SAFE CONTROL OF SEMI-EXPLICIT DIFFERENTIAL-ALGEBRAIC SYSTEMS: CONTROL BARRIER FUNCTIONS WITH SOS VERIFICATION

Mohamad H. Kazma[1], Hongchao Zhang[2], Abdallah A. Albustami[1], Ben Wooding[2], Meiyi Ma[2], Taylor T. Johnson[2] and Ahmad F. Taha[1]

***Abstract*—Differential-algebraic equation (DAE) systems arise in power networks, multibody mechanics, and chemical processes, where algebraic constraints couple dynamic and algebraic states. Standard control barrier function (CBF) methods, designed for ordinary differential equations, fail for DAE systems because the algebraic constraints impose compatibility requirements that may render safety filters infeasible. This paper develops a safety-critical control framework for semi-explicit DAE systems using CBFs that consider compatibility with the algebraic constraints, termed DAE-aware CBFs. We construct projected vector fields on the constraint manifold to account for the hidden dynamics, while ensuring compatibility conditions that keep the algebraic constraints satisfied. We then present sum of squares (SOS) verification conditions that certify both correctness and feasibility of the resulting DAE-aware CBF. The framework is validated on power system case studies.**

I. INTRODUCTION

SAFETY of dynamical systems can be formulated as the positive invariance of a safe set [1]; it requires all trajectories starting within a prescribed region to remain there for all time. For systems modeled by ordinary differential equations (ODEs), *control barrier functions* (CBFs) are considered a computationally efficient tool for realtime safe control [2], [3]. CBFs synthesize safety filters that minimally modify a nominal control input to guarantee safety. A myriad of studies have extended CBFs to high-order systems [4], neural network representations [5], systems evolving on manifolds [6], and partially feedback linearizable systems [7].

While ODE models are common, many engineering systems are described by *differential-algebraic equations* (DAEs) [8] that couple dynamic and algebraic states through algebraic constraints. Algebraic constraints arise from physical conservation laws (such as conservation of mass, energy, and power balance) that must be satisfied at all times, and they restrict the allowable state trajectories to a constraint manifold. For DAEs, standard CBF methods are not directly applicable since the safety filter may demand an input that violates the algebraic constraints, rendering the filter infeasible; see Fig. 1. Safety based on CBFs assumes the existence of a feasible control input satisfying the barrier condition,

The authors are affiliated with the [1]Department of Civil and Environmental Engineering, and [2]Institute for Convergent Software Integrated Systems at Vanderbilt University, Nashville, TN, USA. This work is partially supported by the National Science Foundation (NSF), United States, under grants 2220401, 2152450, and 2550934, and by the Defense Advanced Research Projects Agency (DARPA) under contract number FA8750-23-C-0518. Any opinions, findings, and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of DARPA or NSF. {mohamad.h.kazma, hongchao.zhang, abdallah.b.alalem.albustami, ben.wooding, meiyi.ma, taylor.johnson, ahmad.taha}@vanderbilt.edu

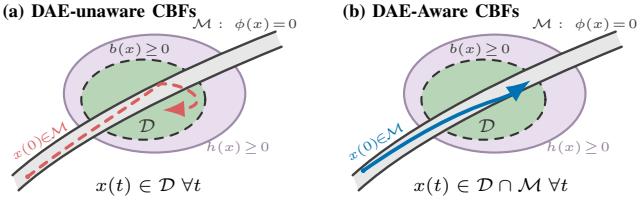

Fig. 1. (a) A standard CBF safety filter applied to a DAE system may produce an input whose resulting velocity is not tangent to the constraint manifold $\mathcal{M}$, rendering the trajectory infeasible. (b) The proposed DAE-aware CBF produces an input that ensures $x(t) \in \mathcal{D} \cap \mathcal{M}\ \forall t \geq 0$.

that can be violated when the algebraic constraint manifold $\mathcal{M} = \{x : \phi(x) = 0\}$ imposes compatibility requirements that standard CBF conditions do not account for.

In this paper, we focus on safety-critical control and verification for power system models that admit a regular semi-explicit DAE representation. Regularity ensures that the algebraic states are uniquely determined by the dynamic states, a standard condition in power system DAEs [9].

Related Work. Existing approaches for DAE safety verification include reachability analysis based on zonotopes [10], Hamilton-Jacobi level set methods [11], and hybrid systems reachability techniques [12]. In power systems, compositional reachability methods have been applied to transient stability analysis [13] and reachability analysis has been used to characterize microgrid dynamics under large disturbances [14], while barrier certificates via SOS programming have been used for voltage constraint verification [15] and distributed safe operation of inverter-based microgrids [16]. These methods provide offline verification or certification, yet do not construct realtime safety filters. On the control synthesis side, DAE stabilization methods based on polynomial Lyapunov functions [17], dissipativity conditions [18], and LMI-based rational control [19] target asymptotic stability rather than strict set invariance. CBFs have been applied to microgrid voltage regulation [20]; however, this formulation does not account for algebraic constraints arising from DAE structure. Recently, CBFs for DAEs have been introduced in [21] for flexible link manipulators; however, that work does not explicitly derive how control inputs can ensure algebraic constraint manifold invariance or present a method to verify candidate CBFs. A general framework for DAE-aware CBFs that addresses both safety filter design and formal verification remains an open problem.

Paper Contributions. This paper introduces a safety-critical control framework for semi-explicit DAE systems by considering DAE-aware CBFs. We address two fundamental challenges. *(i)* We ensure that the control input maintains

invariance of the constraint manifold while enforcing safe set invariance; and *(ii)* we formally verify that the resulting safety filter is both correct and feasible. The contributions are as follows.

- We construct projected vector fields on the constraint manifold that encode the hidden coupling between dynamic and algebraic states. Under this representation, we derive DAE-aware CBF conditions that simultaneously enforce set invariance and manifold compatibility on $\mathcal{M}$; these conditions are then extended to high-order CBFs for barrier functions of arbitrary relative degree.
- We develop SOS-based verification conditions for the resulting CBF that establish correctness (the barrier set lies within the safe set on the manifold) and feasibility (the compatible control input exists and satisfies the safety and algebraic constraints). Both conditions reduce to semidefinite programs.

The work herein considers power system models represented as semi-explicit DAE systems, coupling generator dynamics with algebraic power flow constraints. The extended version [22] generalizes the framework to higher-index DAEs, develops neural network CBF synthesis with SMT-based verification, and presents mechanical system benchmarks. The present paper, however, focuses on a power system case study and introduces an autonomous forward invariance result not covered in [22].

Notation. The boundary and interior of a set $\mathcal{S}$ are denoted $\partial\mathcal{S}$ and $\mathrm{int}(\mathcal{S})$, respectively. A continuous function $\alpha : \mathbb{R} \to \mathbb{R}$ is *class-*$\mathcal{K}_\infty$ if $\alpha(0) = 0$, α is strictly increasing, and $\alpha(r) \to \infty$ as $r \to \infty$. The gradient of a smooth function $y : \mathbb{R}^n \to \mathbb{R}$ is denoted $\nabla y(x) \in \mathbb{R}^n$, and $\nabla_{x_i} y(x)$ denotes the partial gradient with respect to x_i. For a smooth vector field $f : \mathbb{R}^n \to \mathbb{R}^n$, the Lie derivative of y along f is $\mathcal{L}_f y(x) := \nabla y(x)^\top f(x)$, with higher-order Lie derivatives $\mathcal{L}_f^k y := \mathcal{L}_f(\mathcal{L}_f^{k-1} y)$ and $\mathcal{L}_f^0 y := y$.

Paper Organization. Section II provides the required preliminaries and presents the problem formulation. Section III introduces DAE-aware CBFs and derives safety conditions for semi-explicit DAE systems. Section IV introduces the SOS-based verification method. Section V presents power system case studies. The paper is concluded in Section VI.

