Robust Simulation Functions with Disturbance Refinement

Ben Wooding, Abolfazl Lavaei, Vahid Vahidinasab and Sadegh Soudjani

***Abstract*— Simulation functions are Lyapunov-like functions defined over the Cartesian product of state spaces of two (un)perturbed systems, *a.k.a., concrete and abstract systems,* to relate output trajectories of abstract systems to those of concrete ones while the mismatch between two systems remains within some guaranteed error bounds. In this work, we approximate concrete systems with abstractions with lower dimensions (reduced-order models) and develop *robust* simulation functions further to consider the perturbation in the abstract system by designing an interface function for the disturbance. The proposed approach allows concrete systems to have large disturbances, which is the case in many real-life applications, while noticeably reducing the closeness error between the two systems. Accordingly, this enables controller design using a reduced-order form of the concrete system and reducing the computational load required for formal synthesis. We demonstrate the efficacy of our approaches by synthesising a formal controller for a 9-state area of the known New England 39 Bus Test System, using only a 3-state abstract system.**

I. Introduction

Motivations and State of the Art. Cyber-physical systems (CPS) are complex networked models combining both cyber (computation and communication) and physical components, which tightly interact with each other in a feedback loop [1]. In the past few years, CPS have gained remarkable attentions as an important modelling tool for engineering systems spanning a wide range of real-life applications such as autonomous vehicles, medical devices and power systems, to name a few. The interconnection of CPS components in the models often results in high-dimensional systems with complex behaviour specifications that are safety critical in nature.

Providing safety and reliability guarantees on the behaviour of these complex systems is therefore essential but also incredibly challenging as formal methods, which can achieve such guarantees, often suffer from the curse of dimensionality and cannot handle high-dimensional models [2]. In particular, formal methods give a strong mathematical framework to provide guarantees over CPS, whether that is verifying the behaviour of a system or synthesising a controller to create (or enforce) system behaviour [3].

To alleviate the encountered computational complexity, symbolic control is one of the promising techniques, proposed in the relevant literature, for formal analysis of CPS [4]. In this regard, symbolic abstractions replace concrete systems to provide a more appropriate medium for formal verification or controller synthesis of CPS. Since the mismatch between outputs of concrete systems and those of their symbolic abstractions are well-quantified, one can guarantee that concrete systems also satisfy the same property of interest as abstract ones with some quantified error bounds.

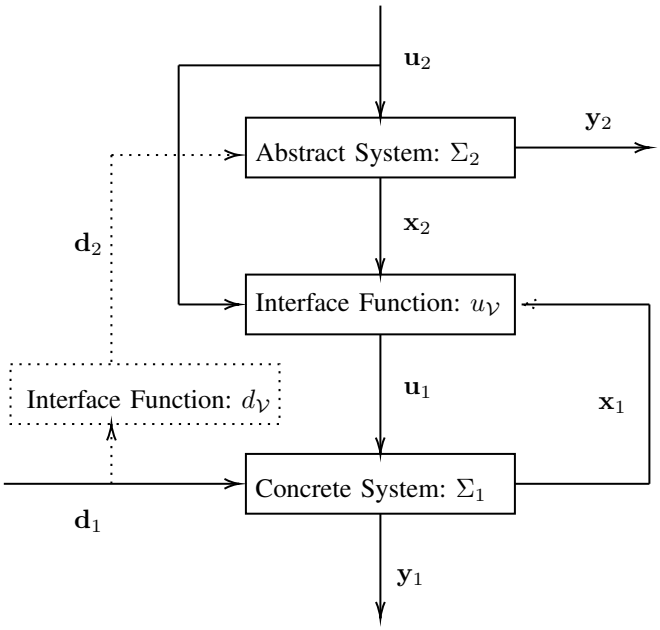

Fig. 1. Hierarchical control system architecture employed in this work. The dashed part considers the need for the disturbance in the low-dimensional abstract system Σ_2 for the sake of control over large measurable disturbances.

In order to relate output trajectories of abstract systems to those of concrete ones, *simulation* and *bisimulation functions* (where both systems can simulate each other) are powerful techniques, proposed in the related literature [4]. If concrete and abstract systems are (bi)similar, one can consider the abstract system as an appropriate substitute in the controller design process with reduced computational loads while still preserving closeness guarantees between the two systems. For underlying systems where expecting the same output may be too strict, *approximate* (bi)simulation functions have been developed in the literature [5], [6].

Approximate (bi)simulation functions aim at establishing a formal relation between the abstract system which is similar to the concrete one, while bounding the closeness between the outputs of two systems by some maximal threshold ϵ, known as the simulation relation error. An interface function is then designed to map the control inputs from the abstract system to the concrete domain enforcing the ϵ-closeness. This notion is extended in [7] to robust simulation functions, which considers small disturbances inside the concrete system, while the abstract system remains unperturbed, to establish an approximate simulation relation between the two systems.

Original Contributions. Our main contribution in this

work is to extend the notion of simulation functions to its robust versions by incorporating the disturbance in the abstract system via designing an interface function for the disturbance, see Fig. 1. This reduces the simulation relation error ϵ, particularly when one is dealing with concrete systems with large disturbances. Incorporating the disturbance in the abstract system enables formal controller synthesis design for the concrete system using the abstract system where ϵ is included in the controller process. Consequently, formal controllers designed on a low-dimensional abstract system can be refined back to control any high-dimensional concrete systems models. We demonstrate the efficacy of our approach on a case study of the New England 39-Bus Test System (NETS).

