Compositional Construction of Safety Controllers for Networks of Continuous-Space POMDPs

Niloofar Jahanshahi, Abolfazl Lavaei, Member, IEEE, and Majid Zamani, Senior Member, IEEE

Abstract—In this article, we propose a compositional framework for the synthesis of safety controllers for networks of partially observable discrete-time stochastic control systems (also known as continuous-space partially observable Markov decision processes (POMDPs)). Given an estimator, we utilize a discretization-free approach to synthesize controllers ensuring safety specifications over finite-time horizons. The proposed framework is based on a notion of so-called local control barrier functions (CBFs) computed for subsystems in two different ways. In the first scheme, no prior knowledge of estimation accuracy is needed. The second framework utilizes a probability bound on the estimation accuracy using a notion of so-called stochastic simulation functions. In both proposed schemes, we derive sufficient small-gain-type conditions in order to compositionally construct control barrier functions for interconnected POMDPs using local barrier functions computed for subsystems. The constructed control barrier functions for the overall networks enable us to compute lower bounds on the probabilities that the interconnected POMDPs avoid certain unsafe regions in finite-time horizons. We demonstrate the effectiveness of our proposed approaches by applying them to an adaptive cruise control problem.

Index Terms—Continuous-space partially observable Markov decision processes (POMDPs), control barrier functions, formal synthesis, large-scale stochastic systems, small-gain conditions, stochastic simulation functions (SSFs).

I. INTRODUCTION

LARGE-SCALE stochastic systems have received significant attention in the past few years due to their broad applications in modeling many engineering systems such as power grids, road traffic networks, and industrial control systems, to name a few. Guaranteeing safety and reliability of such complex systems in a formal as well as time- and cost-effective way has always been very challenging. In principle, safety verifications’ goal is to show that the systems’ trajectories will not enter an unsafe region in the state-space. In the past few years, formal verification and synthesis of controllers against safety specifications have gained considerable attention among both control theorists and computer scientists. In this respect, abstraction-based techniques have been widely employed for the formal synthesis of safety controllers [1], [2]. However, those approaches rely on the state and input set discretization and consequently suffer severely from the curse of dimensionality: computational complexity grows exponentially with the dimension of the system. In order to overcome this difficulty, compositional techniques have been introduced in the past few years to construct finite abstractions of interconnected systems based on abstractions of smaller subsystems [3]–[8].

As another promising alternative, discretization-free approaches based on barrier functions have been introduced in the past decade. Assuming prior knowledge of barrier functions, the results in [9]–[12] introduce several techniques to ensure the safety of non-stochastic dynamical systems. Compositional construction of control barrier functions (CBFs) for nonstochastic systems is presented in [13] and [14]. Existing results for stochastic systems include verification and synthesis of controllers for continuous and stochastic hybrid systems over infinite-time horizons [15]–[17]. Compositional construction of barrier functions for continuous and stochastic hybrid systems is presented in [18] and [19].

Unfortunately, all of the aforementioned literature on discretization-based and -free techniques assumes availability of full state information, which is not the case in many practical applications. Taking this limitation into account, CBFs for stochastic systems with incomplete information under (Gaussian) process and measurement noise have been proposed in [20]. The works in [21]–[24] study verification of partially observable Markov decision processes with finite state and action spaces (finite POMDPs) using barrier certificates. A policy synthesis in multiagent POMDPs via discrete-time barrier functions to enforce safety is proposed in [25] and [26]. The work in [27] studies a controller synthesis scheme for stochastic systems with incomplete information by assuming a prior knowledge of CBFs. Given an estimator with a probabilistic guarantee on the accuracy of estimations, [28] studied the controller synthesis problem for partially observable stochastic systems and proposed a lower bound for the probability of satisfaction for safety specifications over finite-time horizons.

Manuscript received 6 October 2021; revised 22 March 2022; accepted 1 May 2022. Date of publication 27 June 2022; date of current version 13 March 2023. This work was supported in part by H2020 ERC Starting Grant AutoCPS under Grant 804639 and in part by German Research Foundation (DFG) through the Research Training Group under Grant 2428. Recommended by Associate Editor A. Gasparri.

(Corresponding author: Abolfazl Lavaei.)

Niloofar Jahanshahi is with the Computer Science Department, Ludwig Maximilian University of Munich, 80538 Munich, Germany (e-mail: jahanshahi.nil@gmail.com).

Abolfazl Lavaei is with the Institute for Dynamic Systems and Control, ETH Zurich, 8092 Zurich, Switzerland (e-mail: alavaei@ethz.ch).

Majid Zamani is with the Computer Science Department, Ludwig Maximilian University of Munich, 80538 Munich, Germany, and also with the Computer Science Department, University of Colorado Boulder, Boulder, CO 80309 USA (e-mail: majid.zamani@colorado.edu).

Digital Object Identifier 10.1109/TCNS.2022.3186649
A synthesis framework based on barrier functions for partially observable jump diffusion systems enforcing complex properties expressed by deterministic finite automata is proposed in [29], where a prior knowledge of the estimation accuracy is not required anymore.

The proposed techniques in the abovementioned literature on partially observable systems assume that barrier functions have a certain parametric form, such as polynomial, and they search for their corresponding coefficients under certain assumptions using optimization techniques such as sum of squares programming. Although it may be easy to search for those functions for low-dimensional systems via existing tools, it will become computationally very expensive (if not impossible) to compute such functions for large-scale interconnected systems. Motivated by this challenge, in this work, we propose a compositional approach for the construction of CBFs for partially observable discrete-time stochastic control systems (also known as continuous-space POMDPs). In particular, by considering a large-scale partially observable stochastic control system as an interconnection of lower dimensional subsystems, we compute the so-called local control barrier functions (LCBFs) for subsystems along with the corresponding local controllers. We then utilize LCBFs of subsystems to compositionally construct an overall CBF for the interconnected system. In our setting, we only require that CBFs exhibit a c-martingale property, which is a relaxation of a supermartingale one. Remark that a supermartingale property often presupposes stochastic stability and vanishing noise at the equilibrium point which is not the case for the c-martingale property. Hence, finding c-martingale barrier functions is much easier than finding supermartingale ones. On the other hand, requiring only c-martingale property comes at the cost of providing guarantees for finite-time horizon, whereas the supermartingale property provides an infinite-time horizon guarantee. We now formally define the main synthesis problem of this article.

**Problem 1.1:** Given an interconnected partially observable stochastic control system, synthesize a decentralized safety controller ensuring that trajectories of the interconnected system will not enter a given unsafe region over a finite-time horizon with some lower bound on the safety probability.

Finding a solution to Problem 1.1 (if exists) is generally difficult. Here, we provide an approach that is *sound* but not *complete* in solving the problem. This means if our proposed method fails to find a controller, then a controller satisfying the safety specification may or may not exist. To the best of our knowledge, this article is the first to develop a compositional controller synthesis scheme for networks of partially observable stochastic control systems based on barrier functions. By requiring a small-gain type condition, we compositionally construct a CBF for the interconnected system via local barrier functions of subsystems.