II. Preliminaries and Problem Formulation

A. System Model

We consider a nonlinear control affine semi-explicit DAE system in continuous-time given as follows.

$$\dot{x}_d(t) = f_d(x(t)) + g_d(x(t))\, u(t), \tag{1a}$$

$$0 = \phi(x(t)), \tag{1b}$$

where $x_d(t) \in \mathbb{R}^{n_d}$ denotes the dynamic states, $x_a(t) \in \mathbb{R}^{n_a}$ denotes the algebraic states, $x(t) = [x_d(t)^\top, x_a(t)^\top]^\top \in \mathbb{R}^{n_x}$ is the full state with $n_x = n_d + n_a$, and $u(t) \in \mathcal{U} \subseteq \mathbb{R}^{n_u}$ is the control input, where $\mathcal{U}$ denotes the admissible input set. The smooth maps $f_d : \mathbb{R}^{n_x} \to \mathbb{R}^{n_d}$ and $g_d : \mathbb{R}^{n_x} \to \mathbb{R}^{n_d \times n_u}$ are the drift and input fields, and $\phi : \mathbb{R}^{n_x} \to \mathbb{R}^{n_m}$ is the algebraic constraint map. The constraint $\phi(x) = 0$ restricts all trajectories to the *constraint manifold* $\mathcal{M} := \{x \in \mathbb{R}^{n_x} : \phi(x) = 0\}$. We note that $\phi(x)$ is not directly controlled, that is, ϕ does not depend on u. This is the case in power system DAEs, where algebraic power flow balance equations couple with control inputs acting on the generator dynamics. The following definition is essential for characterizing the DAE structure.

Definition 1 (Differentiation index [8])**.** *The differentiation index ν of* (1) *is the minimum number of differentiations of the algebraic constraint required to obtain an explicit ODE via algebraic manipulations.*

Throughout this paper, we consider index-1 systems (1), for which a single differentiation of $\phi(x) = 0$ suffices to determine $\dot{x}_a$. Differentiating (1b) requires the evaluation of the Jacobians of ϕ with respect to the dynamic x_d and algebraic x_a states, defined as follows.

$$J_d(x) := \nabla_{x_d} \phi(x), \qquad J_a(x) := \nabla_{x_a} \phi(x). \tag{2}$$

Assumption 1 (Regularity)**.** *For all $x \in \mathcal{C} \cap \mathcal{M}$, the algebraic Jacobian $J_a(x) \in \mathbb{R}^{n_m \times n_a}$ is square and nonsingular, i.e., $n_m = n_a$ and $\det(J_a(x)) \neq 0$.*

Assumption 1 is the standard regularity condition for index-1 DAEs [8], [9]; it guarantees that, given $\dot{x}_d$, the algebraic state derivative $\dot{x}_a$ is uniquely determined. We note that the assumption is a mild condition and is satisfied by semi-explicit power system DAE models [9].

B. Safety and Control Barrier Functions

Safety of dynamical systems refers to the property that the system state remains within a prescribed set for all time. Let $h : \mathbb{R}^{n_x} \to \mathbb{R}$ define the safe set $\mathcal{C} := \{x \in \mathbb{R}^{n_x} : h(x) \geq 0\}$.

Definition 2 (Safety)**.** *A set $\mathcal{C} \subseteq \mathbb{R}^{n_x}$ is* positively invariant *under* (1) *and policy μ if $x(0) \in \mathcal{C}$ and $u(t) = \mu(x(t))$ for all $t \geq 0$ implies $x(t) \in \mathcal{C}$ for all $t \geq 0$.*

For ODE systems ($\phi(x) \equiv 0$), a CBF $b : \mathbb{R}^{n_x} \to \mathbb{R}$ defines the barrier set $\mathcal{D} := \{x \in \mathbb{R}^{n_x} : b(x) \geq 0\} \subseteq \mathcal{C}$. The following result guarantees positive invariance of $\mathcal{D}$ under appropriate control.

Theorem 1 ([3])**.** *Suppose $b(x)$ is a CBF with $b(x(0)) \geq 0$ and the input $u(t)$ satisfies*

$$\mathcal{L}_f b(x) + \mathcal{L}_g b(x)\, u \geq -\alpha\big(b(x)\big), \tag{3}$$

for all $t \geq 0$, where $f := f_d$ and $g := g_d$. Then $\mathcal{D}$ is positively invariant.

In practice, the input is obtained by solving a CBF-QP that minimally modifies a nominal controller u_{nom} subject to (3)

$$\min_{u \in \mathcal{U}} \ \|u - u_{\mathrm{nom}}\|^2 \quad \text{s.t.} \quad (3). \tag{4}$$

Theorem 1 assumes the existence of a control input satisfying (3). A CBF $b(x)$ is *valid* if *(i)* $\mathcal{D} \subseteq \mathcal{C}$ (correctness); and *(ii)* for every $x \in \mathcal{D}$, there exists $u \in \mathcal{U}$ satisfying (3) (feasibility). Correctness ensures that the barrier set is contained within the safe set, while feasibility guarantees that the CBF-QP (4) admits a solution at every state.

C. Problem Formulation

For DAE systems (1), trajectories are restricted to $\mathcal{M}$, thus safety must be enforced on $\mathcal{D} \cap \mathcal{M}$ rather than $\mathcal{D}$ alone. Directly applying (3) to a DAE introduces two challenges: *(i)* a control input satisfying the barrier inequality may violate

$\phi(x) = 0$, since the Lie derivatives do not account for the coupling between x_d and x_a imposed by (1b); and *(ii)* verifying that a compatible, safe input exists at every state in $\mathcal{D} \cap \mathcal{M}$ requires certifying feasibility of the barrier condition subject to the algebraic constraints. Without accounting for these, the CBF-QP (4) may produce an input that is incompatible with $\mathcal{M}$ (Fig. 1), rendering it infeasible. To overcome these challenges, we solve the following problem.

Problem 1. *Given a semi-explicit DAE* (1) *satisfying Assumption 1, a safe set $\mathcal{C}$, and a candidate barrier function $b(x)$: (i) design a control policy $\mu : \mathbb{R}^{n_x} \to \mathbb{R}^{n_u}$ such that $\mathcal{D} \cap \mathcal{M}$ is positively invariant for all $x(0) \in \mathcal{D} \cap \mathcal{M}$; and (ii) verify that the resulting safety filter is both correct ($\mathcal{D} \cap \mathcal{M} \subseteq \mathcal{C} \cap \mathcal{M}$) and feasible (a compatible, safe input exists at every state).*

To address the above problem, we construct projected vector fields on $\mathcal{M}$ and derive CBF conditions that jointly enforce manifold compatibility and set invariance (Section III). Then we develop SOS-based verification methods to certify correctness and feasibility of the resulting CBFs (Section IV); see Fig. 2 for an overview.

III. DAE-Aware CBFs for Semi-Explicit DAEs

This section presents the main theoretical results: *(i)* projected vector fields that reveal hidden constraints imposed by the algebraic equations; *(ii)* a CBF condition that enforces safety on the constraint manifold; and *(iii)* a high-order extension for barrier functions with arbitrary relative degree.

A. Projected Vector Fields and DAE-Aware CBFs

For any feasible trajectory of (1), the algebraic constraints must hold for all time, that is, $\phi(x(t)) = 0$ for all $t \geq 0$. Differentiating with respect to time and substituting $\dot{x}_d = f_d(x) + g_d(x)u$ yields the *compatibility condition*

$$J_d(x)\big(f_d(x) + g_d(x)u\big) + J_a(x)\dot{x}_a = 0. \tag{5}$$

Under Assumption 1, $J_a(x)$ is nonsingular and (5) admits the unique solution

$$\dot{x}_a(x,u) = -J_a(x)^\dagger J_d(x)\big(f_d(x) + g_d(x)u\big), \tag{6}$$

where $J_a(x)^\dagger$ denotes the Moore-Penrose pseudoinverse. For regular semi-explicit DAEs with $n_m = n_a$, $J_a(x)$ is square and invertible under Assumption 1, thus $J_a(x)^\dagger = J_a(x)^{-1}$. Now, augmenting the differential dynamics with (6) gives the *projected vector fields*

$$\hat{f}(x) := \begin{bmatrix} f_d(x) \\ -J_a^\dagger J_d f_d \end{bmatrix}, \quad \hat{g}(x) := \begin{bmatrix} g_d(x) \\ -J_a^\dagger J_d g_d \end{bmatrix}, \tag{7}$$

where the argument (x) is suppressed for brevity. Since $\nabla\phi = [J_d \;\; J_a]$, expanding gives $\nabla\phi\,\hat{f} = J_d f_d - J_a J_a^\dagger J_d f_d$; under Assumption 1, J_a has full row rank so $J_a J_a^\dagger = I_{n_a}$, yielding $\nabla\phi(x)\hat{f}(x) = 0$ and, similarly, $\nabla\phi(x)\hat{g}(x) = 0$. Thus, any trajectory of $\dot{x} = \hat{f}(x) + \hat{g}(x)u$ starting on $\mathcal{M}$ remains on $\mathcal{M}$.