Related Works. There have been some results, proposed in the past two decades, on establishing (bi)simulation functions for dynamical systems. In this respect, the work [7] extends the approaches of simulation functions to consider small disturbances in the concrete domain providing robustness in the simulation relation. However, for controlling safety-critical CPS, the proposed approach may not be practical given that the simulation relation error increases proportionally to the size of the disturbance. The works [8], [9] demonstrate systems that are approximately equivalent (bisimilar) to their symbolic models. The results in [10] provide an approximation framework that applies to both discrete and continuous systems. The approaches in [11] demonstrate formal control for safety and reachability specifications over complex dynamical systems.

Approximate simulation techniques for switched systems and networks of nonlinear control systems are, respectively, studied in [12], [13] and [14]. The results of [15] employ approximate bisimulations for decentralised supervisory control design, and [16] reduce the number of states in fuzzy automata with approximate bisimulations. The proposed approach in [17] employs approximate bisimulation in transient power systems, which is mainly used for model order reductions: they consider differential-algebraic equations as their model of NETS with bounded disturbances. Reachability and formal analysis of power systems have been studied in [18], [19]. A controller designed based on abstract models for frequency regulation of smart grids is studied in [20]. A data-driven method for constructing the finite abstract model with formal guarantees is proposed in [21].

The rest of the paper is structured as follows. Preliminaries and the formal definition of underlying systems are presented in Section II. Section III contains the solution methodologies while considering the disturbance refinement. We demonstrate our approach over NETS in Section IV and conclude with future directions in Section V.

II. Preliminaries

We employ the following notation throughout the paper. We denote the set of natural numbers, real and non-negative real numbers with, respectively, $\mathbb{N}$, $\mathbb{R}$ and $\mathbb{R}^+$. A function $\gamma : \mathbb{R}^+ \to \mathbb{R}^+$ is a class-κ function if γ is continuous, strictly increasing and $\gamma(0) = 0$. We use $|\cdot|$ for the absolute value, $\|\cdot\|$ for the euclidean norm, and $\|\cdot\|_\infty$ for the infinity norm. Symbol $\mathbb{I}^n$ is the identity matrix in $\mathbb{R}^{n\times n}$ and $a \ll b$ represents a much less than b. All derivatives are taken with respect to time, additionally, notation often omits time for simplicity (*e.g.,* $\mathbf{x}(t) \to \mathbf{x}$).

Class of Systems. We consider two general dynamical systems Σ_1 and Σ_2, modeled as:

$$\Sigma_i : \begin{cases} \dot{\mathbf{x}}_i = f_i(\mathbf{x}_i, \mathbf{u}_i, \mathbf{d}_i), \\ \mathbf{y}_i = g_i(\mathbf{x}_i), \end{cases} \quad i \in \{1, 2\}, \tag{1}$$

where $\mathbf{x}_i \in \mathbb{R}^{n_i}$ are system states, $\mathbf{u}_i \in \mathbb{R}^{p_i}$ are control inputs, $\mathbf{y}_i \in \mathbb{R}^m$ are system outputs, $\mathbf{d}_1 \in \mathbb{R}^q$ is a measurable large disturbance in Σ_1 and $\mathbf{d}_2$ is derived from $\mathbf{d}_1$ with an interface function $d_{\mathcal{V}}$. Without loss of generality, we consider Σ_1 as our original system and Σ_2 as the lower-dimensional abstraction. It can then be taken that $n_2 \leq n_1$.

Linear Temporal Logic Specifications. For the dynamical systems in (1), we consider linear temporal logic (LTL) specifications with syntax [22]

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

where p is the element of an atomic proposition. Let ω be an infinite word, that is, a string composed of letters from the power sets of the atomic proposition, and ω_k be a subsequence (suffix) of ω. Then the satisfaction relation between ω and a property ψ, expressed in LTL, is denoted by $\omega \vDash \psi$. Furthermore, $\omega_k \vDash \neg\psi$ if $\omega_k \nvDash \psi$ and we say that $\omega_k \vDash \psi_1 \wedge \psi_2$ if $\omega_k \vDash \psi_1$ and $\omega_k \vDash \psi_2$. The next operator $\omega_k \vDash \bigcirc\psi$ holds if the property holds at the next time instance. The temporal until operator $\omega_k \vDash \psi_1 \mathsf{U} \psi_2$ holds if $\exists i \in \mathbb{N} : \omega_{k+i} \vDash \psi_2$, and $\forall j \in \mathbb{N} : 0 \leq j < i, \omega_{k+j} \vDash \psi_1$. Disjunction ($\vee$) can be defined by $\omega_k \vDash \psi_1 \vee \psi_2 \;\Leftrightarrow\; \omega_k \vDash \neg(\neg\psi_1 \wedge \neg\psi_2)$. The operator $\omega_k \vDash \Diamond\psi$ is used to denote that the property will eventually happen at some point in the future. The operator $\omega_k \vDash \Box\psi$ signifies that ψ must always be true at all times in the future.

III. Solution Methodologies

The main contribution of our work is to extend the notion of simulation functions to its robust versions by considering disturbance refinement using an interface function for the disturbance in the concrete system to be visible in the abstract domain. Our proposed approach enables the controller synthesis for systems with large disturbances.