We propose two approaches for the construction of CBFs. In the first one, LCBFs are defined over augmented systems consisting of subsystems and their estimators. This formulation makes it possible to search for LCBFs, and the overall one, without requiring explicitly the accuracies of the estimators. In the second framework, LCBFs are constructed using the estimators’ dynamics (without augmenting them with the subsystems’ dynamics), where we utilize a notion of so-called *stochastic simulation functions* (SSFs) to compute a probabilistic bound on the estimation accuracy. We propose a sum-of-squares (SOS) optimization approach to search for LCBFs in both approaches, and accordingly, to compute the corresponding controllers. In order to illustrate the effectiveness of our proposed results, we apply both approaches to an adaptive cruise control (ACC) problem.

## II. PRELIMINARIES AND PROBLEM DEFINITION

### A. Preliminaries

A probability space in this work is presented by tuple \((\Omega, \mathcal{F}, \mathbb{P})\), where \(\Omega\) is a sample space, \(\mathcal{F}\) is a sigma-algebra on \(\Omega\), and \(\mathbb{P}\) is a probability measure that assigns probabilities to events. Random variables introduced here are measurable functions of the form \(X : (\Omega, \mathcal{F}) \rightarrow (\mathbb{R}, \mathcal{B})\) such that any random variable \(X\) induces a probability measure on its space \(\mathbb{P}[A] = \mathbb{P}[X^{-1}(A)]\) for any \(A \in \mathcal{B}\). We denote the empty set by \(\emptyset\).

We call the topological space \(\mathcal{S}\) a Borel space if it is homeomorphic to a Borel subset of a Polish space. Euclidean space \(\mathbb{R}^n\), its Borel subsets endowed with a subspace topology, and hybrid spaces are examples of Borel spaces. A Borel sigma-algebra is denoted by \(\mathcal{B}(\mathcal{S})\), where any Borel space \(\mathcal{S}\) is assumed to be endowed with it. A map \(f : \mathcal{S} \rightarrow \mathcal{Y}\) is measurable whenever it is Borel measurable.

### B. Notation

The sets of non-negative and positive integers are denoted by \(\mathbb{N} := \{0, 1, 2, \ldots\}\) and \(\mathbb{N}_{>0} := \{1, 2, 3, \ldots\}\), respectively. Moreover, symbols \(\mathbb{R}\), \(\mathbb{R}_{>0}\), and \(\mathbb{R}_{>0}\) denote, respectively, the sets of real, positive, and non-negative real numbers. Given \(N\) vectors \(x_i \in \mathbb{R}^{n_i}, n_i \in \mathbb{N}_{>0}, i \in \{1, 2, \ldots, N\}\), we use \(x = [x_1; \ldots; x_N]\) to denote the corresponding column vector of the dimension \(\sum_{i=1}^N n_i\). Given any \(a \in \mathbb{R}\), \(|a|\) denotes the absolute value of \(a\). Given a vector \(x \in \mathbb{R}^n\), \(|x|\) denotes the infinity norm of \(x\), with \(|x| = \max\{|x_1|, \ldots, |x_n|\}\). The identity function and composition of functions are denoted by \(\mathbb{I}\) and the symbol \(\circ\), respectively. A function \(\kappa : \mathbb{R}_{>0} \rightarrow \mathbb{R}_{>0}\) is said to be a class \(\mathcal{K}\) function if it is continuous, strictly increasing, and \(\kappa(0) = 0\). A class \(\mathcal{K}\) function \(\kappa(\cdot)\) is said to be a class \(\mathcal{K}_\infty\) if \(\kappa(r) \rightarrow \infty\) as \(r \rightarrow \infty\). We denote the empty set by \(\emptyset\).

Given functions \(f_i : X_i \rightarrow Y_i\), for any \(i \in \{1, \ldots, N\}\), their Cartesian product \(f_1 \colon X_1 \rightarrow Y_1\) is defined as \((f_1(x_1), \ldots, f_n(x_N))\).
where:

1) \( X \subseteq \mathbb{R}^n \) is a Borel space as the state-space of the system.
2) \( U \subseteq \mathbb{R}^m \) is a Borel space as the external input space of the system;
3) \( W \subseteq \mathbb{R}^p \) is a Borel space as the internal output space of the system;
4) \( \varsigma_i, i \in \{1, 2\}, \) denote sequences of independent and identically distributed random variables from a sample space \( \Omega \) to the uncertainty set \( \mathcal{V}_i \)

\[
\varsigma_i = \{ \varsigma_i(k) : \Omega \rightarrow \mathcal{V}_i, k \in \mathbb{N} \}
\]

5) \( f : X \times U \times W \times \mathcal{V}_1 \rightarrow X \) is a measurable function characterizing the state evolution of the system;
6) \( Y_1 \subseteq \mathbb{R}^q \) is a Borel space as the internal output space of the system;
7) \( Y_2 \subseteq \mathbb{R}^r \) is a Borel space as the external output space of the system;
8) \( h_1 : X \rightarrow Y_1 \) is a measurable function that maps a state \( x \in X \) to its internal output signal \( y_1 = h_1(x) \);
9) \( h_2 : X \times \mathcal{V}_2 \rightarrow Y_2 \) is a measurable function that maps a state \( x(k) \in X \) to its external output signal \( y_2(k) = h_2(x(k), \varsigma_2(k)) \).

An evolution of the state of PO-dt-SCS \( \Sigma \) and its output for given input sequences \( v(\cdot) : \mathbb{N} \rightarrow U \) and \( w(\cdot) : \mathbb{N} \rightarrow W \) are described by

\[
\Sigma : \begin{cases}
 x(k + 1) = f(x(k), v(k), w(k), \varsigma_1(k)) \\
 y_1(k) = h_1(x(k)) \\
 y_2(k) = h_2(x(k), \varsigma_2(k))
\end{cases} \quad k \in \mathbb{N}.
\]

A PO-dt-SCS \( \Sigma \) in (1) can be equivalently represented as a partially observable Markov decision process (POMDP) [30]. Hence, we interchangeably employ terms PO-dt-SCS and POMDP in the remainder of this article.

We associate \( U \) and \( W \) with \( \mathcal{U} \) and \( \mathcal{W} \), respectively, to be collections of sequences \( \{v(k) : \Omega \rightarrow U, k \in \mathbb{N}\} \) and \( \{w(k) : \Omega \rightarrow W, k \in \mathbb{N}\} \), in which \( v(k) \) and \( w(k) \) are independent of \( \varsigma_l(l) \) for any \( k, l \in \mathbb{N}, l \geq k \) and \( i \in \{1, 2\} \). The random sequences \( x_{\text{aux}} : \Omega \times \mathbb{N} \rightarrow X, y_{1, \text{aux}} : \Omega \times \mathbb{N} \rightarrow Y_1, \) and \( y_{2, \text{aux}} : \Omega \times \mathbb{N} \rightarrow Y_2 \) satisfying (2) are called, respectively, the solution process, internal output, and external output processes of \( \Sigma \), respectively, under an external input \( v \), an internal input \( w \), and an initial state \( \alpha \). The external output signal \( y_1 \) and the internal input signal \( w \) represent the interconnections between subsystems, where \( y_1 \) is the information that each subsystem sends to its neighboring subsystems and \( w \) is the information fed to each subsystem by its neighbors.