Based on the above, we define the Lie derivatives along the projected fields as $\mathcal{L}_{\hat{f}} b(x) := \nabla b(x)^\top \hat{f}(x)$ and $\mathcal{L}_{\hat{g}} b(x) := \nabla b(x)^\top \hat{g}(x)$, and introduce the *projection operator*

$$P(x) := I_{n_m} - J_a(x) J_a(x)^\dagger. \tag{8}$$

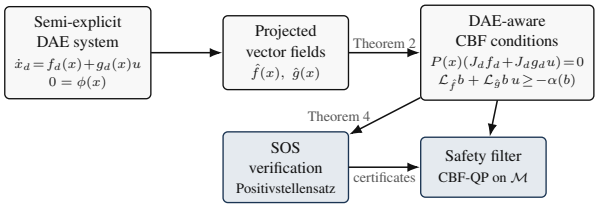

Fig. 2. Overview of the proposed framework. Projected vector fields (7) capture the coupling between dynamic and algebraic states on $\mathcal{M}$. The DAE-aware CBF condition (Theorem 2) and its high-order extension enforce safety on the constraint manifold, while SOS verification (Theorem 4) certifies correctness and feasibility of the resulting safety filter.

Thus, the compatibility condition (5) can be equivalently written as $P(x)\big(J_d(x)f_d(x) + J_d(x)g_d(x)u\big) = 0$.

Remark 1. *For regular index-1 DAEs with $n_m = n_a$, $J_a(x)$ is square and invertible on $\mathcal{C} \cap \mathcal{M}$, so $J_a(x)^\dagger = J_a(x)^{-1}$ and $P(x) = I_{n_m} - J_a J_a^{-1} = 0$. The compatibility condition then drops from the DAE-aware CBF-QP. However, the CBF inequality itself* still *uses the projected fields $(\hat{f}, \hat{g})$ from* (7)*, which differ from the original (f, g). For* (7)*, the lower blocks $-J_a^{-1}J_d f_d$ and $-J_a^{-1}J_d g_d$ encode how the algebraic states respond to the differential dynamics. A naive CBF evaluated along (f, g) ignores this coupling and can drive trajectories off $\mathcal{M}$. The consistency with algebraic constraints, thus, is enforced by both the projected fields* (7) *and the compatibility constraint* (5).

Under Assumption 1 and Remark 1, the projected dynamics $\dot{x} = \hat{f}(x) + \hat{g}(x)u$ are well-defined and locally Lipschitz on $\mathcal{C} \cap \mathcal{M}$, ensuring that standard ODE existence and uniqueness results apply to the system on $\mathcal{M}$. The following theorem provides sufficient conditions for the positive invariance of $\mathcal{D} \cap \mathcal{M}$ under the projected dynamics.

Theorem 2 (Safety of semi-explicit DAEs)**.** *Consider the semi-explicit DAE* (1) *with $\nu = 1$ satisfying Assumption 1. Suppose $b(x(0)) \geq 0$ and $x(0) \in \mathcal{D} \cap \mathcal{M}$. The set $\mathcal{D} \cap \mathcal{M}$ is positively invariant if the input $u(t)$ satisfies, for all $x \in \mathcal{D} \cap \mathcal{M}$,*

$$P(x)\big(J_d(x)f_d(x) + J_d(x)g_d(x)u\big) = 0, \tag{9a}$$

$$\mathcal{L}_{\hat{f}} b(x) + \mathcal{L}_{\hat{g}} b(x)u \geq -\alpha(b(x)). \tag{9b}$$

Proof. Since ϕ does not depend on the control input, differentiating $\phi(x(t)) = 0$ and substituting $\dot{x}_d = f_d(x) + g_d(x)u$ yields the compatibility condition (5). Thus, condition (9a) is equivalent to (5). Now, for $\nu = 1$, $J_a(x)$ is nonsingular on $\mathcal{C} \cap \mathcal{M}$ (Assumption 1), thus $\dot{x}_a$ is uniquely determined by (6) and the projected fields (7) are well-defined with $\nabla\phi(x)\hat{f}(x) = 0$ and $\nabla\phi(x)\hat{g}(x) = 0$. Hence any trajectory of $\dot{x} = \hat{f}(x) + \hat{g}(x)u$ starting on $\mathcal{M}$ remains on $\mathcal{M}$, and differentiating b along the projected dynamics gives $\dot{b}(x(t)) = \mathcal{L}_{\hat{f}} b(x) + \mathcal{L}_{\hat{g}} b(x)u$. Thus, (9b) yields $\dot{b} \geq -\alpha(b)$, where for $\alpha \in \mathcal{K}_\infty$ with $\alpha(0) = 0$ and $b(x(0)) \geq 0$, the comparison lemma [23, Lemma 3.4] gives $b(x(t)) \geq 0$ for all $t \geq 0$. Based on that, any trajectory starting in $\mathcal{D} \cap \mathcal{M}$ remains in $\mathcal{D} \cap \mathcal{M}$. □

Theorem 2 establishes that condition (9b) is exactly (3) with (f, g) replaced by $(\hat{f}, \hat{g})$, while condition (9a) ensures trajectories remain on $\mathcal{M}$. We note that the Lie derivatives $\mathcal{L}_{\hat{f}} b$ and $\mathcal{L}_{\hat{g}} b$ account for the response of the algebraic

states through the projected fields (7); evaluating the CBF condition along the original (f_d, g_d) ignores this coupling and can produce inputs that violate the algebraic constraints. The following corollary is a special case of Theorem 2 for autonomous DAEs. The compatibility condition reduces to a constraint on the drift field f_d.

Corollary 1 (Autonomous DAEs)**.** *Consider the DAE system* (1) *satisfying Assumption 1, with* $g_d(x) \equiv 0$ *(no control input). Suppose* $b(x(0)) \geq 0$ *and* $x(0) \in \mathcal{D} \cap \mathcal{M}$*. Then* $\mathcal{D} \cap \mathcal{M}$ *is positively invariant if, for all* $x \in \mathcal{D} \cap \mathcal{M}$*,*

$$P(x) J_d(x) f_d(x) = 0, \tag{10a}$$

$$\mathcal{L}_{\hat{f}} b(x) \geq -\alpha(b(x)). \tag{10b}$$

Proof. Set $u \equiv 0$ in (9). Condition (9a) reduces to (10a), and condition (9b) reduces to (10b). The proof then follows directly from Theorem 2. □

Corollary 1 is applicable to power system DAEs operating under fixed generation dispatch [15], where no control input is available and safety must be certified from the drift dynamics alone; see Section V. Furthermore, in cases where a control input is present however the barrier function $b(x)$ has relative degree greater than one with respect to the projected dynamics, the conditions of Theorem 2 do not directly apply. The following subsection extends the framework to account for the relative degree of $b(x)$.

B. Relative Degree and High-Order CBFs

The projected dynamics (7) may require more than one differentiation of $b(x)$ before the control input appears. To formalize this, we recall the notion of relative degree.

Definition 3 (Relative degree [24])**.** *The* relative degree *of a smooth function* $b(x)$ *with respect to a control affine system* $\dot{x} = f(x) + g(x)u$ *is* $d \geq 1$ *if* d *is the smallest integer such that (i)* $\mathcal{L}_g \mathcal{L}_f^k b(x) = 0$ *for all* $k < d - 1$*; and (ii)* $\mathcal{L}_g \mathcal{L}_f^{d-1} b(x) \neq 0$*.*

Note that Theorem 1 is considered when $b(x)$ has relative degree one, where u appears directly in $\dot{b}(x)$. For the projected dynamics on $\mathcal{M}$, the relative degree of $b(x)$ is determined by the structure of $\hat{g}$ in (7). That is, the control enters through the lower block $-J_a^\dagger J_d g_d$, and this propagation can increase the effective relative degree beyond what would be observed in the unconstrained ODE. The following lemma formalizes this relationship for semi-explicit DAE systems.