In the following section, we show how incorporating the disturbance of the concrete system into the abstract one through the 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 the high-dimensional original system while improving the scalability of the control scheme.

A. Robust Approximate Simulation with Disturbance Refinement

Given the systems in (1), a robust approximate simulation with disturbance refinement is defined with a robust simula-

tion function $\mathcal{V}$ and two interface functions $u_{\mathcal{V}}$ and $d_{\mathcal{V}}$. The function $\mathcal{V}$ has the following Lyapunov-like properties:

Definition 1. *Consider the two systems in* (1)*. Let* $\mathcal{V} : \mathbb{R}^{n_1} \times \mathbb{R}^{n_2} \to \mathbb{R}^+$ *be a differentiable function,* $u_{\mathcal{V}} : \mathbb{R}^{p_2} \times \mathbb{R}^{n_1} \times \mathbb{R}^{n_2} \to \mathbb{R}^{p_1}$ *and* $d_{\mathcal{V}} : \mathbb{R}^{q} \times \mathbb{R}^{n_1} \times \mathbb{R}^{n_2} \to \mathbb{R}^{q}$ *be continuous functions. Then the function* $\mathcal{V}$ *is called a robust simulation function from* Σ_2 *to* Σ_1 *with the associated interface functions* $u_{\mathcal{V}}$ *and* $d_{\mathcal{V}}$ *if there exists class-*κ *functions* γ_1 *and* γ_2 *such that for all* $\mathbf{x}_1 \in \mathbb{R}^{n_1}$ *and* $\mathbf{x}_2 \in \mathbb{R}^{n_2}$*,*

$$\|g_1(\mathbf{x}_1) - g_2(\mathbf{x}_2)\| \leq \mathcal{V}(\mathbf{x}_1, \mathbf{x}_2), \tag{2}$$

and for any $\mathbf{d}_1$ *and* $\mathbf{u}_2$ *satisfying* $\gamma_1(\|\mathbf{d}_1\|) + \gamma_2(\|\mathbf{u}_2\|) \leq \mathcal{V}(\mathbf{x}_1, \mathbf{x}_2)$*,*

$$\frac{\partial \mathcal{V}}{\partial \mathbf{x}_2} f_2(\mathbf{x}_2, \mathbf{u}_2, d_{\mathcal{V}}(\mathbf{d}_1, \mathbf{x}_1, \mathbf{x}_2)) + \frac{\partial \mathcal{V}}{\partial \mathbf{x}_1} f_1(\mathbf{x}_1, u_{\mathcal{V}}(\mathbf{u}_2, \mathbf{x}_1, \mathbf{x}_2), \mathbf{d}_1) \leq 0. \tag{3}$$

We say Σ_1 *robustly approximately simulates* Σ_2 *if there exists a robust simulation function* $\mathcal{V}$ *of* Σ_2 *by* Σ_1*.*

Remark 1. *Definition 1 is a generalisation of the robust approximate simulation notation proposed in the literature [7]. In particular, when* $d_{\mathcal{V}} = 0$*, then the existing robust approximate simulation is recovered.*

In the next subsection, we focus on the class of linear control systems with potentially large measurable disturbances and propose an approach to construct its reduced-dimensional abstractions together with a robust simulation function as presented in Definition 1.

B. Linear Systems under Large Measurable Disturbance

Here, we focus on the class of linear control systems with (potentially large) measurable disturbances, defined as follows:

$$\Sigma_1 : \begin{cases} \dot{\mathbf{x}}_1 = A_1\mathbf{x}_1 + B_1\mathbf{u}_1 + D_1\mathbf{d}_1, \\ \mathbf{y}_1 = C_1\mathbf{x}_1, \end{cases} \tag{4a}$$

$$\Sigma_2 : \begin{cases} \dot{\mathbf{x}}_2 = A_2\mathbf{x}_2 + B_2\mathbf{u}_2 + D_2\mathbf{d}_2, \\ \mathbf{y}_2 = C_2\mathbf{x}_2, \end{cases} \tag{4b}$$

where A_i, B_i, C_i, and D_i are matrices of appropriate dimensions, and $\mathbf{d}_1$ is the measured disturbance having some known bound $\|\mathbf{d}_1\|_\infty \leq d_{\max}$. We now state the main problem that we aim to solve in this paper.

Problem 1. *Given a linear system* Σ_1 *as in* (4a) *under (potentially large) measurable disturbances and an LTL specification* ψ*, construct its reduced-dimensional abstraction* Σ_2 *as in* (4b) *together with robust simulation functions according to Definition 1. Employ the constructed abstraction* Σ_2 *and design a formal controller through robust simulation relations with disturbance refinement such that the specification is satisfied over the original system.*

In order to address Problem 1, we need to raise the following lemma and theorems. Note that the next lemma is similar to the one presented in [5] but it is adapted here to our setting by incorporating the measurable disturbance inside our dynamics.