Since the main goal of this work is to study networks of systems, the tuple representing interconnected systems, not containing internal inputs and outputs, is \( \Sigma = (X, U, s_1, f, Y, h, s_2) \),

where \( f : X \times U \times \mathcal{V}_1 \rightarrow X \), and

\[
\Sigma : \begin{cases}
 x(k + 1) = f(x(k), v(k), \varsigma_1(k)) \\
 y(k) = h(x(k), \varsigma_2(k)), \quad k \in \mathbb{N}.
\end{cases}
\]

For the sake of controller synthesis using CBFs, which are explained later in detail, we raise the following assumption on the existence of an estimator that estimates the state of the PO-dt-SCS in (2).

**Assumption 2.2:** Consider a PO-dt-SCS \( \Sigma \) as in (2). States of \( \Sigma \) can be estimated by a proper estimator \( \hat{\Sigma} \), which is characterized by the tuple \( \hat{\Sigma} = (X, U, W, f, Y_1, Y_2, h_1) \) and represented in the following form:

\[
\hat{\Sigma} : \begin{cases}
 \hat{x}(k + 1) = f(\hat{x}(k), v(k), \hat{w}(k), y_2(k)) \\
 \hat{y}_1(k) = h_1(\hat{x}(k))
\end{cases}
\]

where \( v \) and \( y_2 \) are external input and output signals of \( \Sigma \), and \( \hat{w} \) is the internal input signal coming from other estimators. We explain later how \( \hat{w} \) is being fed by the estimators of other neighboring subsystems.

There exist numerous results in the relevant literature for designing the estimator in (4) (cf. [31]–[33]).

In the next section, we introduce LCBFs and CBFs for, respectively, POMDPs (with internal and external inputs) and interconnected POMDPs (without internal inputs and outputs).

### III. (LOCAL) CONTROL BARRIER FUNCTIONS

First, we define (local) control barrier functions (L)CBF over an augmented system consisting of the stochastic (sub)system’s and its estimator’s dynamics. This formulation enables one to search for (local) CBFs with no prior knowledge of the estimation accuracy. Second, we formulate (local) CBFs over only the estimator’s dynamics by utilizing a given probability bound on the estimation accuracy computed via a notion of so-called SSFs.

#### A. Notion of (L)CBF Without Using Estimation Accuracy

Here, we first define the augmented process \( [x(k); \hat{x}(k)] \), where \( x(k) \) and \( \hat{x}(k) \) are the solution processes of subsystems \( \Sigma \) in (2) and their estimators \( \hat{\Sigma} \) in (4), respectively. The corresponding augmented stochastic subsystem \( \hat{\Sigma} \) can be defined as

\[
\hat{\Sigma} : \begin{cases}
 x(k + 1) = [f(x(k), v(k), w(k), \varsigma_1(k))] \\
 \hat{x}(k + 1) = [f(\hat{x}(k), v(k), \hat{w}(k), y_2(k))]
\end{cases}
\]

Now, the LCBF is defined for system \( \hat{\Sigma} \) in (5).

**Remark 3.1:** Using the augmented system \( \hat{\Sigma} \) allows us to provide one of the main results of the article without requiring explicitly any prior knowledge of the probabilistic distance between the actual and estimated states. This provides flexibility in designing estimators via any existing method.

We now formally define LCBFs constructed over the augmented system \( \hat{\Sigma} \).

**Definition 3.2:** Consider a POMDP \( \Sigma \) as in (2), its estimator \( \hat{\Sigma} \) in (4), and the resulting augmented system \( \hat{\Sigma} \) in (5). Let
$X_a, X_b \subseteq X$ represent some initial and unsafe regions, respectively. A function $B : X \times X \to \mathbb{R}_{\geq 0}$ is called a LCBF for $\Sigma$ if there exist constants $\bar{\psi}, \bar{\gamma} \in \mathbb{R}_{\geq 0}$ and $\bar{\lambda} \in \mathbb{R}_{> 0}$, such that

1) $\forall (x, \hat{x}) \in X \times X$

$$B(x, \hat{x}) \geq \alpha \left( \left\| h_1(x) \right\|_{h_1(\hat{x})}^{\bar{\lambda}} \right)$$

(6)

2) $\forall (x, \hat{x}) \in X_a \times X_a$

$$B(x, \hat{x}) \leq \bar{\gamma}$$

(7)

3) $\forall (x, \hat{x}) \in X_b \times X$

$$B(x, \hat{x}) \geq \bar{\lambda}$$

(8)

4) $\forall \bar{x}(k) \in X \forall \bar{w}(k) \in W, \exists \bar{v}(k) \in U, \text{such that } \forall x(k) \in X, \forall w(k) \in W$

$$\mathbb{E} \left[ B \left( f(x(k), v(k), w(k), \varsigma_1(k)), \hat{f}(\bar{x}(k), v(k), \bar{w}(k), y_2(k)) \right) \right] \leq \max \left\{ \bar{\kappa} B(x(k), \hat{x}(k)), \rho \left( \left\| \bar{w}(k) \right\|_{\bar{w}(\hat{x})}^{\bar{\psi}} \right), \bar{\psi} \right\}$$

(9)

for some $\alpha \in \mathcal{K}_{\infty}$, $\rho \in \mathcal{K}_{\infty} \cup \{0\}$, and $0 < \bar{\kappa} < 1$. Definition 3.2 can also be stated for interconnected systems without internal inputs and outputs by eliminating all the terms related to the internal input $w$, its estimation $\bar{w}$, internal output $h_1(x)$, and its estimation $h_1(\hat{x})$ as defined below.

**Definition 3.3:** Consider an (interconnected) POMDP $\Sigma$ as in (3), its estimator $\bar{\Sigma}$ also without internal inputs and outputs, and the augmented system $\Sigma = [\Sigma; \bar{\Sigma}]$. Let $X_a, X_b \subseteq X$, respectively, represent initial and unsafe regions. A function $B : X \times X \to \mathbb{R}_{\geq 0}$ is called a CBF for $\Sigma$ if there exist constants $\bar{\psi}, \bar{\gamma} \in \mathbb{R}_{\geq 0}$ and $\bar{\lambda} \in \mathbb{R}_{> 0}$, such that $\gamma < \bar{\lambda}$, and

1) $\forall (x, \hat{x}) \in X_a \times X_a$

$$B(x, \hat{x}) \leq \bar{\gamma}$$

(10)

2) $\forall (x, \hat{x}) \in X_b \times X$

$$B(x, \hat{x}) \geq \bar{\lambda}$$

(11)

3) and $\forall \bar{x}(k) \in X, \exists \bar{v}(k) \in U, \text{such that } \forall x(k) \in X$

$$\mathbb{E} \left[ B \left( f(x(k), v(k), \varsigma_1(k)), \hat{f}(\bar{x}(k), v(k), \bar{v}(k)) \right) \right] \leq \max \left\{ \kappa B(x(k), \hat{x}(k)), \psi \right\}$$

(12)

for some $0 < \kappa < 1$.

**Remark 3.4:** Note that the compositionality conditions in this article are based on the so-called max-type small-gain approach. Thus, the upper bound in (12) is in the max form and the overall CBF is the maximum of LCBF of subsystems under some scaling (this is explained further in Section V).