Lemma 1 (Index and relative degree)**.** *Consider the DAE system* (1) *satisfying Assumption 1. Let* d' *denote the smallest integer such that* $J_d(x) \mathcal{L}_{g_d} \mathcal{L}_{f_d}^{d'-1} x_d(x) \neq 0$*. Then, the relative degree,* d*, of the algebraic constraint* $\phi(x)$ *with respect to system* (1) *satisfies* $d = \nu + d' - 1$*. For index-1 systems* ($\nu = 1$)*, we have* $d = d'$*.*

Proof. For a single differentiation of $\phi(x(t)) = 0$, the compatibility condition (5) yields $J_d(x)\dot{x}_d + J_a(x)\dot{x}_a = 0$. Since $\nu = 1$, $J_a(x)$ is invertible and $\dot{x}_a$ is determined by $\dot{x}_d$. The control u appears in the ν-th derivative of ϕ through $J_d(x)$; for u to have a nonzero coefficient, d' additional derivatives of x_d through $J_d(x)$ are required (Definition 3). Hence $d = \nu + d' - 1$, and for $\nu = 1$, $d = d'$. □

Lemma 1 reveals that even for index-1 DAEs, the actuation structure of the differential subsystem can produce $d' > 1$, requiring a high-order CBF (HOCBF). When $d' = 1$ (i.e., $J_d(x) g_d(x) \neq 0$), the standard CBF condition of Theorem 2 suffices. When $d' > 1$, the control input does not appear in the first $d - 1$ time derivatives of $b(x)$ along $\mathcal{M}$, and the following extension of Theorem 2 is required.

Corollary 2 (DAE-aware HOCBF for semi-explicit systems)**.** *Consider a semi-explicit DAE system satisfying Assumption 1. Let* $b(x)$ *have relative degree* $d \geq 1$ *on* $\mathcal{M}$ *with respect to* (7)*. Define the HOCBF hierarchy* $\psi_0(x) := b(x)$ *and*

$$\psi_i(x) := \mathcal{L}_{\hat{f}} \psi_{i-1}(x) + \alpha_i(\psi_{i-1}(x)), \quad i = 1, \ldots, d, \tag{11}$$

for class-$\mathcal{K}_\infty$ *functions* α_i*. Then* $\mathcal{D} \cap \mathcal{M}$ *is positively invariant if there exists* u *such that*

$$P(x)\big(J_d(x) f_d(x) + J_d(x) g_d(x) u\big) = 0, \tag{12a}$$

$$\mathcal{L}_{\hat{f}} \psi_{d-1}(x) + \alpha_d(\psi_{d-1}(x)) + \mathcal{L}_{\hat{g}} \psi_{d-1}(x) u \geq 0, \tag{12b}$$

hold for all $x \in \mathcal{D} \cap \mathcal{M}$ *with* $\psi_i(x(0)) \geq 0$ *for* $i = 0, \ldots, d$*.*

Proof. Condition (12a) ensures $x(t) \in \mathcal{M}$ by Theorem 2. On $\mathcal{M}$, the dynamics can be written as $\dot{x} = \hat{f}(x) + \hat{g}(x)u$, and $b(x)$ has relative degree d with respect to this system (Definition 3). Condition (12b) is the HOCBF condition [4] applied to the projected dynamics, giving $b(x(t)) \geq 0$ via iterated comparison arguments. □

Corollary 2 enforces manifold invariance through the compatibility condition (12a) and enforces safety via the HOCBF hierarchy in (12b) that is constructed from the projected Lie derivatives $\mathcal{L}_{\hat{f}}$ and $\mathcal{L}_{\hat{g}}$. When $d = 1$, this reduces to $\psi_0 = b(x)$, and condition (12b) recovers the CBF inequality (9b).

C. DAE-Aware CBF-QP

Based on the safety conditions in Theorem 2, we formulate a DAE-aware CBF-QP for relative degree one as follows.

$$\begin{aligned} \min_{u \in \mathcal{U}} \quad & \|u - u_{\text{nom}}\|^2 \\ \text{s.t.} \quad & P(x)\big(J_d(x) f_d(x) + J_d(x) g_d(x) u\big) = 0, \\ & \mathcal{L}_{\hat{f}} b(x) + \mathcal{L}_{\hat{g}} b(x) u \geq -\alpha(b(x)). \end{aligned} \tag{13}$$

In contrast to the standard CBF-QP (4), the DAE-aware formulation (13) jointly enforces the compatibility condition and the barrier inequality, ensuring that the resulting input maintains both manifold invariance and safety. Since the DAE system (1) is control-affine, the nominal controller u_{nom} can be any state-feedback policy (e.g., LQR, droop, or MPC); the CBF-QP (13) minimally modifies the supplied nominal input. For barriers with relative degree $d > 1$, the second constraint in (13) is replaced by (12b) from Corollary 2, while the compatibility constraint is unchanged. Theorem 2 guarantees safety for relative degree one, given a barrier function $b(x)$ that admits a compatible, safe input $u \in \mathcal{U}$ satisfying (9) at every $x \in \mathcal{D} \cap \mathcal{M}$. The following definition formalizes the notion of a valid DAE-aware CBF.

Definition 4 (Valid DAE-aware CBF)**.** *A smooth function* $b : \mathbb{R}^{n_x} \to \mathbb{R}$ *is a* valid DAE-aware CBF *for the safe set* $\mathcal{C}$ *under DAE* (1) *if (i)* $\mathcal{D} \cap \mathcal{M} \subseteq \mathcal{C} \cap \mathcal{M}$ *(correctness); and*

(ii) for every $x \in \mathcal{D} \cap \mathcal{M}$, there exists $u \in \mathcal{U}$ satisfying (9) *(feasibility).*

Definition 4 extends the standard valid CBF notion [3] to DAE systems, where correctness ensures the barrier set lies within the safe set on $\mathcal{M}$, and feasibility ensures the DAE-aware CBF-QP (13) admits a solution. The next section introduces the framework to verify both conditions using SOS-based verification methods.

IV. SOS-Based Verification

We now address the verification of a candidate DAE-aware CBF introduced in Definition 4. The following problem formalizes the verification part of Problem 1.

Problem 2. *Given a candidate DAE-aware CBF $b : \mathbb{R}^{n_x} \to \mathbb{R}$, verify (i)* correctness*, i.e., $\mathcal{D} \cap \mathcal{M} \subseteq \mathcal{C} \cap \mathcal{M}$; and (ii)* feasibility*, i.e., for every $x \in \mathcal{D} \cap \mathcal{M}$, there exists $u \in \mathcal{U}$ such that* (9) *holds.*

A. Correctness Verification

We begin with correctness verification, which requires certifying that $b(x) \geq 0$ for all $x \in \mathcal{D} \cap \mathcal{M}$. First, recall the Positivstellensatz (Psatz), a central result in real algebraic geometry for certifying emptiness of semialgebraic sets [25]. A polynomial $p(x)$ is *a sum of squares* (SOS) if $p(x) = \sum_i (p_i(x))^2$ for some polynomials p_i. Let Σ denote the SOS cone, $\mathcal{N}$ the multiplicative monoid, and $\mathbb{I}$ the polynomial ideal generated by a given set of polynomials [25]. The following result provides a necessary and sufficient condition for emptiness of semialgebraic sets.

Theorem 3 (Psatz [25])**.** *The set $\{x \in \mathbb{R}^{n_x} : \Phi_i(x) \geq 0,\ \chi_j(x) \neq 0,\ \Gamma_\ell(x) = 0\}$ is empty iff there exist $\Phi \in \Sigma$, $\chi \in \mathcal{N}$, and $\Gamma \in \mathbb{I}$ such that $\Phi + \chi^2 + \Gamma = 0$.*

Correctness requires $h(x) \geq 0$ for all $x \in \mathcal{D} \cap \mathcal{M}$. We encode the violation set using a slack variable $s \neq 0$, where $\mathcal{S}_{\text{viol}} := \{(x, s) : \phi(x) = 0,\ b(x) \geq 0, -h(x) - s^2 \geq 0\}$. The following lemma applies Theorem 3 to certify correctness.