Lemma 1. *If* Σ_1 *is stabilisable, there are matrices* K_2, P, D_2, Q_1 *such that* $(A_1 + B_1K_2 - PD_2Q_1)$ *is Hurwitz, and there exist a positive definite matrix* M *and positive scalar constant* λ *such that the following matrix inequalities hold:*

$$C_1^T C_1 \leq M, \tag{5a}$$

$$(A_1 + B_1K_2 - PD_2Q_1)^T M + M(A_1 + B_1K_2 - PD_2Q_1) \leq -2\lambda M. \tag{5b}$$

Remark 2. *The matrices* M *and* K_2 *in Lemma 1 can be computed using semi-definite programming by letting* $\bar{K} = K_2M^{-1}$ *and* $\bar{M} = M^{-1}$*. We then gain the equivalent linear matrix inequality conditions:*

$$\begin{bmatrix} \bar{M} & \bar{M}C_1^T \\ C_1\bar{M} & \mathbb{I} \end{bmatrix} \geq 0, \text{ and}$$

$$\bar{M}A_1^T + A_1\bar{M} + \bar{K}^T B_1^T + B_1\bar{K} + \bar{M}Q_1^T D_2^T P^T + PD_2Q_1\bar{M} \leq -2\lambda\bar{M}.$$

Under Lemma 1, we now propose the next theorem to construct the robust simulation function $\mathcal{V}$.

Theorem 1. *Consider two systems of the form* (4)*. Assume that* Σ_1 *is stabilisable, a feedback gain* K_1 *exists for* Σ_2 *and that there exist matrices* P*,* K_2*,* Q_1 *and* Q_2 *such that* $(A_1 + B_1K_2 - PD_2Q_1)$ *is Hurwitz, and the following matrix equalities hold:*

$$A_1P + B_1Q_2 = PA_2 + PD_2Q_1P, \tag{7a}$$

$$C_2 = C_1P. \tag{7b}$$

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 a robust simulation function from Σ_2 *to* Σ_1 *with its associated interfaces*

$$u_{\mathcal{V}} = R_2\mathbf{u}_2 + Q_2\mathbf{x}_2 + K_2(\mathbf{x}_1 - P\mathbf{x}_2), \tag{8a}$$

$$d_{\mathcal{V}} = R_1\mathbf{d}_1 + Q_1\mathbf{x}_1 + K_1(\mathbf{x}_1 - P\mathbf{x}_2). \tag{8b}$$

In addition, the class-κ *functions* γ_1 *and* γ_2 *are designed as*

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

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

where R_1 *and* R_2 *are some arbitrary matrices of appropriate dimensions and* M, λ *are such that* (5) *holds.*

Proof. From (5a) and (7b), we have

$$\mathcal{V}(\mathbf{x}_1, \mathbf{x}_2) \geq \sqrt{(\mathbf{x}_1 - P\mathbf{x}_2)^T C_1^T C_1(\mathbf{x}_1 - P\mathbf{x}_2)} = \|C_1\mathbf{x}_1 - C_2\mathbf{x}_2\|,$$

so condition (2) holds. We proceed to showing condition (3), as well. Using conditions (5b) and (7a), one has

$$\begin{aligned}
&\frac{\partial \mathcal{V}}{\partial \mathbf{x}_2}(A_2\mathbf{x}_2 + B_2\mathbf{u}_2 + D_2 d_{\mathcal{V}}) \\
&\quad + \frac{\partial \mathcal{V}}{\partial \mathbf{x}_1}(A_1\mathbf{x}_1 + B_1 u_{\mathcal{V}} + D_1\mathbf{d_1}) \\
&\leq -\lambda \mathcal{V}(\mathbf{x}_1, \mathbf{x}_2) \\
&\quad + \|\sqrt{M}(D_1 - PD_2R_1)\mathbf{d}_1 + \sqrt{M}(B_1R_2 + PB_2)\mathbf{u}_2\| \\
&\leq -\lambda \mathcal{V}(\mathbf{x}_1, \mathbf{x}_2) + \|\sqrt{M}(D_1 - PD_2R_1)\|\|\mathbf{d}_1\| \\
&\quad + \|\sqrt{M}(B_1R_2 + PB_2)\|\|\mathbf{u}_2\|
\end{aligned}$$

Therefore, for all $\mathbf{d}_1$ and $\mathbf{u}_2$ satisfying

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

we have

$$\begin{aligned}
&\frac{\partial \mathcal{V}}{\partial \mathbf{x}_2}(A_2\mathbf{x}_2 + B_2\mathbf{u}_2 + D_2 d_{\mathcal{V}}) \\
&\quad + \frac{\partial \mathcal{V}}{\partial \mathbf{x}_1}(A_1\mathbf{x}_1 + B_1 u_{\mathcal{V}} + D_1\mathbf{d}_1) \leq 0.
\end{aligned}$$

□

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 a robust simulation function from Σ_2 to Σ_1 with its associated interface function $u_{\mathcal{V}}$. Let $\mathbf{u}_2(t)$ be an admissible input of Σ_2 and $\mathbf{x}_1(t)$ be a state trajectory of Σ_1 satisfying*

$$\dot{\mathbf{x}}_1 = A_1\mathbf{x}_1 + B_1 u_{\mathcal{V}} + D_1\mathbf{d}_1. \tag{11}$$

Then

$$\begin{aligned}
&\|\mathbf{y}_1(t) - \mathbf{y}_2(t)\| \leq \\
&\quad \max\{\mathcal{V}(\mathbf{x}_1(0), \mathbf{x}_2(0)), \gamma_1(\|\mathbf{d}_1\|_\infty) + \gamma_2(\|\mathbf{u}_2\|_\infty)\}.
\end{aligned}$$