**Remark 3.5:** Note that we need the condition $\gamma < \bar{\lambda}$ (i.e., $X_a \cap X_b = \emptyset$) in order to provide a meaningful probability in Theorem 3.6 later. This requirement is only for the interconnected system and not for subsystems. In particular, LCBFs are mainly utilized for the compositional construction of CBFs over interconnected systems and are not directly employed for ensuring the probability of safety satisfaction. The above definition associates a policy $\eta : X \to U$ with a CBF, where $X$ here is the state set of the estimator $\bar{\Sigma}$. Definition 3.3 gives such a policy according to the existential quantifier over the input for any estimator’s state $\bar{x} \in X$.

The next theorem shows the usefulness of having a CBF to quantify an upper bound on the exit probability (i.e., the probability that the solution process of the interconnected system reaches the unsafe region in a finite-time horizon) of POMDP (without internal inputs and outputs).

**Theorem 3.6:** Let $\Sigma = (X, U, \varsigma_1, f, Y, h, \varsigma_2)$ be a POMDP (without internal inputs and outputs) and $\bar{\Sigma}$ be its corresponding estimator. Suppose $B$ is a CBF according to Definition 3.3 with a policy $\eta : X \to U$. Then, the probability that the solution process of $\Sigma$ starts from any initial states $x(0) = a \in X_a$ and reaches $X_b$ under the control policy $\eta$ within a time horizon $[0, T_d]$ is formally upper bounded as

$$\mathbb{P} \left[ x_{av}(k) \in X_b \text{ for some } k \in [0, T_d] \mid a, \bar{v} \right] \leq \delta$$

(13)

where

$$\delta := \left\{ \begin{array}{ll}
1 - \left( 1 - \frac{2}{\kappa} \right) \left( 1 - \frac{\psi}{1 - \kappa} \right) T_d, & \text{if } \lambda \geq \frac{\psi}{1 - \kappa} \\
\frac{2\kappa T_d + \left( \frac{\psi}{1 - \kappa} \right) (1 - \kappa T_d), }{1 - \kappa} & \text{if } \lambda < \frac{\psi}{1 - \kappa}.
\end{array} \right.$$

(14)

The proof of Theorem 3.6 is provided in the Appendix.

**Remark 3.7:** Utilizing the augmented system $\Sigma$ as in (5) provides us with the results in Theorem 3.6 without requiring the estimation accuracy explicitly. This allows more flexibility in designing the estimator and potentially results in tighter upper bounds.

In the next subsection, we formulate CBFs only over the estimators’ dynamics by utilizing a probability bound on the estimation accuracy.

**B. Notion of (L)CBF Using Estimation Accuracy**

Given an estimator with a probabilistic guarantee on the accuracy of the estimation, we propose an approach to construct a CBF defined only over the states of the estimator $\bar{\Sigma}$. For a given time horizon $T_d$, we assume the probabilistic bound on the accuracy of the estimator is given by [34]

$$\forall \epsilon > 0, \exists \theta \in (0, 1] \text{, such that }$$

$$\mathbb{P} \left[ \sup_{0 \leq k \leq T_d} \left\| x_{av}(k) - \bar{x}_{av}(k) \right\| < \epsilon \mid a, \bar{v} \right] \geq 1 - \theta$$

(15)

for any $a, \bar{a} \in X$ and any $v \in \mathcal{U}$. In order to quantify the distance (also known as error) between a system’s state and its estimation, we employ notions of so-called stochastic (pseudo)-simulation functions (SPSFs). To do so, we first introduce SPSFs for POMDPs with both internal and external inputs. We then define SPSFs for interconnected POMDPs without internal inputs and outputs.

**Definition 3.8:** Consider a POMDP $\Sigma$ in (2) and its corresponding estimator $\bar{\Sigma}$ in (4). A function $\phi : X \times X \to \mathbb{R}_{\geq 0}$ is called an SPSF from $\bar{\Sigma}$ to $\Sigma$ if
1) ∀x ∈ X ∀\hat{x} ∈ X, ε(||x - \hat{x}||) ≤ φ(x, \hat{x})
2) ∀\hat{x}(k) ∈ X, ∀\hat{w}(k) ∈ W, ∀v(k) ∈ U, ∀x(k) ∈ X and ∀ w(k) ∈ W,
   \[ \mathbb{E}[\phi(f(x(k), v(k), w(k), s_1(k))) \mid x(k), \hat{x}(k), v(k), \hat{w}(k)] \leq \max \left\{ \bar{\mu} \phi(x(k), \hat{x}(k)), 0(||w(k) - \hat{w}(k)||, \delta) \right\} \]
   for some 0 < \bar{\mu} < 1, ε ∈ K_\infty, φ ∈ K_\infty \cup \{0\}, and \delta ∈ \mathbb{R}_>.

Definition 3.9: Consider an (interconnected) POMDP Σ = (X, U, s_1, f, Y, h, s_2) and its estimator \( \hat{\Sigma} \). A function \( \phi : X \times X \to \mathbb{R}_{\geq0} \) is called an SSF from \( \hat{\Sigma} \) to Σ if

1) ∀x ∈ X ∀\hat{x} ∈ X, ε(||x - \hat{x}||) ≤ φ(x, \hat{x})
2) ∀\hat{x}(k) ∈ X ∀v(k) ∈ U, and ∀x(k) ∈ X
   \[ \mathbb{E}[\phi(f(x(k), v(k), s_1(k)), f(\hat{x}(k), v(k), y(k))) \mid x(k), \hat{x}(k), v(k)] \leq \max \{ \mu \phi(x(k), \hat{x}(k), \gamma) \} \]
   for some 0 < μ < 1, ε ∈ K_\infty, and γ ∈ \mathbb{R}_>.

The next theorem shows how an SSF can be employed to obtain the probability bound on the estimation accuracy.

Theorem 3.10: Consider a POMDP Σ in (3), its estimator \( \hat{\Sigma} \) in (4) (without internal inputs and outputs), and ε > 0. Suppose \( \phi \) is an SSF from \( \hat{\Sigma} \) to Σ. For any v ∈ U, and for any random variables a and \( \hat{a} \) as initial states of Σ and \( \hat{\Sigma} \), respectively, the following inequality holds:

\[ \mathbb{P} \left[ \sup_{0 \leq k \leq T_d} \| x_{a,v}(k) - \hat{x}_{a,v}(k) \| \geq \varepsilon \mid a, \hat{a}, v \right] \leq \theta \]

where

\[ \theta := \left\{ 1 - \left( 1 - \frac{\phi(a, \hat{a})}{\varepsilon} \right) \left( 1 - \frac{\varepsilon}{\varepsilon} \right) T_d, \right. \quad \text{if} \; \varepsilon(\varepsilon) \geq \frac{\varepsilon}{1 - \mu} \right\} \]
\[ \left. + \frac{\phi(a, \hat{a})}{(1 - \mu) \varepsilon} (1 - \mu T_d), \quad \text{if} \; \varepsilon(\varepsilon) < \frac{\varepsilon}{1 - \mu} \right\}. \]

(16)

The proof of Theorem 3.10 is provided in Appendix 3.

