & 0^3 \\
0^8 & 0^8 & -14.29 & 0 & 0 & 0 & -0.74 & 0 & 0^2 & 0^3 \\
0^8 & 0^8 & 0 & -14.29 & 0 & 0.12 & -0.65 & 0^3 & 0^2 & -0.17 \\
0^8 & 0^8 & 0 & 0 & -12.5 & 0.12 & -0.67 & 0^2 & 0^3 & -0.17 \\
0^4 & -0.51 & 0^3 & 0^4 & -0.22 & 0^3 & 0^4 & 0.77 & 0^3 & 0^3 \\
0^8 & 0^8 & 0^2 & 0 & -6.28 & -0.096 & 3.33 & 2.5 & 2.44 & 0^3 \\
0^8 & 0^8 & 14.29 & 0^2 & 0 & 0 & -3.33 & 0 & 0 & 0^3 \\
0^8 & 0^8 & 0 & 14.29 & 0 & 0 & 0^2 & -2.5 & 0 & 0^3 \\
0^8 & 0^8 & 0 & 0 & 12.5 & 0 & 0 & 0^2 & -2.44 & 0^3 \\
0 & 0 & 0 & 6.28 & 2.08 & 0^2 & 0 & 0^8 & 0^8 & 0^3 \\
0^8 & 0 & 0 & 0 & 6.28 & 2.16 & 0^2 & 0 & 0^8 & 0^3 \\
0^8 & 0^8 & 0 & 0 & 0 & 6.28 & 2.24 & 0^2 & 0 & 0^3
\end{bmatrix}$$

$$B_2 = \begin{bmatrix} -0.8580 & 0.5378 & 0.6956 \end{bmatrix}^T$$
$$D_2 = \begin{bmatrix} 0.8580 & -0.5378 & -0.6956 \end{bmatrix}^T$$
$$C_2 = \begin{bmatrix} -1.7990 & 0.1141 & 0.5998 \end{bmatrix}$$
$$Q_2 = \begin{bmatrix} 0.0238 & -0.0407 & 0.3401 \end{bmatrix}$$
$$P = \begin{bmatrix} 0.04 & 0.03 & 0.03 & 0.02 & -0.88 & 0.025 & 0.044 & 0.03 & 0.66 \\ -0.01 & -0.01 & -0.01 & 0.29 & 0.06 & -0.10 & -0.98 & -0.99 & 0.36 \\ -0.03 & -0.18 & -0.018 & -0.18 & 0.29 & -0.33 & -0.25 & -0.31 & 0.52 \end{bmatrix}^T.$$

as Area 1: Area 2 from rows and columns 9–16 and 26, and Area 3 from rows and columns 17–24 and 27, with the reduced-order abstraction then obtained by `balreal` truncation to order 3 exactly as for Area 1.

DATA ACCESS STATEMENT

No external data were used in this study. The system matrices underlying the case study are given in the Appendix.

ACKNOWLEDGMENT

The authors thank Abolfazl Lavaei for his input during early iterations of this work.

REFERENCES

[1] E. A. Lee, "Cyber physical systems: Design challenges," in *Proc. 11th IEEE Int. Symp. Object Component-Oriented Real-Time Distrib. Comput. (ISORC)*, May 2008, pp. 363–369.
[2] A. Pnueli, "The temporal logic of programs," in *Proc. 18th Annu. Symp. Found. Comput. Sci. (SFCS)*, Sep. 1977, pp. 46–57.
[3] A. Lavaei, S. Soudjani, A. Abate, and M. Zamani, "Automated verification and synthesis of stochastic hybrid systems: A survey," *Automatica*, vol. 146, Dec. 2022, Art. no. 110617.
[4] H. Bevrani, *Robust Power System Frequency Control*. Cham, Switzerland: Springer, 2009.
[5] P. Kundur, N. Balu, and M. Lauby, *Power System Stability and Control*. New York, NY, USA: McGraw-Hill, 1994.
[6] J. Heidary, M. Gheisarnejad, H. Rastegar, and M. H. Khooban, "Survey on microgrids frequency regulation: Modeling and control systems," *Electr. Power Syst. Res.*, vol. 213, Dec. 2022, Art. no. 108719.

[7] R. R. Kumar, A. K. Yadav, and M. Ramesh, "Hybrid PID plus LQR based frequency regulation approach for the renewable sources based standalone microgrid," *Int. J. Inf. Technol.*, vol. 14, no. 5, pp. 2567–2574, Aug. 2022.

[8] X. Liu, C. Wang, X. Kong, Y. Zhang, W. Wang, and K. Y. Lee, "Tube-based distributed MPC for load frequency control of power system with high wind power penetration," *IEEE Trans. Power Syst.*, vol. 39, no. 2, pp. 3118–3129, Mar. 2024.