Proof. For the sake of an easier presentation, we slightly abuse the notation and denote $\mathcal{V}(\mathbf{x}_1(t), \mathbf{x}_2(t))$ by $\mathcal{V}(t)$. Let

$$\epsilon = \max\{\mathcal{V}(0), \gamma_1(\|\mathbf{d}_1\|_\infty) + \gamma_2(\|\mathbf{u}_2\|_\infty)\}.$$

We show $\mathcal{V}(t) \leq \epsilon$ for all t. As (11) involves a feedback composition, we assume the composition is well-defined and for any initial state there exists a unique solution defined on the interval $t \subseteq \mathbb{R}^+$. Showing $\mathcal{V}(0) \leq \epsilon$ is straightforward due to the definition of ϵ. Assume there exists $\tau > 0$ such that $\mathcal{V}(\tau) > \epsilon$. Then there also exists some $0 \leq \tau' < \tau$ such that $\mathcal{V}(\tau') = \epsilon$ and $\forall t \in (\tau', \tau], \mathcal{V}(t) > \epsilon$. Note that we have, $\forall t \in (\tau', \tau]$,

$$\begin{aligned}
&\gamma_1(\|\mathbf{d}_1\|) + \gamma_2(\|\mathbf{u}_2\|) \leq \\
&\quad \gamma_1(\|\mathbf{d}_1\|_\infty) + \gamma_2(\|\mathbf{u}_2\|_\infty) \leq \epsilon < \mathcal{V}(t).
\end{aligned}$$

From (3), we then have $\frac{\partial \mathcal{V}(t)}{\partial t} \leq 0$ for all $t \in (\tau', \tau]$, which implies

$$\mathcal{V}(\tau) - \mathcal{V}(\tau') = \int_{\tau'}^{\tau} \frac{\partial \mathcal{V}(t)}{\partial t} \partial t \leq 0.$$

This contradicts $\mathcal{V}(\tau) > \epsilon = \mathcal{V}(\tau')$. Therefore, $\mathcal{V}(t) \leq \epsilon, \forall t$. Finally from (2) we have:

$$\mathcal{V}(\mathbf{x}_1(t), \mathbf{x}_2(t)) \leq \epsilon \implies \|\mathbf{y}_1(t) - \mathbf{y}_2(t)\| \leq \epsilon.$$

□

IV. Case Study

To show the efficacy of our proposed approach, we employ a model of the New England 39-Bus Test System (NETS) which is similar in design to the three-control area power system in [23], [24]. NETS has 10 machines, 39 buses and three areas. Here, we consider just one area of this model, containing 9 states with one input and one disturbance. The single line diagram for this system is depicted in Fig. 2. A linear model for Area 1 of NETS is acquired using the Simulink Model Linearizer on the closed-loop system.

We assume that the large disturbance $\mathbf{d}_1$ is measurable in the power system domain as the disturbance may represent changes in the behaviour of generation and load components, e.g., generators, plug-in electric vehicles (EVs) and energy storage systems (ESSs). The generation or load values of these components may be known to operators and the connection and 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 [25] and frequency regulation of smart grids [20].

The dynamics of the model can be presented as a linear system Σ_1 equivalent to (4a) whose matrices can be found in the Appendix. A power loss disturbance of 1 per unit (100 MW, equivalent to a typical generator or 35,000 households) is applied to Σ_1 in all the scenarios of this case study. We construct our abstract system Σ_2 using MATLAB's *balreal* function by truncating the matrices to a reduced-state order of 3. We employ YALMIP [26] and MOSEK [27] for solving LMIs and optimisations in MATLAB on macOS with 8 GB RAM and Intel Core i5 Processor. Simulations are run over a time horizon of 6 seconds, with a time step of 0.005 seconds.

A. System Specification

For this system we consider a specification for primary frequency control. The frequency f can deviate away from its steady state value $f_0 = 50Hz$, this deviation is denoted by $\Delta f = f - f_0$. We bound two regions that the frequency deviation should never transition into; $\mathcal{A}_{ub} = (\mathbf{BW:}0.5, +\infty)$ and $\mathcal{A}_{lb} = (-\infty, -0.35)$. Additionally, whenever there are deviations, it should come back the target range $\mathcal{T} = [-0.3, \mathbf{BW:}0.5]$. Therefore the desired system behaviour can be described by the LTL formula:

$$\psi = \Box(\psi_1 \wedge \psi_2) \text{ with } \psi_1 = \Diamond\mathcal{T}, \psi_2 = \neg(\mathcal{A}_{ub} \vee \mathcal{A}_{lb}). \tag{12}$$

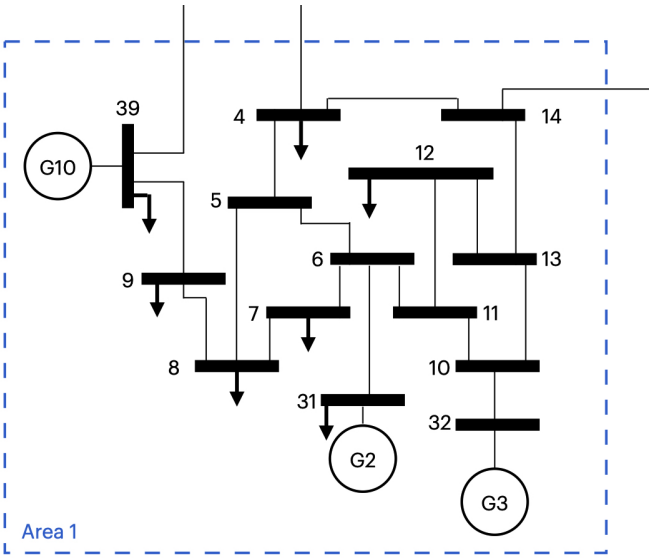

Fig. 2. A single line diagram of Area 1 of the New England 39 Bus Test System.