We now propose our second formulation of CBFs defined only over the estimators’ dynamics as the following.

Definition 3.11: Consider a POMDP Σ as in (2), its estimator \( \hat{\Sigma} \), and ε > 0. Let X_a, X_b ⊆ X denote, respectively, initial and unsafe sets. Let us define X' := {\( \hat{x} ∈ X \mid \exists x ∈ X_b, \| \hat{x} - x \| ≤ \varepsilon \)} (i.e., unsafe set for \( \hat{\Sigma} \)). A function \( \hat{B} : X \to \mathbb{R}_{\geq0} \) is called a LCBF for \( \hat{\Sigma} \) if there exist constants \( \bar{\psi}, \gamma \in \mathbb{R}_{\geq0} \) and \( \lambda \in \mathbb{R}_{>0} \), such that

1) ∀x ∈ X,
   \[ \hat{B}(x) ≥ \alpha(\|h_1(x)\|^2) \]
   (17)
2) ∀x ∈ X_a,
   \[ \hat{B}(x) ≤ \bar{\gamma} \]
   (18)
3) ∀x ∈ X_b,
   \[ \hat{B}(x) ≥ \bar{\lambda} \]
   (19)
4) and ∀\hat{x}(k) ∈ X, ∀\hat{w}(k) ∈ W, ∀v(k) ∈ U, such that ∀x(k) ∈ X
   \[ \mathbb{E}[\hat{B}(f(\hat{x}(k), v(k), \hat{w}(k), h_2(x(k), s_2(k)))) \mid \hat{x}(k), v(k), \hat{w}(k), x(k)] ≤ \max \{ \bar{\rho} B(\hat{x}(k)), \rho(\|\hat{w}(k)\|^2), \]
   \[ x(\|x(k) - \hat{x}(k)\|^2), \hat{x}(k) \} \]
   (20)
for some 0 < \bar{\rho} < 1, \alpha, \lambda ∈ K_\infty, and \rho ∈ K_\infty \cup \{0\}.

We now modify Definition 3.11 and present it for the interconnected POMDPs as the following.

Definition 3.12: Consider an (interconnected) POMDP Σ = (X, U, s_1, f, Y, h, s_2), its estimator \( \hat{\Sigma} \) without internal inputs and outputs, and ε > 0. Let X_a, X_b ⊆ X denote, respectively, initial and unsafe sets. Let us define \( X'_a := \{ \hat{x} ∈ X \mid \exists x ∈ X_b, \| \hat{x} - x \| ≤ \varepsilon \} \). A function \( \hat{B} : X \to \mathbb{R}_{\geq0} \) is called a CBF for \( \hat{\Sigma} \) if there exist constants \( \hat{\psi}, \gamma \in \mathbb{R}_{\geq0} \) and \( \lambda \in \mathbb{R}_{>0} \) such that \( \gamma ≤ \lambda \) and

1) ∀x ∈ X_a, \( \hat{B}(x) ≤ \gamma \)
2) ∀x ∈ X'_a, \( \hat{B}(x) ≥ \lambda \)
3) and ∀\hat{x}(k) ∈ X, ∀v(k) ∈ U, such that ∀x(k) ∈ X
   \[ \mathbb{E}[\hat{B}(f(\hat{x}(k), v(k), h(x(k), s_2(k)))) \mid \hat{x}(k), v(k), x(k)] ≤ \max \{ \kappa B(\hat{x}(k)), \hat{x}(\|x(k) - \hat{x}(k)\|^2), \hat{x}(k) \}
   \]
   (21)
for some 0 < \kappa < 1, and \( \kappa ∈ K_\infty \).

In the next Theorem, we provide an upper bound on the exit probability of POMDP using the estimation accuracy.

Theorem 3.13: Let Σ = (X, U, s_1, f, Y, h, s_2) be a POMDP without internal inputs and outputs, Σ be its estimator with accuracy ε, and a probability bound on the estimation accuracy \( \theta \), as in Theorem 3.10. Suppose \( \hat{B} \) is a CBF for \( \hat{\Sigma} \) as in Definition 3.12 with a policy \( \eta : X \to U \). Then, the probability that the solution process of Σ starts from any initial state \( x(0) = a ∈ X_a \) and not reaches \( X_b \) under the control policy \( \eta \) within a time horizon \([0, T_d] \) is lower bounded as

\[ \mathbb{P} \left[ x_{a,v}(k) \notin X_b \forall k ∈ [0, T_d] \mid a, v \right] ≥ (1 - \delta)(1 - \theta) \]

(21)
where \( \delta \) is computed as in (16), and \( \delta \) is computed as in (14) with \( \psi \) in (14) being replaced with a constant \( \hat{\psi} ≥ \hat{x}(\|x\|^2) + \psi \).

The proof of Theorem 3.13 is provided in the Appendix.

Remark 3.14: Note that the first proposed approach does not require a prior knowledge of the estimation accuracy, which gives flexibility on the estimator design. Moreover, in the first approach the computation of the exit probability can be done in one shot without utilizing SSFs and, hence, be less conservative. However, computational complexity in the first approach is more than the second one since the CBF should be constructed over the augmented system.
In the next sections, we analyze networks of POMDP and discuss under which conditions one can construct a CBF of an interconnected system based on LCBF of its subsystems.

IV. INTERCONNECTED POMDP

We consider a collection of partially observable stochastic control subsystems and their estimators as
\[
\Sigma_i = (X_i, U_i, W_i, \xi_i, f_i, Y_{1i}, Y_{2i}, h_{1i}, h_{2i}, \varsigma_i)
\]
\[
\tilde{\Sigma}_i = (X_i, U_i, W_i, \tilde{f}_i, Y_{1i}, Y_{2i}, h_{1i}), \ i \in \{1, \ldots, N\}
\]
where internal inputs and outputs are partitioned as
\[
w_i = [w_{i1}; \ldots; w_{i(i-1)}; w_{i(i+1)}; \ldots; w_{iN}]
\]
\[
y_{1i} = [y_{11}; \ldots; y_{1(i-1)}; y_{1(i+1)}; \ldots; y_{1N}]
\]
and their internal output spaces and functions are of the form
\[
Y_{1i} = \prod_{j=1, j \neq i}^N Y_{ij}
\]
where \(i \neq j\) are internal outputs, which are employed for the sake of interconnections. If there is a connection from \(\tilde{\Sigma}_j\) to \(\tilde{\Sigma}_i\), we assume that \(w_{ij}\) is equal to \(y_{ij}\). Otherwise, the connecting output function is identically zero, i.e., \(h_{1i} \equiv 0\). The same interconnections hold for the estimators. If there is a connection from \(\tilde{\Sigma}_j\) to \(\tilde{\Sigma}_i\), we assume that \(\tilde{u}_{ij}\) is equal to \(\tilde{y}_{ij}\). Otherwise, the connecting output function is identically zero, i.e., \(h_{1i} \equiv 0\). Now we define interconnected partially observable stochastic control systems as follows.