Lemma 2 (Correctness via Psatz)**.** *Assume h, b, and ϕ are polynomials and $\mathcal{D} \cap \mathcal{M}$ is compact. Then $\mathcal{D} \cap \mathcal{M} \subseteq \mathcal{C} \cap \mathcal{M}$ if there exist SOS polynomials $\sigma_0, \sigma_1, \sigma_2$, polynomial multipliers ρ_ℓ for $\ell = 1, \ldots, n_m$, and integer $k \geq 1$ such that*

$$\sigma_0 + \sigma_1 b(x) + \sigma_2(-h(x) - s^2) + s^{2k} + \sum_{\ell=1}^{n_m} \rho_\ell \phi_\ell(x) = 0. \quad (14)$$

Proof. Identity (14) certifies $\mathcal{S}_{\text{viol}} = \emptyset$ by Theorem 3 applied to the cone generated by b and $-h - s^2$, the monoid generated by s, and the ideal generated by ϕ_ℓ. Emptiness of $\mathcal{S}_{\text{viol}}$ implies that no $x \in \mathcal{D} \cap \mathcal{M}$ satisfies $h(x) < 0$, i.e., $\mathcal{D} \cap \mathcal{M} \subseteq \mathcal{C} \cap \mathcal{M}$. □

Condition (14) is checked via an SOS feasibility program that *(i)* fixes degree bounds on $\sigma_0, \sigma_1, \sigma_2, \rho_\ell$; *(ii)* enforces $\sigma_i \in \Sigma$; and *(iii)* matches polynomial coefficients, reducing to a semidefinite program.

B. Feasibility Verification

We now verify that a compatible, safe input exists at every state in $\mathcal{D} \cap \mathcal{M}$. Let n_u^c denote the number of linear input constraints $A_u u \leq r_u$, where $A_u \in \mathbb{R}^{n_u^c \times n_u}$ and $r_u \in \mathbb{R}^{n_u^c}$. For a given $x \in \mathcal{D} \cap \mathcal{M}$, the existence of u that satisfies compatibility, the CBF condition, and input constraints is equivalent to feasibility of the affine system $A_{\text{dae}}(x)u \leq r_{\text{dae}}(x)$, where

$$A_{\text{dae}}(x) := \begin{bmatrix} -P(x)J_d(x)g_d(x) \\ P(x)J_d(x)g_d(x) \\ -\mathcal{L}_{\hat{g}} b(x) \\ A_u \end{bmatrix}, \quad (15)$$

$$r_{\text{dae}}(x) := \begin{bmatrix} P(x)J_d(x)f_d(x) \\ -P(x)J_d(x)f_d(x) \\ \mathcal{L}_{\hat{f}} b(x) + \alpha(b(x)) \\ r_u \end{bmatrix}. \quad (16)$$

The rows $\pm P(x)J_d(x)g_d(x)$ together enforce the compatibility equality (9a) via opposing inequalities; the row $-\mathcal{L}_{\hat{g}} b(x)$ encodes the CBF condition (9b); and A_u imposes input bounds. The following result provides the dual alternative used to certify feasibility.

Lemma 3 (Farkas' Lemma [26])**.** *The system $Au \leq r$ has a solution iff there is no $\lambda \geq 0$ with $\lambda^\top A = 0^\top$ and $\lambda^\top r < 0$.*

By Lemma 3, $A_{\text{dae}}(x)u \leq r_{\text{dae}}(x)$ is feasible if and only if there is no $\lambda \geq 0$ with $\lambda^\top A_{\text{dae}}(x) = 0^\top$ and $\lambda^\top r_{\text{dae}}(x) < 0$.

Separating interior and boundary conditions, we define the interior matrices $A_{\text{int}}(x)$, $r_{\text{int}}(x)$ (compatibility and input bounds only, omitting the CBF row) and boundary matrices

$$A_{\text{bnd}}(x) := \begin{bmatrix} A_{\text{int}}(x) \\ -\mathcal{L}_{\hat{g}} b(x) \end{bmatrix}, \quad r_{\text{bnd}}(x) := \begin{bmatrix} r_{\text{int}}(x) \\ \mathcal{L}_{\hat{f}} b(x) \end{bmatrix}.$$

The separation into interior and boundary is motivated by the tangent cone characterization of positive invariance [27]. At interior points of $\mathcal{D}$, any compatible input preserves barrier nonnegativity since $b(x) > 0$; at boundary points $\partial\mathcal{D}$, the input must additionally satisfy the CBF tangency condition to prevent trajectories from leaving $\mathcal{D}$.

Theorem 4 (DAE-aware CBF verification)**.** *Let b define the barrier set $\mathcal{D} := \{x : b(x) \geq 0\}$. Then b is a valid DAE-aware CBF (Definition 4) if and only if*

1) *(Correctness) $\mathcal{D} \cap \mathcal{M} \subseteq \mathcal{C} \cap \mathcal{M}$;*
2) *(Interior feasibility) For every $x \in \text{int}(\mathcal{D}) \cap \mathcal{M}$, the dual system $\lambda^\top A_{\text{int}}(x) = 0^\top$, $\lambda^\top r_{\text{int}}(x) < 0$ admits no $\lambda \geq 0$;*
3) *(Boundary tangency) For every $x \in \partial\mathcal{D} \cap \mathcal{M}$, the dual system $\lambda^\top A_{\text{bnd}}(x) = 0^\top$, $\lambda^\top r_{\text{bnd}}(x) < 0$ admits no $\lambda \geq 0$.*

Proof. By Lemma 3, $A_{\text{int}}(x)u \leq r_{\text{int}}(x)$ is feasible if and only if condition 2 holds, and $A_{\text{bnd}}(x)u \leq r_{\text{bnd}}(x)$ is feasible if and only if condition 3 holds. Together, these guarantee the existence of admissible inputs satisfying compatibility and input bounds at interior points, and additionally the tangency condition at boundary points. Positive invariance of $\mathcal{D} \cap \mathcal{M}$ then follows from Theorem 2. □

We note that the conditions in Theorem 4 are exact in that they do not impose a particular choice of class-$\mathcal{K}_\infty$ function α. This provides maximal flexibility in the feasibility analysis, since certifying the existence of *any* compatible safe input suffices. By contrast, Corollary 2 requires selecting $\alpha_1, \ldots, \alpha_d$ a priori, committing to a specific class-$\mathcal{K}_\infty$ parameterization in exchange for an online QP formulation.

C. Polynomial SOS Certificates

If the system mapping functions f_d, g_d, J_d, P, and b, and the sets $\mathcal{M}$, $\mathcal{C}$ are polynomial, and $\mathcal{D} \cap \mathcal{M}$ is compact, then

all entries of $A_{\mathrm{int}}(x)$, $A_{\mathrm{bnd}}(x)$, $r_{\mathrm{int}}(x)$, and $r_{\mathrm{bnd}}(x)$ are polynomial in x. Infeasibility of the dual systems can then be certified via the Psatz applied to the semialgebraic sets.

Proposition 1 (Polynomial DAE-aware certificates)**.** *Let f_d, g_d, J_d, P, and b be polynomial, let $\mathcal{M}$ and $\mathcal{C}$ admit polynomial equality and inequality expressions, and let $\mathcal{D} \cap \mathcal{M}$ be compact. Then conditions 2 and 3 of Theorem 4 hold if there exist SOS polynomials and multipliers that satisfy*

$$\Phi_{\mathrm{int}}(x, \lambda_{\mathrm{int}}) + s_{\mathrm{int}}^2 + \varphi_{\mathrm{int}}(x, \lambda_{\mathrm{int}}) = 0, \quad (17)$$

$$\Phi_{\mathrm{bnd}}(x, \lambda_{\mathrm{bnd}}) + s_{\mathrm{bnd}}^2 + \varphi_{\mathrm{bnd}}(x, \lambda_{\mathrm{bnd}}) = 0, \quad (18)$$

where $\Phi_{\mathrm{int}} \in \Sigma_{\mathrm{int}}$ denotes the cone generated by $b(x) \geq 0$, $\lambda_{\mathrm{int}} \geq 0$; $\Phi_{\mathrm{bnd}} \in \Sigma_{\mathrm{bnd}}$ denotes the cone generated by $\lambda_{\mathrm{bnd}} \geq 0$; monoid terms encode strict inequalities; and

$$\begin{aligned}\varphi_{\mathrm{int}}(\cdot) &= \textstyle\sum_q \rho_q(\cdot)\big[\lambda_{\mathrm{int}}^\top A_{\mathrm{int}}(x)\big]_q + \sum_\ell \rho_\ell^{\phi}(\cdot)\phi_\ell(x) \\ &\quad + \rho^s(\cdot)\big(-\lambda_{\mathrm{int}}^\top r_{\mathrm{int}}(x) - s_{\mathrm{int}}^2\big), \\ \varphi_{\mathrm{bnd}}(\cdot) &= \textstyle\sum_q \rho_q(\cdot)\big[\lambda_{\mathrm{bnd}}^\top A_{\mathrm{bnd}}(x)\big]_q + \sum_\ell \rho_\ell^{\phi}(\cdot)\phi_\ell(x) \\ &\quad + \rho^b(\cdot)b(x) + \rho^s(\cdot)\big(-\lambda_{\mathrm{bnd}}^\top r_{\mathrm{bnd}}(x) - s_{\mathrm{bnd}}^2\big).\end{aligned}$$