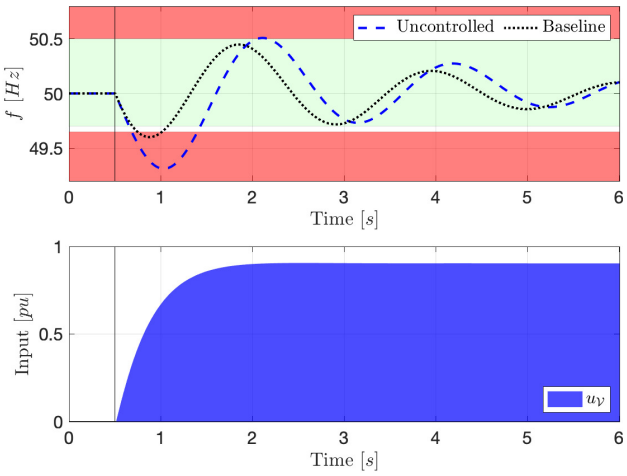

Fig. 3. **Top.** Target range $\mathcal{T}$ is shown in green, $\mathcal{A}_{ub}$ and $\mathcal{A}_{lb}$ are shown in red as two regions that the system should never transition into. The baseline controller notably improves the frequency response of the system in compare with the uncontrolled system. However, both curves still fall into the red unsafe region. **Bottom.** The input $u_\mathcal{Y}$ is a byproduct of the simulation relation interface keeping Σ_1 and Σ_2 ϵ-close. No controller is synthesised over Σ_2, so $\mathbf{u}_2 = 0$.

We modify the specification in (12) appropriately with the error ϵ of the robust simulation function to get a more conservative specification $\hat{\psi}$ on Σ_2. This modification ensures that whenever Σ_2 satisfies $\hat{\psi}$, we get that Σ_1 satisfies ψ by applying the appropriate input and disturbance interface functions for refining the controller. Then, we have the modified specification

$$\hat{\psi} = \Box(\hat{\psi}_1 \wedge \hat{\psi}_2) \text{ with } \hat{\psi}_1 = \Diamond\hat{\mathcal{T}}, \hat{\psi}_2 = \neg(\hat{\mathcal{A}}_{ub} \vee \hat{\mathcal{A}}_{lb}), \quad (13)$$

with $\hat{\mathcal{T}} = [-0.3+\epsilon, \textbf{BW:}0.5-\epsilon]$, $\hat{\mathcal{A}}_{ub} = (\textbf{BW:}0.5-\epsilon, +\infty)$ and $\hat{\mathcal{A}}_{lb} = (-\infty, -0.35+\epsilon)$.

B. Simulation Relation Error

Our primary goal of employing robust simulation functions is to construct an abstract system Σ_2 which is ϵ-close to the concrete system Σ_1, where ϵ remains small enough. Note that in the modified specification (13), any value $\epsilon \geq 0.3$ results in $\hat{\mathcal{T}} = \emptyset$ and the set of controllers enforcing the specification becomes empty. Therefore, our approximation approach must provide error thresholds small enough to give a feasible controller on the abstract system.

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

Abstraction without disturbance refinement. We minimise the error threshold ϵ under the assumption of no disturbance refinement ($D_2 = 0$), $\lambda = 1.7$, $\|\mathbf{u}_2\|_\infty = 0.5$, and $0.01\,\mathbb{I}_9 \leq \bar{M} \leq 120\,\mathbb{I}_9$. This gives the value $\epsilon_{\text{min}} = 3.9156$, which makes the specification $\hat{\psi}$ unsatisfiable.

Abstraction with disturbance refinement. We now use the approach from Theorems 1–2 with the proposed disturbance interface function. We assume λ and the bounds on $\bar{M}$ and $\|\mathbf{u}_2\|_\infty$ are selected as before, $R_1 = 1$, and $Q_1 = K_1 = 0$. We optimise D_2 and B_2 to minimise (9) and (10), respectively. Accordingly, we get the value $\epsilon_{\text{min}} = 0.1019$.

In both cases of the approach with and without disturbance refinement, we construct the same matrices for Σ_2. These matrices can be found in the appendix. The only difference is that $D_2 = 0$ for the case without disturbance refinement.

C. Controller Synthesis Process

Baseline controller. We consider our robust simulation function with the designed abstract system Σ_2 and the interface functions (8) but we put $\mathbf{u}_2 = 0$ 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 the outputs of the two systems within distance ϵ. When the power system frequency moves away from its steady-state value, the input interface function $u_\mathcal{Y}$ generates a control input for Σ_1, which we consider as the *baseline controller*. Fig. 3 shows the frequency response in Σ_1 without EV participation (uncontrolled system with $\mathbf{u}_1 = 0$) against the baseline controller. Although the baseline controller reduces the frequency deviations, it is still unable to satisfy the required specification ψ.