[9] R. Sepehrzad, S. Nakhaeisharif, A. Al-Durra, M. Allahbakhshi, and A. Moridi, "Islanded micro-grid frequency control based on the optimal-intelligent Lyapunov algorithm considering power dynamic and communication uncertainties," *Electric Power Syst. Res.*, vol. 208, Jul. 2022, Art. no. 107917.

[10] L. Dritsas, E. Kontouras, E. Vlahakis, I. Kitsios, G. Halikias, and A. Tzes, "Modelling issues and aggressive robust load frequency control of interconnected electric power systems," *Int. J. Control*, vol. 95, no. 3, pp. 753–767, Mar. 2022.

[11] M. Althoff, "Benchmarks for the formal verification of power systems," in *Proc. 9th Int. Workshop Appl. Verification Continuous Hybrid Syst.*, 2022, pp. 26–43.

[12] C. Baier and J.-P. Katoen, *Principles of Model Checking*. Cambridge, MA, USA: MIT Press, 2008.

[13] P. Tabuada, *Verification Control Hybrid Systems: A Symbolic Approach*. Cham, Switzerland: Springer, 2009.

[14] A. Girard and G. J. Pappas, "Hierarchical control system design using approximate simulation," *Automatica*, vol. 45, no. 2, pp. 566–571, Feb. 2009.

[15] V. Kurtz, P. M. Wensing, and H. Lin, "Robust approximate simulation for hierarchical control of linear systems under disturbances," in *Proc. Amer. Control Conf. (ACC)*, Jul. 2020, pp. 5352–5357.

[16] Y. Nie, Z. Wang, L. Gao, J. Li, and Y. Zhao, "Frequency-weighted residual truncation and Padé approximant for model reduction of power system with constant time delay," *IEEE Access*, vol. 8, pp. 63018–63026, 2020.

[17] N. Tong, Z. Jiang, L. Zhu, and Y. Liu, "Dynamic model reduction for large-scale power systems using wide-area measurements," *IEEE Access*, vol. 8, pp. 97863–97872, 2020.

[18] K. Hsu, R. Majumdar, K. Mallik, and A.-K. Schmuck, "Multi-layered abstraction-based controller synthesis for continuous-time systems," in *Proc. 21st Int. Conf. Hybrid Syst., Comput. Control (part CPS Week)*, Apr. 2018, pp. 120–129.

[19] F. Kerber and A. van der Schaft, "Compositional analysis for linear control systems," in *Proc. 13th ACM Int. Conf. Hybrid Syst., Comput. control*. New York, NY, USA: Association for Computing Machinery, Apr. 2010, pp. 21–30.

[20] G. Frehse, "Compositional verification of hybrid systems using simulation relations," Ph.D. dissertation, Radboud Univ. Nijmegen, Nijmegen, The Netherlands, 2005.

[21] A. Saoud, A. Girard, and L. Fribourg, "Assume-guarantee contracts for continuous-time systems," *Automatica*, vol. 134, Dec. 2021, Art. no. 109910.

[22] P. Nuzzo, H. Xu, N. Ozay, J. B. Finn, A. L. Sangiovanni-Vincentelli, R. M. Murray, A. Donzé, and S. A. Seshia, "A contract-based methodology for aircraft electric power system design," *IEEE Access*, vol. 2, pp. 1–25, 2014.

[23] X. Liu, "Compositional verification using geodesic distance via assume-guarantee reasoning," *IEEE Access*, vol. 12, pp. 92612–92621, 2024.

[24] G. Pola, P. Pepe, and M. D. Di Benedetto, "Symbolic models for networks of control systems," *IEEE Trans. Autom. Control*, vol. 61, no. 11, pp. 3663–3668, Nov. 2016.

[25] Y. Tazaki and J.-I. Imura, "Bisimilar finite abstractions of interconnected systems," in *Proc. Int. Workshop Hybrid Syst., Comput. Control*. Cham, Switzerland: Springer, 2008, pp. 514–527.

[26] A. Lavaei, S. Soudjani, and M. Zamani, "Compositional construction of infinite abstractions for networks of stochastic control systems," *Automatica*, vol. 107, pp. 125–137, Sep. 2019.

[27] A. Lavaei and M. Zamani, "From dissipativity theory to compositional synthesis of large-scale stochastic switched systems," *IEEE Trans. Autom. Control*, vol. 67, no. 9, pp. 4422–4437, Sep. 2022.

[28] A. M. Stankovic, S. D. Đukic, and A. T. Saric, "Approximate Bisimulation-based reduction of power system dynamic models," *IEEE Trans. Power Syst.*, vol. 30, no. 3, pp. 1252–1260, May 2015.