Definition 4.1: Consider \(N \in \mathbb{N}_1\) POMDPs \(\Sigma_i = (X_i, U_i, W_i, \xi_i, f_i, Y_{1i}, Y_{2i}, h_{1i}, h_{2i}, \varsigma_i), i \in \{1, \ldots, N\}\), with the input–output configuration as in (22)–(23). The interconnection of \(\Sigma_i\), for any \(i \in \{1, \ldots, N\}\), is the interconnected POMDP \(\Sigma = (X, U, \xi_1, f, Y, h, \varsigma)\), denoted by \(\mathcal{T}(\Sigma_1, \ldots, \Sigma_N)\), such that \(X := \prod_{i=1}^N X_i, U := \prod_{i=1}^N U_i, \xi_1 = [\xi_1; \ldots; \xi_N], f := \prod_{i=1}^N f_i, Y := \prod_{i=1}^N Y_i, h := \prod_{i=1}^N h_i\), and \(\varsigma = [\varsigma_1; \ldots; \varsigma_N]\), subjected to the following constraint:
\[
\forall i, j \in \{1, \ldots, N\}, i \neq j : w_{ij} = y_{ij}, Y_{ij} \subseteq W_{ji}.
\]
Similarly, we define the interconnection of estimators as follows.

Definition 4.2: Consider \(N \in \mathbb{N}_1\) estimators \(\tilde{\Sigma}_i = (X_i, U_i, W_i, \tilde{f}_i, Y_{1i}, Y_{2i}, h_{1i}), i \in \{1, \ldots, N\}\), with the input–output configuration as in (22)–(23). The interconnection of \(\tilde{\Sigma}_i\), for any \(i \in \{1, \ldots, N\}\), is the interconnected estimator \(\tilde{\Sigma} = (X, U, \tilde{f}, Y), \tilde{T}(\tilde{\Sigma}_1, \ldots, \tilde{\Sigma}_N)\), such that \(X := \prod_{i=1}^N X_i, U := \prod_{i=1}^N U_i, \tilde{f} := \prod_{i=1}^N \tilde{f}_i\), and \(Y := \prod_{i=1}^N Y_i\), subject to the following constraint:
\[
\forall i, j \in \{1, \ldots, N\}, i \neq j : \tilde{w}_{ij} = \tilde{y}_{ij}, Y_{ij} \subseteq W_{ji}.
\]

An example of the interconnection of two POMDPs \(\Sigma_1\) and \(\Sigma_2\) is illustrated in Fig. 1.

V. COMPOSITIONAL CONSTRUCTION OF CBF

In this section, we analyze networks of POMDP and provide a compositional approach to construct a CBF of an interconnected POMDP based on LCBF of its subsystems. For \(i \in \{1, \ldots, N\}\), consider the PO-dt-SCS \(\Sigma_i\) in (2), its corresponding estimator \(\tilde{\Sigma}_i\) in (4), and the augmented system \(\Sigma\) in (5). Assume there exists an LCBF \(\mathcal{B}\), as defined in Definition 3.2 or 3.11 with functions \(\sigma_i \in \mathcal{K}_\infty, \rho_i \in \mathcal{K}_\infty \cup \{0\}\) and constants \(\lambda_i, \psi_i \in \mathbb{R}_{>0}, \gamma_i \in \mathbb{R}_{>0}\), and \(0 < \kappa_i < 1\). Now we raise the following small-gain assumption that is essential for the compositional results of this section.

Assumption 5.1: Assume that \(\mathcal{K}_\infty\) functions \(\kappa_{ij}\) defined as
\[
\tilde{\kappa}_{ij} := \begin{cases} \kappa_{ij}, & \text{if } i = j, \\ \rho_{ij} \circ \alpha_{ij}^{-1}, & \text{if } i \neq j, \end{cases}
\]
satisfy
\[
\tilde{\kappa}_{1i}, \tilde{\kappa}_{2j}, \ldots, \tilde{\kappa}_{N-1i}, \tilde{\kappa}_{Ni} < \mathcal{I}_d
\]
for all sequences \((i_1, \ldots, i_r) \in \{1, \ldots, N\}^r\) and \(r \in \{1, \ldots, N\}\).

Remark 5.2: The small-gain condition (24) implicitly states that in every strongly connected component of the graph representing the topology of the interconnected system, the effect of strong interconnections can be compensated by weak ones as long as their composition is less than identity.

Remark 5.3: Note that the small-gain condition (24) is a standard one in studying the stability of large-scale interconnected systems via ISS Lyapunov functions [35], [36]. This condition can be readily satisfied if each \(\tilde{\kappa}_{ij}\) is less than identity \((\tilde{\kappa}_{ij} < \mathcal{I}_d \forall i, j \in \{1, \ldots, N\}\)). Since each \(\tilde{\kappa}_{ij}\) is less than identity \((0 < \tilde{\kappa}_{ij} < 1 \forall i, j \in \{1, \ldots, N\}\)) by Definitions 3.2 or 3.11, one only needs to satisfy \(\rho_{ij} \circ \alpha_{ij}^{-1} < \mathcal{I}_d \forall i, j \in \{1, \ldots, N\}, i \neq j\).

The small-gain condition (24) implies the existence of \(\mathcal{K}_\infty\) functions \(\sigma_i > 0\) [37, Th. 5.5], satisfying
\[
\max_{i,j} [\sigma_i^{-1} \circ \tilde{\kappa}_{ij} \circ \sigma_j] < \mathcal{I}_d, \quad i, j \in \{1, \ldots, N\}.
\]

In the next theorem, we show that if Assumption 5.1 holds and \(\max\{\sigma_i^{-1}\} \equiv \mathcal{I}_d\) (in order to employ Jensen’s inequality), then one can compute a CBF for the interconnected system \(\Sigma\) as in Definition 3.3 in a compositional fashion.

Theorem 5.4: Consider the interconnected POMDP \(\Sigma = \mathcal{T}(\Sigma_1, \ldots, \Sigma_N)\) induced by \(N \in \mathbb{N}_1\) subsystems \(\Sigma_i\). Suppose that for each \(\Sigma_i\), there exists an estimator \(\tilde{\Sigma}_i\) together with a corresponding LCBF \(\mathcal{B}\), as defined in Definition 3.2 with initial and unsafe sets \(X_{a_i}\) and \(X_{b_i}\), respectively. If Assumption 5.1
holds and \( \max_i \sigma_i^{-1} \) for \( \sigma_i \) as in (25) is concave and

\[
\max_i \{ \sigma_i^{-1}(\gamma_i) \} < \max_i \{ \sigma_i^{-1}(\hat{\lambda}_i) \}
\]  

(26)

then, function \( B(x, \hat{x}) \) defined as

\[
B(x, \hat{x}) := \max_i \{ \sigma_i^{-1}(B_i(x_i, \hat{x}_i)) \}
\]  

(27)

is a CBF for the augmented system \( \bar{\Sigma} = [\Sigma \ \bar{\Sigma}] \) with initial and unsafe sets \( X_a = \prod_{i=1}^N X_{a_i} \), \( X_b = \prod_{i=1}^N X_{b_i} \), respectively.

The proof of Theorem 5.4 is provided in the Appendix.

**Remark 5.5:** Note that inequality (26) in general is not very restrictive. Indeed, functions \( \sigma_i \) in (25) play the role of rescaling LCBFs of the individual subsystems while normalizing the effect of internal gains of other subsystems (see [36] for a similar discussion in the context of Lyapunov stability). Due to this scaling, one can expect that such an inequality holds in many applications.

