On Resilience Guarantees by Finite-Time Robust Control Barrier Functions

Kamil Hassan, Daniel Selvaratnam and Henrik Sandberg

I. Introduction

In this study, we provide a control-theoretic description of resilience with the aim of establishing a unified framework for resilient control design for safety-critical systems. Resilience, in its essence, refers to the faculty to 1) oppose deviation from nominal behavior and, 2) quickly recover from a perturbed state [1]. These two attributes, referred to in this study as *durability* and *recoverability*, respectively, form the defining characteristics of a resilient system. To capture these traits in our control-theoretic formulation of resilience, we define durability and recoverability in the ensuing fashion.

Definition 1. *A system is deemed* **resilient** *with respect to its safe set if it satisfies the following criteria.*

1) ***(Durability)*** *The system trajectories (starting from inside the safe set) remain within the safe set as long as the nominal conditions are upheld.*
2) ***(Recoverability)*** *If the nominal conditions are intermittently perturbed because of an adversarial intervention, for example, the system trajectories could leave the safe set. However, once these conditions are restored, the system recovers in* finite time *to re-establish the given safety constraints.*

In a departure from the current literature, our formulation provides measurable metrics to assess resilience in a system, and also offers quantifiable control objectives to establish a framework for safety-critical control design. This framework is then developed using finite-time robust control barrier functions in our study.

II. System Description and Problem Formulation

In this work, we consider system dyanamics of the form

$$\dot{x}(t) = f(x(t)) + g(x(t))u(t) + d_m(t) + d_a(t), \tag{1a}$$
$$x(t_0) = x_0, \tag{1b}$$

where $x(t) \in \mathcal{X} \subset \mathbb{R}^n$, and $u(t) \in \mathcal{U} \subset \mathbb{R}^p$. Furthermore, d_m, $d_a : \mathbb{R}^+ \to \mathbb{R}^n$ are Lebesgue measurable exogenous inputs to (1) such that $d_m(t)$ is known (measured), for all t, and $d_a(t)$, while unknown and possibly adversarial, is assumed to remain Φ-bounded under *nominal conditions*: $\|d_a(t)\| \leq \Phi \in \mathbb{R}^+$, $\forall t$. Then the problem addressed in this study is formulated as follows.

K. Hassan, D. Selvaratnam and H. Sandberg are with the School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, Sweden. {kamilha,selv,hsan}@kth.se

Problem: Design a state-feedback controller for (1) such that it renders the resulting closed-loop system *resilient* with respect to a given safe set $S \subset \mathbb{R}^n$, per Definition 1[1].

III. Results

Firstly, we define finite-time robust control barrier functions (FR-CBFs).

Definition 2. *A continuously differentiable function $h : \mathcal{X} \to \mathbb{R}$ is called a* Finite-Time Robust Control Barrier function (FR-CBF) *with respect to its 0-superlevel set S[2] for* (1) *if there exists $\gamma > 0$ and $c \in [0,1)$ such that $\forall t$, and for all $x \in \mathcal{X} \subset \mathbb{R}^n$,*

$$\sup_{u \in \mathcal{U}} \Big(L_f h(x) + L_g h(x) u + \frac{\partial h}{\partial x}(x) d_m(t) - \Psi\Phi \Big) \geq -\text{sign}(h(x))\, \gamma |h(x)|^c, \tag{2}$$

where $\Psi = \sup_{x \in \mathcal{X}} \| \frac{\partial h}{\partial x}(x) \|$.

Correspondingly, if the set

$$\Omega(d_m, x) := \big\{ \mathrm{u} \in \mathcal{U} \mid L_f h(x) + L_g h(x) \mathrm{u} + \frac{\partial h}{\partial x}(x) d_m - \Psi\Phi \geq -\text{sign}(h(x))\, \gamma |h(x)|^c \big\} \tag{3}$$

is non-empty for all $x \in \mathcal{X}$, and $d_m \in \mathbb{R}^n$, then h is a valid FR-CBF for (1). Now we present the following result that uses the above mentioned FR-CBF-based set of point-wise admissible controls to solve the given problem.

Theorem 1. *Let the* 0*-superlevel set S of the FR-CBF h in Definition 2 be the given safe set for* (1)*. If the controller for* (1) *is designed such that for all t, the corresponding control input*

$$u(t) \in \Omega(d_m(t), x(t)), \tag{4}$$

then the resulting closed-loop system is rendered resilient and the given problem is solved.

Theorem 1 provides us with a condition in (4) to design a controller that offers resilience guarantees for (1). However, owing to sampling delays, it may not be feasible to update the controller in continuous time to satisfy (4) for all t. To address that case, in this work, we also develop sufficient conditions for the design of a zero-order-hold (ZOH) piecewise-constant control input for (1) that solves the given problem. The details regarding this could be found in [2].

[1] As mentioned under (1), the Φ-boundedness of $d_a(t)$ constitutes the nominal conditions that quantify the resilience objectives pursued for (1), per Definition 1.

[2] That is, $S := \{x \in \mathcal{X} \mid h(x) \geq 0\}$.