[29] M. Althoff, "Formal and compositional analysis of power systems using reachable sets," *IEEE Trans. Power Syst.*, vol. 29, no. 5, pp. 2270–2280, Sep. 2014.

[30] Y. Li, P. Zhang, M. Althoff, and M. Yue, "Distributed formal analysis for power networks with deep integration of distributed energy resources," *IEEE Trans. Power Syst.*, vol. 34, no. 6, pp. 5147–5156, Nov. 2019.

[31] D. Zonetti, A. Saoud, A. Girard, and L. Fribourg, "A symbolic approach to voltage stability and power sharing in time-varying DC microgrids," in *Proc. 18th Eur. Control Conf. (ECC)*, Jun. 2019, pp. 903–909.

[32] A. Venzke and S. Chatzivasileiadis, "Verification of neural network behaviour: Formal guarantees for power system applications," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 383–397, Jan. 2021.

[33] W. M. Dahmane, S. Ouchani, and H. Bouarfa, "Towards a reliable smart city through formal verification and network analysis," *Comput. Commun.*, vol. 180, pp. 171–187, Dec. 2021.

[34] T. C. Bui, H. T. Bui, V. L. Nguyen, D. T. Nguyen, D. A. Nguyen, and M. H. Luong, "Towards formal verification of smart grids: An effective modelling approach and some first experimentation," *VNUHCM J. Eng. Technol.*, vol. 6, no. 3, pp. 1924–1936, 2023.

[35] B. Qin and D. Liu, "Formal modeling and verification method of power grid cyber physical system based on coupling of information and energy flow," in *Proc. 25th Int. Conf. Electr. Distrib. (CIRED)*. Madrid, Spain: AIM, 2019, pp. 1–5.

[36] T. Ladner, M. Eichelbeck, and M. Althoff, "Formal verification of graph convolutional networks with uncertain node features and uncertain graph structure," *Trans. Mach. Learn. Res.*, pp. 1–29, Apr. 2025.

[37] A. M. Tumlin, B. Wooding, Z. Shao, D. M. Lopez, T. Derr, and T. T. Johnson, "Reachability-based formal verification of graph neural networks with node and edge features," in *Proc. 3rd Int. Symp. (SAIV)*, Lisbon, Portugal. Cham, Switzerland: Springer, 2026, pp. 271–298.

[38] M. Abdelghany and S. Tahar, "Reliability analysis of smart grids using formal methods," in *Handbook of Smart Energy Systems*. Cham, Switzerland: Springer, 2022, pp. 1–17.

[39] W. Ahmad, O. Hasan, F. Awwad, N. Bastaki, and S. R. Hasan, "Formal reliability analysis of an integrated power generation system using theorem proving," *IEEE Syst. J.*, vol. 14, no. 4, pp. 4820–4831, Dec. 2020.

[40] B. Wooding, A. Lavaei, and S. Soudjani, "Formal control of new England 39-bus test system: An assume-guarantee approach," 2023, *arXiv:2307.03467*.

[41] B. Wooding, A. Lavaei, V. Vahidinasab, and S. Soudjani, "Robust simulation functions with disturbance refinement," in *Proc. Eur. Control Conf. (ECC)*, Jun. 2023, pp. 1–6.

[42] K. Mallik, A.-K. Schmuck, S. Soudjani, and R. Majumdar, "Compositional synthesis of finite-state abstractions," *IEEE Trans. Autom. Control*, vol. 64, no. 6, pp. 2629–2636, Jun. 2019.

[43] H. Xin, D. Gan, Z. Qu, and J. Qiu, "Impact of saturation nonlinearities/disturbances on the small-signal stability of power systems: An analytical approach," *Electric Power Syst. Res.*, vol. 78, no. 5, pp. 849–860, May 2008.

[44] S. Prajna, A. Papachristodoulou, and P. A. Parrilo, "Introducing SOSTOOLS: A general purpose sum of squares programming solver," in *Proc. 41st IEEE Conf. Decis. Control*, vol. 1, Aug. 2002, pp. 741–746.

[45] L. de Moura, B. Dutertre, and N. Shankar, "A tutorial on satisfiability modulo theories: (invited tutorial)," in *Proc. Int. Conf. Comput. aided verification*. Cham, Switzerland: Springer, 2007, pp. 20–36.

[46] M. C. Campi and S. Garatti, "Wait-and-judge scenario optimization," *Math. Program.*, vol. 167, no. 1, pp. 155–189, Jan. 2018.

[47] S. Garatti and M. C. Campi, "Risk and complexity in scenario optimization," *Math. Program.*, vol. 191, no. 1, pp. 243–279, Jan. 2022.