Proof. The proof follows from Lemma 3. The interior and boundary dual systems are infeasible iff their semialgebraic representations are empty. Theorem 3 then certifies such emptiness through the stated cone, monoid, and ideal identities. Given that all functions are polynomial, this is reduced to an SOS feasibility program. □

Proposition 1, combined with Lemma 2, provides a complete SOS-based verification framework for DAE-aware CBFs, where correctness is certified by (14) and feasibility is certified by (17)-(18). Both reduce to semidefinite programs that can be solved using standard SOS solvers. While Proposition 1 requires polynomial mappings, non-polynomial algebraic constraints (e.g., trigonometric power flow equations) can be handled by introducing auxiliary variables that lift the system to a polynomial DAE on an extended manifold [17]; see Section V.

V. Case Studies

Based on the results in Sections III and IV, we investigate the following research questions.

- (Q1) Does the DAE-aware CBF in Theorem 2 guarantee manifold compatibility and safe set invariance?
- (Q2) Do the candidate barriers satisfy the validity conditions in Theorem 4, as certified by the SOS programs in Lemma 2 and Proposition 1?
- (Q3) For an autonomous power DAE from [15] with $u \equiv 0$, does Corollary 1 certify positive invariance of $\mathcal{D} \cap \mathcal{M}$?

To answer these questions, we consider two semi-explicit power system DAEs. We first apply the DAE-aware CBF-QP (Theorem 2) and the SOS verification framework (Theorem 4 via Lemma 2 and Proposition 1) to a nonlinear network preserving DAE model [9], [17], [28]. We then consider a two bus polynomial benchmark from [15] to verify Corollary 1.

A. Nonlinear Power System DAE Model

The model is a classical network preserving power system DAE with a second-order generator model [17]. This formulation couples the swing equations for generator dynamics with algebraic power balance constraints at load buses. The solvability and index-1 structure of such models are established in [9]. We consider a two bus network with one generator bus and one load bus; see Fig. 3. Let the dynamic states be $x_d = [\delta_g, \omega_g]^\top \in \mathbb{R}^2$ and the algebraic states be $x_a = [\delta_\ell, V_\ell]^\top \in \mathbb{R}^2$, where δ_g and ω_g denote generator rotor angle and speed, and δ_ℓ and V_ℓ denote load bus voltage angle and magnitude. The nonlinear semi-explicit DAE model can be written as

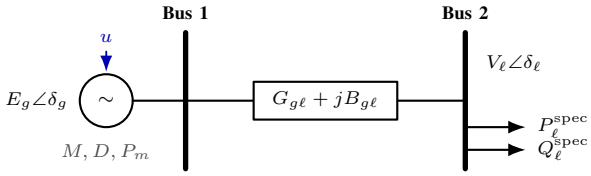

Fig. 3. Single-line diagram of the two-bus power system (19). Dynamic states x_d are the generator rotor angle and speed; algebraic states x_a are the load bus voltage angle and magnitude, coupled through the power flow constraints (19c)-(19d).

$$\dot{\delta}_g = \omega_g, \quad (19a)$$

$$M\dot{\omega}_g = -D\omega_g + P_m - P_e(x) + u, \quad (19b)$$

$$0 = \phi_1(x) := P_\ell^{\mathrm{spec}} - P_\ell(\delta_g, \delta_\ell, V_\ell), \quad (19c)$$

$$0 = \phi_2(x) := Q_\ell^{\mathrm{spec}} - Q_\ell(\delta_g, \delta_\ell, V_\ell), \quad (19d)$$

where $\vartheta := \delta_g - \delta_\ell$ is the angle difference across the transmission line, $P_e(x) := E_g^2 G_{gg} + E_g V_\ell (G_{g\ell}\cos\vartheta + B_{g\ell}\sin\vartheta)$ is the electrical power injected by the generator, $P_\ell := V_\ell^2 G_{\ell\ell} + V_\ell E_g (G_{\ell g}\cos\vartheta - B_{\ell g}\sin\vartheta)$ and $Q_\ell := -V_\ell^2 B_{\ell\ell} - V_\ell E_g (G_{\ell g}\sin\vartheta + B_{\ell g}\cos\vartheta)$ are the active and reactive power absorbed at the load bus. The parameters $M > 0$ and $D > 0$ are inertia and damping coefficients, P_m is mechanical power, $P_\ell^{\mathrm{spec}}, Q_\ell^{\mathrm{spec}}$ are active and reactive load setpoints, E_g is the internal generator voltage magnitude, and G_{ij}, B_{ij} are entries of the network admittance matrix.

The safety specification enforces voltage boundedness at the load bus, requiring $V_\ell \in [V_{\min}, V_{\max}]$ to prevent voltage violations that can trigger protective relay actions. Defining $h(x) := (V_\ell - V_{\min})(V_{\max} - V_\ell)$, the safe set is $\mathcal{C} = \{x : h(x) \geq 0\}$. We consider a quadratic candidate barrier function

$$\begin{aligned}b(x) :=& \beta_0 - \beta_1(\delta_g - \delta_g^\star)^2 - \beta_2\omega_g^2 \\ &- \beta_3(\delta_\ell - \delta_\ell^\star)^2 - \beta_4(V_\ell - V_\ell^\star)^2, \end{aligned} \quad (20)$$

with coefficients $\beta_i > 0$ selected around an equilibrium $(\delta_g^\star, \delta_\ell^\star, V_\ell^\star)$, so $\mathcal{D} = \{x : b(x) \geq 0\}$.

Note that the derivation of candidate DAE-aware CBFs is outside the scope of this paper. The two-bus model isolates the generator-load algebraic coupling that is the building block of larger network-preserving DAE models, which makes it a canonical benchmark for validating DAE safety methods before scaling to higher-dimensional systems.

The parameters are $M = 0.1$, $D = 0.05$, $E_g = 1.05$, $P_m = 0.8$, with a symmetric two bus admittance matrix $Y_{gg} = Y_{\ell\ell} = 5 - j15$ and $Y_{g\ell} = Y_{\ell g} = -5 + j15$. The load setpoints are $P_\ell^{\mathrm{spec}} = -0.78$, $Q_\ell^{\mathrm{spec}} = -0.56$, yielding the equilibrium $\delta_g^\star \approx 0.034$, $\omega_g^\star = 0$, $\delta_\ell^\star = 0$, $V_\ell^\star = 1.0$. The voltage limits are $V_{\min} = 0.9$ and $V_{\max} = 1.1$, and the

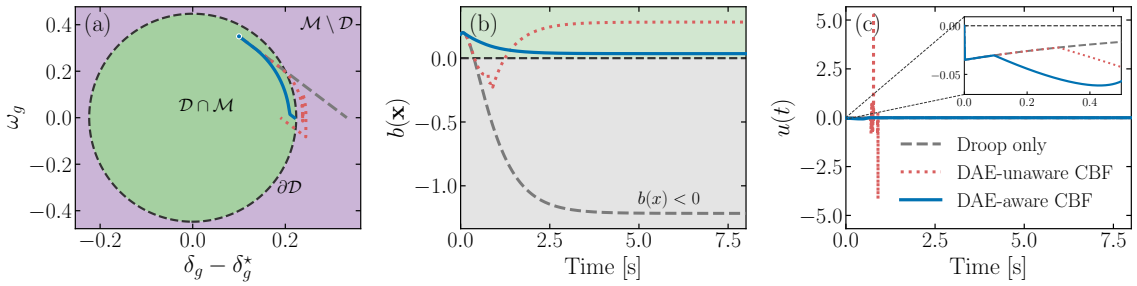

Fig. 4. A power system DAE (19) with droop nominal controller $u_{\text{nom}} = -K_p\omega_g$, $K_p = 0.1$. **(a)** Phase portrait in dynamic states $(\delta_g - \delta_g^\star, \omega_g)$: the DAE-aware CBF (blue) stays inside the barrier boundary $\partial\mathcal{D} \cap \mathcal{M}$, while both the DAE-unaware CBF (red, dotted) and droop-only (gray, dashed) trajectories exit $\mathcal{D}$. **(b)** Barrier function $b(x)$: the DAE-aware filter maintains $b \geq 0$; the droop-only system reaches $b = -1.22$; the DAE-unaware CBF drives b to -0.23. **(c)** Control inputs: the DAE-aware CBF applies modest corrections ($\max|u| = 0.061$), while the DAE-unaware CBF produces destabilizing inputs ($\max|u| = 5.26$).

barrier coefficients are $(\beta_0, \ldots, \beta_4) = (1, 10, 5, 10, 100)$. All computations use Drake 1.40.0 [29] with MOSEK 10.2 on an Apple M1 Pro with 16 GB RAM.