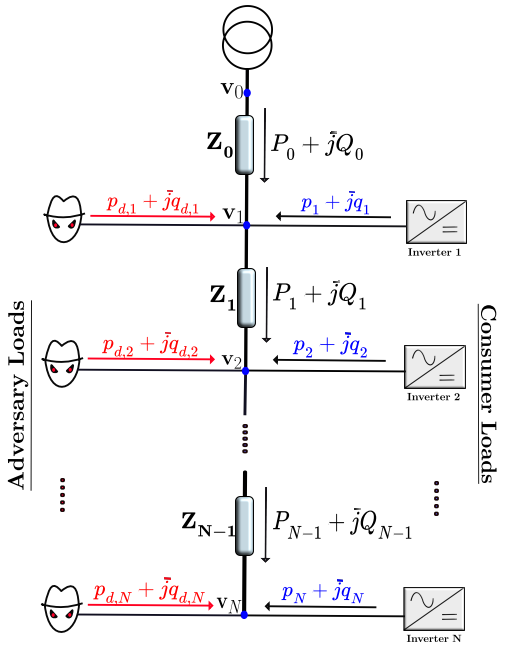


Fig. 1: Inverter-interfaced power distribution network with radial grid topology.

IV. Resilient Control of Power Inverter Networks

In this section, the theory developed previously is applied to power inverter networks of the form shown in Fig. 1. In particular, we require the voltage magnitude $v_i(t) \in \mathbb{R}^+$ at each node i of the considered grid to lie within a specified distance $\xi \in \mathbb{R}^+$ from the nominal voltage $\bar{v} \in \mathbb{R}^+$ such that, for all t,

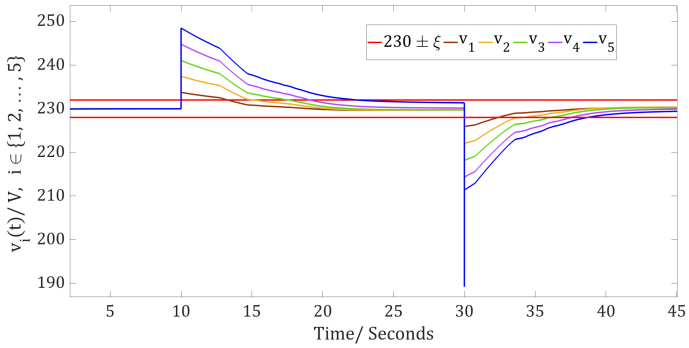
$$|\bar{v} - v_i(t)| \leq \xi, \quad \forall i \in \{1,2,\ldots,N\}. \tag{5}$$

This then allows us to formulate the safe set for each node as $S_v = \{v \in \mathbb{R} \mid |\bar{v} - v| \leq \xi\}$. For all i, the objective is to regulate the voltage trajectory $v_i(t)$ using reactive power compensation from the consumer inverters such that the given grid is deemed resilient with respect to S_v per Definition 1. To that end, the dynamics considered for the reactive power compensation from consumer inverter i, for all i, is given by

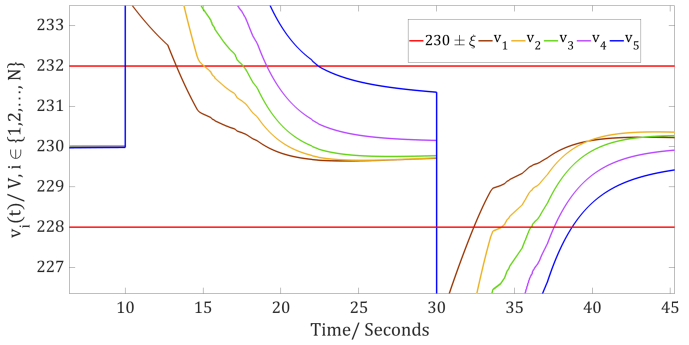
$$\dot{q}_i(t) = \frac{1}{\tau_i} q_i(t) + u_i(t), \quad \in \mathbb{R}, \tag{6}$$

where $\tau_i \in \mathbb{R}^+$ is the inverter's time constant. The controller u_i in (6) is then designed according to (4), yielding results shown in Fig. 2 for a grid with $N = 5$ nodes.

Note that for the simulation results shown in Fig. 2, the nominal voltage $\bar{v} = 230$ V and the relative safety range $\xi = 2$ V. Correspondingly, the safe set for this example is given by the values lying between (and including) the horizontal red lines in Fig. 2. Furthermore, the perturbation of the voltage trajectories seen at Time $= 10$ and 30 seconds in Fig. 2 corresponds to the violation of the nominal conditions under which it is indeed permissible for the trajectories to leave the safe set, per Definition 1. However, once the nominal conditions were restored (instantaneously, in each case), we



(a)



(b)

Fig. 2: For all $i \in \{1,2,\ldots,5\}$, the voltage magnitude v_i evolving under the control action designed according to (4). In the sub-Figure 2b, a zoomed-in plot of the voltage trajectories from sub-Figure 2a is shown to highlight the finite-time recovery of the trajectories to the safe set post-transgression.

can observe that the nodal trajectories converged back to the given safe range in finite time, thereby demonstrating the trait of recoverability from the definition of the resilience framework. Furthermore, excluding the time at which the nominal conditions were intermittently violated and the time between each violation and recovery, the voltage trajectories remained within the safe set, thereby showcasing the attribute of durability from Definition 1. Therefore, in conclusion, the grid is deemed resilient according to Definition 1.

References

[1] H. T. Tran, M. Balchanos, J. C. Domerçant, and D. N. Mavris, "A framework for the quantitative assessment of performance-based system resilience," *Reliability Engineering & System Safety*, vol. 158, pp. 73–84, 2017.

[2] K. Hassan, D. Selvaratnam, and H. Sandberg, "On resilience guarantees by finite-time robust control barrier functions with application to power inverter networks," *IEEE Open Journal of Control Systems*, 2024.