Controller using robust simulation functions. 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 with the guarantee on satisfying ψ. To do so, we consider the tool SCOTS [28] for the synthesis of the symbolic controller using a high-performance computer with 2 nodes and 11 GB memory per core, taking 55 minutes. Note that applying such a symbolic design directly to the 9-dimensional system Σ_1 is

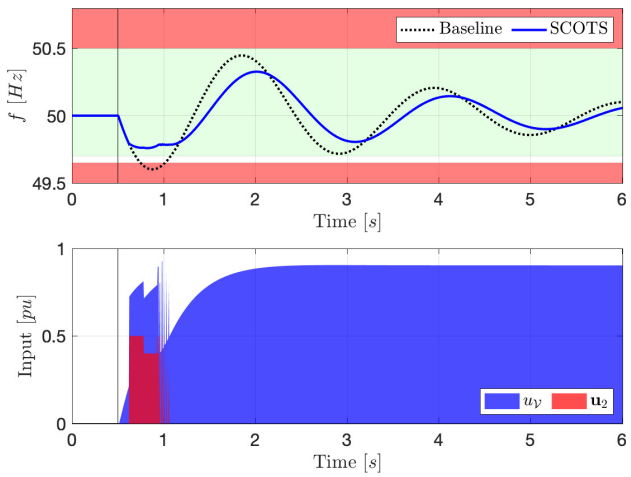

Fig. 4. **Top.** Target range $\mathcal{T}$ is shown in green, unsafe regions $\mathcal{A}_{ub}$ and $\mathcal{A}_{lb}$ are shown in red. The controller designed using SCOTS and the robust simulation function with disturbance refinement successfully satisfy ψ, compared with the baseline controller which violates the specification. **Bottom.** The control input $\mathbf{u}_2$ designed using SCOTS for Σ_2 and the refined control input $\mathbf{u}_1$ for Σ_1 using our robust simulation function.

infeasible due the required exponentially large computational time and memory space.

Fig. 4 compares the baseline controller against the controller designed by combining our robust simulation function with SCOTS. The input $\mathbf{u}_2$ designed by SCOTS is taken as the minimum value that guarantees satisfaction of the specification ψ (to use participation of EVs only if needed). Successful synthesis of the controller over Σ_2 by SCOTS proves formally that ψ holds on Σ_1. Fig. 4 (bottom) shows that over the time interval $t \in [0.5, 1]$, the controller designed on Σ_2 takes non-zero values to bring back the frequency to the intended target region, thus enabling Σ_1 to satisfy ψ.

Overall, we have provided formal guarantees using symbolic control over a 9-dimensional system while only requiring the computational load of a 3-dimensional system. Verifying Theorem 2, we calculate the maximum mismatch between the output trajectories of Σ_1 and Σ_2 from simulations. We acquire 0.6872 for the approach without disturbance refinement and 0.0449 for the approach with disturbance refinement. This confirms our theoretical error bounds ϵ for both cases.

V. Conclusion and Future Direction

In this work, we extended the notion of simulation functions to its robust version by considering large disturbances in the dynamics and introducing an interface function for the disturbance refinement. To do so, we approximated concrete systems with abstractions with lower dimensions (reduced-order models) and developed *robust* simulation functions to consider the perturbation in the abstract system. The proposed approach enables controller design using a reduced-order form of the concrete system and reducing the computational load required for formal synthesis. We illustrated the applicability of our approach by synthesising a formal controller for a 9-state area of the known New England 39-Bus Test System, using only a 3-state abstract system. Future directions could consider all three areas of NETS with assume guarantee conditions used to formally guarantee control across the whole of NETS. Developing a construction scheme for robust simulation functions as proposed in this work but for *nonlinear dynamical systems* is under investigation as a future work.

VI. Acknowledgement

The authors would like to thank Arman Oshnoei for providing the Simulink model of NETS.

References

[1] E. A. Lee, "Cyber physical systems: Design challenges," in *2008 11th IEEE international symposium on object and component-oriented real-time distributed computing (ISORC)*. IEEE, 2008, pp. 363–369.

[2] K. Hsu, R. Majumdar, K. Mallik, and A.-K. Schmuck, "Multi-layered abstraction-based controller synthesis for continuous-time systems," in *Proceedings of the 21st International Conference on Hybrid Systems: Computation and Control (part of CPS Week)*, 2018, pp. 120–129.

[3] A. Pnueli, "The temporal logic of programs," in *18th Annual Symposium on Foundations of Computer Science (sfcs 1977)*, 1977, pp. 46–57.

[4] P. Tabuada, *Verification and control of hybrid systems: a symbolic approach*. Springer Science & Business Media, 2009.

[5] A. Girard and G. J. Pappas, "Approximate bisimulation relations for constrained linear systems," *Automatica*, vol. 43, no. 8, pp. 1307–1317, 2007.

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

[7] V. Kurtz, P. M. Wensing, and H. Lin, "Robust approximate simulation for hierarchical control of linear systems under disturbances," in *2020 American Control Conference (ACC)*. IEEE, 2020, pp. 5352–5357.

[8] G. Pola, A. Girard, and P. Tabuada, "Approximately bisimilar symbolic models for nonlinear control systems," *Automatica*, vol. 44, no. 10, pp. 2508–2516, 2008.