Note that the barrier (20) has relative degree $d = 1$ with respect to the projected dynamics (7). To see this, note that $g_d(x) = [0,\ 1/M]^\top$ enters $\dot{\omega}_g$ directly via (19b) and $b(x)$ depends on ω_g through the term $-\beta_2\omega_g^2$; since ϕ is independent of ω_g, we have $J_d(x)g_d(x) = 0$ and the lower block of $\hat{g}$ in (7) vanishes, yielding $\mathcal{L}_{\hat{g}}b(x) = \nabla b(x)^\top \hat{g}(x) = -2\beta_2\omega_g/M \neq 0$ near $\partial\mathcal{D} \cap \mathcal{M}$. Hence $d = \nu + d' - 1 = 1$ (Definition 3), and Theorem 2 applies directly without the HOCBF hierarchy of Corollary 2. On the operating set, the Jacobian $J_a(x) = \nabla_{x_a}\phi(x) \in \mathbb{R}^{2\times 2}$ is nonsingular, satisfying Assumption 1. Although this is a mild assumption, we verify regularity by sampling 1000 points in $\mathcal{D} \cap \mathcal{M}$ and find $\min|\det J_a| = 249.1$. The nominal controller is a proportional frequency droop $u_{\text{nom}} = -K_p\omega_g$ with $K_p = 0.1$. We simulate the DAE-aware CBF-QP with class-$\mathcal{K}_\infty$ function $\alpha(r) = r$ and initial condition $(\delta_g(0), \omega_g(0)) = (\delta_g^\star + 0.1\text{ rad},\ 0.35\text{ rad/s})$ (near the boundary of $\mathcal{D}$, $b(x(0)) = 0.188$), using backward Euler integration with step size $\Delta t = 0.002$ s over a horizon of $T = 8$ s (4000 steps). With the DAE-aware CBF filter active, $\min_t b(x(t)) \geq 3.5 \times 10^{-2} > 0$ and $\max_t|u(t)| = 0.061$, confirming that $\mathcal{D} \cap \mathcal{M}$ is positively invariant. For comparison, we also run a *DAE-unaware* CBF-QP that evaluates the Lie derivatives along the original (f_d, g_d) instead of the projected $(\hat{f}, \hat{g})$, ignoring the algebraic response $\dot{x}_a = -J_a^{-1}J_d(f_d + g_d u)$. The DAE-unaware filter produces $\min_t b(x(t)) = -0.23$ and $\max_t|u(t)| = 5.26$, violating safety despite applying large control effort. The droop-only case also violates safety ($\min_t b = -1.22$), as shown in Fig. 4. This confirms that ignoring the algebraic coupling leads to safety violations, thereby answering (Q1).

We now verify the correctness and feasibility conditions in Theorem 4 according to the proposed SOS framework. We adopt the standard polynomial lifting used for power system DAEs [17] as follows.

$$z_1 := \sin(\delta_g - \delta_\ell), \qquad z_2 := \cos(\delta_g - \delta_\ell).$$

This replaces the trigonometric terms in the power flow equations with polynomial variables. To ensure that (z_1, z_2) remains consistent with a physical angle difference, we add the algebraic constraint

$$0 = \phi_3(x, z) := z_1^2 + z_2^2 - 1, \tag{21}$$

where the lifted state and constraint vector are defined as $\bar{x} := [x^\top, z_1, z_2]^\top \in \mathbb{R}^{n_x+2}$ and $\bar{\phi}(\bar{x}) := [\phi_1(x), \phi_2(x), \phi_3(x, z)]^\top$. Then ϕ_1, ϕ_2 become polynomial in (x, z). Thus, substituting z_1, z_2 into (19) yields a polynomial DAE on the lifted manifold $\bar{\mathcal{M}} := \{\bar{x} : \bar{\phi}(\bar{x}) = 0\}$.

For correctness (Lemma 2), the choice $\beta_4 = 1/(h(x^\star)) = 100$ admits the analytical Psatz identity (14) with $\sigma_1 = h(x^\star) = 0.01$, $\sigma_2 = 1$, $\sigma_0 = \sigma_1[\beta_1(\delta_g - \delta_g^\star)^2 + \beta_2\omega_g^2 + \beta_3(\delta_\ell - \delta_\ell^\star)^2]$, $\rho_\ell = 0$, and $k = 1$. This certificate uses no algebraic constraint multipliers: $b(x) \geq 0$ directly implies $(V_\ell - V_\ell^\star)^2 \leq h(x^\star)$ and hence $h(x) \geq 0$. Correctness is also confirmed numerically by solving (14) as an SDP with degree-0 multipliers σ_1 and ρ_ℓ on the six-variable lifted model ($n_x + 2 = 6$ variables, $n_m = 3$ constraints); MOSEK returns a feasible certificate in 0.02 s. For feasibility (Proposition 1), since u is unconstrained and $P(x) = 0$, the DAE-aware CBF condition reduces to $\mathcal{L}_{\hat{f}}b(x) + \mathcal{L}_{\hat{g}}b(x)u \geq -\alpha(b(x))$, which admits a solution whenever $\mathcal{L}_{\hat{g}}b(x) \neq 0$. Sampling 282 points near $\partial\mathcal{D} \cap \mathcal{M}$, we find $\min|\mathcal{L}_{\hat{g}}b| = 0.34 > 0$, confirming feasibility. This answers (Q2) for the nonlinear power DAE.

B. Verification of Voltage Constraints

We now consider the two bus system in [15], where bus 1 is a slack bus with fixed voltage magnitude and angle $(V_1, \delta_1) = (1, 0)$, and bus 2 is a load bus. Unless stated otherwise, the model equations, parameter values, voltage limits, and certificate in this subsection follow [15]. The active and reactive load powers at bus 2 are modeled by the following linear dynamic model

$$\dot{x} = \begin{bmatrix} 0 & \omega & 0 \\ -\omega & 0 & 0 \\ 0 & 0 & -1/\tau \end{bmatrix} x, \tag{22a}$$

$$\begin{bmatrix} p_2 \\ q_2 \end{bmatrix} = \begin{bmatrix} c_{11} & 0 & c_{13} \\ c_{21} & 0 & c_{23} \end{bmatrix} x + \begin{bmatrix} d_1 \\ d_2 \end{bmatrix}. \tag{22b}$$

The parameter values are $\omega = 2\pi/24$, $\tau = 400$, $c_{11} = 0.045$, $c_{13} = 0.015$, $c_{21} = 0.008$, $c_{23} = 0.015$, $d_1 = -0.83$, and $d_2 = -0.62$.

For the polynomial DAE form, define algebraic variables

$$z_1 := V_2, \qquad z_2 := \sin(\delta_2), \qquad z_3 := \cos(\delta_2).$$

Let $x_d := x \in \mathbb{R}^3$, $x_a := z \in \mathbb{R}^3$, and $x = [x_d^\top, x_a^\top]^\top \in \mathbb{R}^6$.

The algebraic constraints are

$$0 = \phi_1(x) := p_2 - \psi_p(z), \tag{23a}$$
$$0 = \phi_2(x) := q_2 - \psi_q(z), \tag{23b}$$
$$0 = \phi_3(x) := z_2^2 + z_3^2 - 1, \tag{23c}$$

where ψ_p, ψ_q denote the active and reactive power flow expressions written in lifted polynomial coordinates, induced by the two bus admittance matrix in [15]; we use voltage limits $V_{\min} = 0.9$ and $V_{\max} = 1.1$.