[48] A. Benveniste, B. Caillaud, D. Nickovic, R. Passerone, J.-B. Raclet, P. Reinkemeier, A. Sangiovanni-Vincentelli, W. Damm, T. Henzinger, and K. G. Larsen, "Contracts for system design," *Found. Trends Electron. Design Autom.*, vol. 12, nos. 2–3, pp. 124–400, 2018.

[49] A. Saoud, A. Girard, and L. Fribourg, "On the composition of discrete and continuous-time assume-guarantee contracts for invariance," in *Proc. Eur. Control Conf. (ECC)*, Jun. 2018, pp. 435–440.

[50] E. S. Kim, M. Arcak, and S. A. Seshia, "A small gain theorem for parametric assume-guarantee contracts," in *Proc. 20th Int. Conf. Hybrid Syst., Comput. Control*, Apr. 2017, pp. 207–216.

[51] E. S. Kim, S. Sadraddini, C. Belta, M. Arcak, and S. A. Seshia, "Dynamic contracts for distributed temporal logic control of traffic networks," in *Proc. IEEE 56th Annu. Conf. Decis. Control (CDC)*, Dec. 2017, pp. 3640–3645.

[52] S. Oshnoei, A. Oshnoei, A. Mosallanejad, and F. Haghjoo, "Novel load frequency control scheme for an interconnected two-area power system including wind turbine generation and redox flow battery," *Int. J. Electr. Power Energy Syst.*, vol. 130, Sep. 2021, Art. no. 107033.
[53] B. Wooding, "Model-based and data-driven formal synthesis of power systems," Ph.D. dissertation, School Comput., Newcastle Univ., Newcastle Upon Tyne, U.K., 2023.
[54] J. Löfberg, "YALMIP: A toolbox for modeling and optimization in MATLAB," in *Proc. CACSD Conf.*, Taipei, Taiwan, 2004, pp. 284–289.
[55] MOSEK ApS. (2019). *The MOSEK Optimization Toolbox for MATLAB Manual. Version 9.0.* [Online]. Available: http://docs.mosek.com/9.0/toolbox/index.html
[56] M. Rungger and M. Zamani, "SCOTS: A tool for the synthesis of symbolic controllers," in *Proc. 19th Int. Conf. Hybrid Systems: Comput. Control*, Apr. 2016, pp. 99–104.
[57] S. Izadkhast, P. Garcia-Gonzalez, and P. Frías, "An aggregate model of plug-in electric vehicles for primary frequency control," *IEEE Trans. Power Syst.*, vol. 30, no. 3, pp. 1475–1482, May 2015.
[58] C. Mu, W. Liu, and W. Xu, "Hierarchically adaptive frequency control for an EV-integrated smart grid with renewable energy," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 4254–4263, Sep. 2018.
[59] B. Wooding, V. Vahidinasab, M. Kazemi, and S. Soudjani, "Control and management of active buildings," in *Active Building Energy Systems*. Cham, Switzerland: Springer, 2022, pp. 161–192.
[60] B. Wooding, V. Vahidinasab, and S. Soudjani, "Formal controller synthesis for frequency regulation utilising electric vehicles," in *Proc. Int. Conf. Smart Energy Syst. Technol. (SEST)*, Sep. 2020, pp. 1–6.
[61] X. Luo, Y. Kantaros, and M. M. Zavlanos, "An abstraction-free method for multirobot temporal logic optimal control synthesis," *IEEE Trans. Robot.*, vol. 37, no. 5, pp. 1487–1507, Oct. 2021.



BEN WOODING (Member, IEEE) received the integrated M.Comp. degree in computer science (security and resilience) and the Ph.D. degree in formal methods and control from Newcastle University, Newcastle upon Tyne, U.K., in 2019 and 2023, respectively. He is currently a Postdoctoral Researcher with the Institute for Convergent Software Integrated Systems, Vanderbilt University, USA. On completion of his Ph.D., he was awarded an EPSRC Doctoral Prize Fellowship.



SADEGH SOUDJANI (Member, IEEE) is currently a Professor and the Chair in cyber-physical systems with the University of Birmingham, where he directs the CPS Laboratory and serves as the Director of global engagement with the School of Computer Science. He is also a Senior Research Group Leader with the Max Planck Institute for Software Systems, Germany. His research develops formal and data-driven methods for designing and verifying safe, reliable and scalable cyber-physical and autonomous systems operating under uncertainty, with applications in robotics, energy systems, and multi-agent systems. He previously held positions with Newcastle University and the University of Oxford. He has authored more than 180 research publications and led national, international and industry-funded research projects. He has received an ERC Consolidator Grant, in 2023, was a recipient of the EPSRC New Investigator Award, in 2021, and coordinated the EIC Pathfinder Project SymAware.