[9] A. Girard, G. Pola, and P. Tabuada, "Approximately bisimilar symbolic models for incrementally stable switched systems," *IEEE Transactions on Automatic Control*, vol. 55, no. 1, p. 116 – 126, 2010.

[10] A. Girard and G. J. Pappas, "Approximate bisimulation: A bridge between computer science and control theory," *European Journal of Control*, vol. 17, no. 5-6, pp. 568–578, 2011.

[11] A. Girard, "Controller synthesis for safety and reachability via approximate bisimulation," *Automatica*, vol. 48, no. 5, pp. 947–953, 2012.

[12] A. Saoud and A. Girard, "Optimal multirate sampling in symbolic models for incrementally stable switched systems," *Automatica*, vol. 98, pp. 58–65, 2018.

[13] W. Xiang, H.-D. Tran, and T. T. Johnson, "Output reachable set estimation for switched linear systems and its application in safety verification," *IEEE Transactions on Automatic Control*, vol. 62, no. 10, pp. 5380–5387, 2017.

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

[15] G. Pola, P. Pepe, and M. D. D. Benedetto, "Decentralized supervisory control of networks of nonlinear control systems," *IEEE Transactions on Automatic Control*, vol. 63, no. 9, pp. 2803–2817, 2018.

[16] C. Yang and Y. Li, "Approximate bisimulations and state reduction of fuzzy automata under fuzzy similarity measures," *Fuzzy Sets and Systems*, vol. 391, pp. 72–95, 2020.

[17] A. M. Stanković, S. D. Đukić, and A. T. Sarić, "Approximate bisimulation-based reduction of power system dynamic models," *IEEE Transactions on Power Systems*, vol. 30, no. 3, pp. 1252–1260, 2015.

[18] M. Althoff and B. H. Krogh, "Reachability analysis of nonlinear differential-algebraic systems," *IEEE Transactions on Automatic Control*, vol. 59, no. 2, pp. 371–383, 2014.

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

[20] B. Wooding, V. Vahidinasab, and S. Soudjani, "Formal controller synthesis for frequency regulation utilising electric vehicles," in *2020 International Conference on Smart Energy Systems and Technologies (SEST)*. IEEE, 2020, pp. 1–6.

[21] M. Kazemi, R. Majumdar, M. Salamati, S. Soudjani, and B. Wooding, "Data-driven abstraction-based control synthesis," *arXiv preprint arXiv:2206.08069*, 2022.

[22] C. Baier and J.-P. Katoen, *Principles of model checking*. MIT press, 2008.

[23] P. Babahajiani, Q. Shafiee, and H. Bevrani, "Intelligent demand response contribution in frequency control of multi-area power systems," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 1282–1291, 2018.

[24] 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," *International Journal of Electrical Power & Energy Systems*, vol. 130, p. 107033, 2021.

[25] S. Soudjani and A. Abate, "Aggregation and control of populations of thermostatically controlled loads by formal abstractions," *IEEE Trans. on Control Systems Technology*, vol. 23, no. 3, pp. 975–990, 2015.

[26] J. Löfberg, "YALMIP : A Toolbox for Modeling and Optimization in MATLAB," in *In Proceedings of the CACSD Conference*, Taipei, Taiwan, 2004.

[27] MOSEK ApS, *The MOSEK optimization toolbox for MATLAB manual. Version 9.0.*, 2019. [Online]. Available: http://docs.mosek.com/9.0/toolbox/index.html

[28] M. Rungger and M. Zamani, "SCOTS: A tool for the synthesis of symbolic controllers," in *HSCC*. ACM, 2016, p. 99–104.

APPENDIX

The matrices of the NETS single area Σ_1 are given as:

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

$$B_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}^T$$

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

$$C_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 2.05 & 0 & 0 & 0 & 0 \end{bmatrix}$$

The reduced-order model Σ_2 is constructed as:

$$A_2 = \begin{bmatrix} -0.6333 & 3.0028 & 0.4428 \\ -3.0028 & -0.0026 & -0.0263 \\ -0.4428 & -0.0263 & -1.5159 \end{bmatrix}$$

$$B_2 = \begin{bmatrix} -0.8580 & 0.5378 & 0.6956 \end{bmatrix}^T$$

$$D_2 = \begin{bmatrix} 0.8580 & -0.5378 & -0.6956 \end{bmatrix}^T$$

$$C_2 = \begin{bmatrix} -1.7990 & 0.1141 & 0.5998 \end{bmatrix}$$

Note that we have $D_2 = 0$ for the method without the disturbance refinement. The matrices obtained for establishing our robust simulation relation are as follows:

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

$$P = \begin{bmatrix} 0.04 & 0.03 & 0.03 & 0.02 & -0.88 & 0.025 & 0.044 & 0.03 & 0.66 \\ -0.01 & -0.01 & -0.01 & 0.29 & 0.06 & -0.10 & -0.98 & -0.99 & 0.36 \\ -0.03 & -0.18 & -0.018 & -0.18 & 0.29 & -0.33 & -0.25 & -0.31 & 0.52 \end{bmatrix}^T$$

$$Q_1 = K_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

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

$$Q_2 = \begin{bmatrix} 0.0238 & -0.0407 & 0.3401 \end{bmatrix}$$

$$R_1 = R_2 = 1.$$

SS: After finishing this paper, I would like you to look into documents on primary and secondary frequency response, to have a section of specifications required the frequency to satisfy. The current specification is very simple, reach-avoid and safety.