The safety specification is voltage boundedness at bus 2, defined by $h(x) := (z_1 - V_{\min})(V_{\max} - z_1)$, with safe set $\mathcal{C} = \{x : h(x) \geq 0\}$. We consider the following candidate barrier function from [15]

$$b(x) := 8.52 - 0.416x_1^2 - 0.416x_2^2 - 0.171x_3^2, \tag{24}$$

defining the barrier set $\mathcal{D} = \{x : b(x) \geq 0\}$.

We apply Corollary 1 to (22)-(23). Since $n_m = n_a = 3$, the Jacobian $J_a(x) \in \mathbb{R}^{3\times 3}$ is square and $P(x) = 0$ (Remark 1), so the compatibility condition (10a) is trivially satisfied. Sampling 2000 points in $\mathcal{D} \cap \mathcal{M}$, we find $\min |\det J_a| = 500.9$, confirming regularity (Assumption 1). For the CBF condition (10b), note that b depends only on x_d (i.e., $\nabla_{x_a} b = 0$), thus the projected Lie derivative reduces to $\mathcal{L}_{\hat{f}} b(x) = \nabla_{x_d} b \cdot A x_d$. The skew-symmetric oscillator block of A cancels the x_1-x_2 cross terms, yielding $\mathcal{L}_{\hat{f}} b(x) = (2\beta_3/\tau)x_3^2 \geq 0$ for all x, where $\beta_3 = 0.171$ is the coefficient of x_3^2 in (24) and $\tau = 400$. Since $\mathcal{L}_{\hat{f}} b \geq 0 \geq -\alpha(b)$ on $\mathcal{D}$ for any $\alpha \in \mathcal{K}_\infty$, condition (10b) holds and Corollary 1 certifies positive invariance of $\mathcal{D} \cap \mathcal{M}$. Correctness ($\mathcal{D} \cap \mathcal{M} \subseteq \mathcal{C} \cap \mathcal{M}$) is confirmed by sampling: $\min_{\mathcal{D}\cap\mathcal{M}} h(x) = 4.2 \times 10^{-3} > 0$. This answers (Q3) and concludes the case studies.

VI. Conclusion

This paper develops a DAE-aware CBF framework for regular semi-explicit DAE systems. We introduce a projected dynamics representation on the constraint manifold, which yields safety conditions that enforce set invariance together with algebraic consistency. We then provide SOS verification conditions for correctness and feasibility of candidate barrier functions. Power system case studies illustrate the proposed results and show that accounting for algebraic coupling is essential for reliable safety guarantees.

References

[1] F. Blanchini, "Set invariance in control," *Automatica*, vol. 35, no. 11, pp. 1747–1767, 1999.

[2] A. D. Ames, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs with application to adaptive cruise control," in *53rd IEEE Conference on Decision and Control*, 2014, pp. 6271–6278.

[3] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, "Control barrier functions: Theory and applications," in *2019 18th European Control Conference (ECC)*, 2019, pp. 3420–3431.

[4] W. Xiao and C. Belta, "High-order control barrier functions," *IEEE Transactions on Automatic Control*, vol. 67, no. 7, pp. 3655–3662, 2022.

[5] C. Dawson, S. Gao, and C. Fan, "Safe control with learned certificates: A survey of neural Lyapunov, barrier, and contraction methods for robotics and control," *IEEE Transactions on Robotics*, vol. 39, no. 3, pp. 1749–1767, 2023.

[6] G. Wu and K. Sreenath, "Safety-Critical and Constrained Geometric Control Synthesis using Control Lyapunov and Control Barrier Functions for Systems Evolving on Manifolds," in *2015 American Control Conference (ACC)*. IEEE, 2015, pp. 2038–2044.

[7] M. H. Cohen, R. K. Cosner, and A. D. Ames, "Constructive Safety-Critical Control: Synthesizing Control Barrier Functions for Partially Feedback Linearizable Systems," *IEEE Control Systems Letters*, vol. 8, pp. 2229–2234, 2024.

[8] P. Kunkel and V. Mehrmann, *Differential-algebraic Equations: Analysis and Numerical Solution*, ser. EMS textbooks in mathematics. European Mathematical Society, 2006.

[9] T. Groß, S. Trenn, and A. Wirsen, "Solvability and stability of a power system DAE model," *Systems and Control Letters*, vol. 97, pp. 12–17, 2016.

[10] 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.

[11] E. A. Cross and I. M. Mitchell, "Level set methods for computing reachable sets of systems with differential algebraic equation dynamics," in *2008 American Control Conference*, 2008, pp. 2260–2265.

[12] T. Dang, A. Donzé, and O. Maler, "Verification of analog and mixed-signal circuits using hybrid system techniques," in *Formal Methods in Computer-Aided Design*, A. J. Hu and A. K. Martin, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 21–36.

[13] M. Althoff, "Formal and Compositional Analysis of Power Systems Using Reachable Sets," *IEEE Transactions on Power Systems*, vol. 29, no. 5, pp. 2270–2280, 2014.

[14] Y. Zhou, P. Zhang, and M. Yue, "Reachable Dynamics of Networked Microgrids With Large Disturbances," *IEEE Transactions on Power Systems*, vol. 36, no. 3, pp. 2416–2427, 2021.

[15] R. Pedersen, C. Sloth, and R. Wisniewski, "Verification of power grid voltage constraint satisfaction – A barrier certificate approach," *2016 European Control Conference (ECC)*, pp. 447–452, 2016.

[16] S. Kundu, S. Geng, S. P. Nandanoori, I. A. Hiskens, and K. Kalsi, "Distributed Barrier Certificates for Safe Operation of Inverter-Based Microgrids," in *2019 American Control Conference (ACC)*, 2019, pp. 1042–1047.

[17] S. Kundu and M. Anghel, "Stability and control of power systems using vector Lyapunov functions and sum-of-squares methods," *2015 European Control Conference, ECC 2015*, pp. 253–259, 2015.

[18] E. Jensen, N. Junnarkar, M. Arcak, X. Wu, and S. Gumussoy, "Certifying Stability and Performance of Uncertain Differential-Algebraic Systems: A Dissipativity Framework," *IEEE Transactions on Control of Network Systems*, vol. 12, no. 1, pp. 18–27, 2025.

[19] A. Portela, I. Bessa, R. Márquez, and M. Bernal, "A Novel LMI-Based Design of Rational Control Laws for a Class of Nonlinear Systems Modeled as Differential Algebraic Equations," *IEEE Control Systems Letters*, vol. 9, pp. 2199–2204, 2025.

[20] G. Michos and G. C. Konstantopoulos, "Decentralized voltage control of ac microgrids with constant power loads using control barrier functions," *IEEE Transactions on Control of Network Systems*, vol. 13, no. 2, pp. 1134–1145, 2026.

[21] Y. Park and C. Sloth, "Differential-algebraic equation control barrier function for flexible link manipulator," in *2024 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, 2024, pp. 12 408–12 413.

[22] H. Zhang, M. H. Kazma, M. Ma, T. T. Johnson, and A. F. Taha, "Verification and Forward Invariance of Control Barrier Functions for Differential-Algebraic Systems," *arXiv preprint arXiv:2603.13509*, 2026.

[23] H. Khalil, *Nonlinear Systems*. Prentice Hall, 2002.

[24] A. Isidori, "The zero dynamics of a nonlinear system: From the origin to the latest progresses of a long successful story," *European Journal of Control*, vol. 19, no. 5, pp. 369–378, 2013.

[25] P. A. Parrilo, "Semidefinite programming relaxations for semialgebraic problems," *Mathematical programming*, vol. 96, pp. 293–320, 2003.

[26] J. Matousek and B. Gärtner, *Understanding and Using Linear Programming*, ser. Universitext. Springer Berlin Heidelberg, 2006.

[27] F. Blanchini and S. Miani, *Set-Theoretic Methods in Control*, ser. Systems & Control: Foundations & Applications. Springer International Publishing, 2015.

[28] S. A. Nugroho and A. F. Taha, "Load- and renewable-following control of linearization-free differential algebraic equation power system models," *IEEE Transactions on Control Systems Technology*, vol. 31, no. 4, pp. 1774–1786, 2023.

[29] R. Tedrake and the Drake Development Team, "Drake: Model-based design and verification for robotics," 2019.