**Remark 5.6:** The \( K_\infty \) functions \( \sigma_i, i \in \{1, \ldots, N\} \), can always be chosen as identity provided that \( \bar{\gamma}_{ij} < I_{d} \forall i, j \in \{1, \ldots, N\} \), for functions \( \bar{\gamma}_{ij} \) defined in Assumption 5.1.

Similarly, we propose the next theorem to compute a CBF for an interconnected system \( \bar{\Sigma} \) as in Definition 3.12 in a compositional way based on LCBFs of subsystems.

**Theorem 5.7:** Consider an interconnected POMDP \( \Sigma = I(\Sigma_1, \ldots, \Sigma_N) \) induced by \( N \in \mathbb{N}_{>1} \) subsystems \( \Sigma_i \). Suppose that for each \( \Sigma_i \), there exists an estimator \( \hat{\Sigma}_i \) together with a corresponding LCBF \( B_i \) as defined in Definition 3.11 with initial and unsafe sets \( X_{a_i} \) and \( X_{b_i}^* \), respectively. If Assumption 5.1 holds and \( \max_i \sigma_i^{-1} \) for \( \sigma_i \) as in (25) is concave and

\[
\max_i \{ \sigma_i^{-1}(\gamma_i) \} < \max_i \{ \sigma_i^{-1}(\hat{\lambda}_i) \}
\]  

(28)

then, function \( B(x) \) defined as

\[
B(x) := \max_i \{ \sigma_i^{-1}(B_i(x_i)) \}
\]  

(29)

is a CBF for the estimator \( \bar{\Sigma} = I(\bar{\Sigma}_1, \ldots, \bar{\Sigma}_N) \) with initial and unsafe sets \( X_a = \prod_{i=1}^N X_{a_i} \), \( X_b = \prod_{i=1}^N X_{b_i} \), respectively.

The proof of Theorem 5.7 follows the same reasoning as that of Theorem 5.4 and is omitted here due to lack of space.

**Remark 5.8:** In the case of sum-of-squares optimization approach, the computational complexity of finding polynomial-type local barrier functions depends on both the degree of polynomials and the number of state variables. One can easily see that for fixed degrees of polynomials, the required computations grow polynomially with respect to the dimension of the (augmented) subsystems [38]. Furthermore, the computational complexity of finding a CBF for the interconnected system is linear with respect to the number of subsystems. In the counter example guided inductive synthesis (CEGIS) approach, due to its iterative nature and lack of guarantee on the termination, it is difficult to provide any analysis on the computational complexity with respect to the dimension of subsystems. Evidently in both SOS and CEGIS approaches, the computational complexity is independent of the time horizon \( T_f \).

Finally, we provide an approach to compositionally construct an SSF for an interconnected POMDP \( \Sigma \) based on LCBFs of its subsystems. Note that the constructed SSF is one of the main ingredients used in Theorem 3.13. First, we raise the following small-gain assumption.

**Assumption 5.9:** Assume that \( K_\infty \) functions \( \mu_{ij} \) defined as

\[
\mu_{ij} := \begin{cases} \hat{\mu}_{ij}, & \text{if } i = j, \\ \hat{\theta}_i \circ \sigma_j^{-1}, & \text{if } i \neq j, \end{cases} \forall i, j \in \{1, \ldots, N\}
\]  

(30)

for all sequences \( (i_1, \ldots, i_r) \) \( \in \{1, \ldots, N\}^r \) and \( r \in \{1, \ldots, N\} \).

The small-gain condition (30) implies the existence of \( K_\infty \) functions \( \zeta_i > 0 \) [37, Th. 5.5], satisfying

\[
\max_i \{ \zeta_i^{-1} \circ \mu_{ij} \circ \zeta_j \} < I_{d}, \ i, j = \{1, \ldots, N\}. \tag{31}
\]

In the next proposition, we show that if Assumption 5.9 holds and \( \max_i \zeta_i^{-1} \) is concave, then we can compositionally construct an SSF for an interconnected system based on LCBFs of its subsystems.

**Proposition 5.10:** Consider an interconnected POMDP \( \Sigma = I(\Sigma_1, \ldots, \Sigma_N) \) induced by \( N \in \mathbb{N}_{>1} \) subsystems \( \Sigma_i \). Suppose that for each \( \Sigma_i \), there exists an estimator \( \hat{\Sigma}_i \) together with a corresponding SSF \( \phi_i(x_i, \hat{x}_i) \). If Assumption 5.9 holds and \( \max_i \zeta_i^{-1} \) for \( \zeta_i \) as in (31) is concave, then the function \( \phi(x, \hat{x}) \) defined as

\[
\phi(x, \hat{x}) := \max_i \{ \zeta_i^{-1}(\phi_i(x_i, \hat{x}_i)) \}
\]

is an SSF from \( \bar{\Sigma} = I(\bar{\Sigma}_1, \ldots, \bar{\Sigma}_N) \) to \( \Sigma = I(\Sigma_1, \ldots, \Sigma_N) \), as defined in Definition 3.9, with

\[
\mu(s) = \max_{i,j} \{ \zeta_i^{-1} \circ \hat{\mu}_{ij} \circ \zeta_j(s) \}, \ i, j = \{1, \ldots, N\}
\]

\[
c = \max_i \zeta_i^{-1}(\bar{\gamma}_i).
\]

The proof of Proposition 5.10 follows the same reasoning as that of Theorem 5.4 and is omitted here.

**VI. CASE STUDY**

In this section, we illustrate our proposed results by applying them to an ACC system consisting of \( N \) vehicles in a platoon (see Fig. 2). This model is adapted from [39]. The evolution of states can be described by the interconnected PO-dt-SCS

\[
\Sigma: \begin{cases} x(k+1) = \bar{A}x(k) + \bar{B}u(k) + \zeta_1(k) \\ y(k) = \bar{C}x(k) + \zeta_2(k) \end{cases}
\]

where \( \bar{A} \) is a block matrix with diagonal blocks \( A \), and off-diagonal blocks \( A_{ij(i-1)} = A_{w}, i \in \{2, \ldots, N\}, \) where
The functions and constants associated with this SPSF are required for the compositionality result. By taking \( \sigma_i(s) = s, i \in \{1, \ldots, N\} \), condition (24) and, as a result, condition (25) are always satisfied without any restriction on the number of vehicles. Hence, \( B(x, \dot{x}) = \max_i B_i(x_i, \dot{x}_i) \) is a CBF for \( \Sigma \) satisfying conditions in Definition 3.3 with \( \gamma = 0.1, \lambda = 2, \kappa = 0.95 \), and \( \psi = 0.001 \). By employing Theorem 3.6, one can guarantee that states of the interconnected system starting from \( X_0 \) remain in the safe set \( X \setminus X_0 \) within the time horizon \( T_d = 60 \) with a probability of at least 92.19\% (i.e., \( 1 - \delta = 0.9219 \)). Closed-loop state and input trajectories of a representative vehicle with different noise realizations are illustrated in Fig. 3 with only 10 trajectories. We now construct the LCBF \( B_i(x_i) \) of an order 4 for the estimator, as described in Section III-B, and compute its corresponding controller as:

\[
v_i(d_i, \hat{v}_i, \dot{v}_{i-1}) = 0.08d_i - 0.9\hat{v}_i + 0.02\dot{v}_{i-1} - 0.1 \tag{33}
\]

for \( i \in \{1, \ldots, N\} \) with a computation time of about 2 min. The corresponding constants and functions in Definition 3.11 are quantified as \( \sigma_i(s) = 10^{-5}s, s \in \mathbb{R}_{\geq 0}, \gamma_i = 0.1, \lambda_i = 2, \kappa_i = 0.95, \rho_i(s) = 2 \times 10^{-8}s, s \in \mathbb{R}_{\geq 0}, \psi_i = 0.001 \), and \( \varphi_i(s) = 10^{-6}s, s \in \mathbb{R}_{\geq 0} \). Similar to the first method, we check the small gain condition (24) for the compositionality result. By taking \( \sigma_i(s) = s, i \in \{1, \ldots, N\} \), condition (24) and, as a result, condition (25) are both satisfied. Hence, \( B(\dot{x}) = \max_i B_i(x_i) \) is a CBF for \( \Sigma \) satisfying conditions in Definition 3.12 with \( \gamma = 0.1, \lambda = 2, \kappa = 0.95, \psi = 0.001 \), and \( \varphi_i(s) = 10^{-6}s, s \in \mathbb{R}_{\geq 0} \). By employing the result of Theorem 3.6, one can guarantee that the states of the estimator, with accuracy \( \epsilon = 0.01 \), starting from \( X_0 \) will not reach \( X_0^c \) within the time horizon \( T_d = 60 \) with a probability of at least 92.19\% (i.e., \( 1 - \delta = 0.9219 \)). Now, in order to compute the exit probability bound for the interconnected system, we search for an SPDF of a quadratic form \( \Phi_i(x_i, \dot{x}_i) = (x_i - \bar{x}_i)^T M (x_i - \bar{x}_i) \), where \( M \) is a positive-definite matrix. Since the dynamic of the system is linear, the conditions in Definition 3.8 reduce to solving the following matrix inequality:

\[
(1 + 2/\bar{\pi})(A - \kappa C) M (A - \kappa C) \leq \mu M
\]

where \( K \) is the estimator gain, and \( \bar{\pi} > 0 \). By using the tool YALMIP [41], we compute \( M = \begin{bmatrix} 0.0257 & 0.0259 \\ 0.0259 & 0.0262 \end{bmatrix} \), with \( \bar{\pi} = 1 \). The functions and constants associated with this SPDF are computed by following the compositional construction method for linear systems introduced in [42, Th. 6.10] as \( \varepsilon(s) = 0.3s^2, s \in \mathbb{R}_{\geq 0}, \mu = 0.4, \rho(s) = 0.002s^2, s \in \mathbb{R}_{\geq 0}, \epsilon = 10^{-6} \). Hence, \( \phi(x, \dot{x}) = \max_i \Phi_i(x_i, \dot{x}_i) \) is an SFF from \( \Sigma \) to \( \Sigma \) satisfying the conditions in Definition 3.9 with \( \varepsilon(s) = 0.3s^2, s \in \mathbb{R}_{\geq 0}, \mu = 0.4, c = 10^{-6}, \) and \( \epsilon = 0.01 \). An upper bound of 2.31\% (i.e., \( \theta = 0.0231 \)) on the probability of the estimation accuracy is computed according to Theorem 3.10 within the time horizon \( T_d = 60 \). Employing Theorem 3.13, the probability that the solution process of the system starting from the initial region \( X_0 \) and not reaching \( X_0 \) is at least 90.06\% (i.e., \( (1 - \delta)(1 - \theta) = 0.9006 \)). Closed-loop state and input trajectories of a representative vehicle with different noise realizations are illustrated in Fig. 4.
Fig. 3. Closed-loop state and input trajectories of a representative vehicle with different noise realizations under controller (32).

Fig. 4. Closed-loop state and input trajectories of a representative vehicle with different noise realizations under controller (33).

VII. CONCLUSION

In this article, we proposed a compositional approach based on CBFs for the synthesis of safety controllers for networks of POMDP by utilizing small-gain type reasoning. The proposed scheme provides an upper bound on the probability that the interconnected system reaches an unsafe region in a finite-time horizon. In this respect, we first quantified probability bounds without any prior information on the estimation accuracy. This is achieved by constructing local barrier functions over an augmented system composed of subsystems and their corresponding estimators. Alternatively, we formulated local barrier functions based on only estimators’ dynamics and computed the exit probability by utilizing the probability bound on the estimation accuracy computed via notions of SSFs. We finally demonstrated the effectiveness of our proposed results by applying them to an ACC problem.

APPENDIX

A. Proofs

Proof: (Theorem 3.6) According to condition (11), $X_b \times X \subseteq \{(x, \hat{x}) \in X \times X \mid B(x, \hat{x}) \geq \lambda \}$. Then, we have

$$P \left[ x_{av}(k) \in X_b \land \hat{x}_{av}(k) \in X \text{ for some } k \in [0, T_d] \mid a, \hat{a}, v \right]$$

$$\leq P \left[ \sup_{0 \leq k \leq T_d} B(x_{av}(k), \hat{x}_{av}(k)) \geq \lambda \mid a, \hat{a}, v \right] \leq \delta. \quad (A.1)$$

The proposed bounds in (13) follow directly by applying [43, Th. 3, Ch. III] to the above inequality and employing conditions (12) and (10), respectively. Inequality (A.1) is obtained by utilizing the result of [44, Th. 1]. Now we get

$$P \left[ x_{av}(k) \in X_b \land \hat{x}_{av}(k) \in X \text{ for some } k \in [0, T_d] \mid a, \hat{a}, v \right]$$

$$\leq P \left[ x_{av}(k) \in X_b \text{ for some } k \in [0, T_d] \mid a, \hat{a}, v \right]$$

$$+ P \left[ \hat{x}_{av}(k) \in X \text{ for some } k \in [0, T_d] \mid \hat{a}, v \right]$$

$$- P \left[ x_{av}(k) \in X_b \lor \hat{x}_{av}(k) \in X \text{ for some } k \in [0, T_d] \mid a, \hat{a}, v \right].$$

Since, the second and last terms trivially hold with probability 1, one has

$$P \left[ x_{av}(k) \in X_b \land \hat{x}_{av}(k) \in X \text{ for some } k \in [0, T_d] \mid a, \hat{a}, v \right]$$

$$\leq P \left[ x_{av}(k) \in X_b \text{ for some } k \in [0, T_d] \mid a, v \right].$$

Now, since the right term of the conjunction (i.e., $\land$) holds for all time, the inequality above becomes an equality and one gets $P \left[ x_{av}(k) \in X_b \text{ for some } k \in [0, T_d] \mid a, v \right] \leq \delta$, which concludes the proof.

Proof: (Theorem 3.10) Since $\phi$ is an SPSF from $\hat{\Sigma}$ to $\Sigma$, one has

$$P \left[ \sup_{0 \leq k \leq T_d} \| x_{av}(k) - \hat{x}_{av}(k) \| \geq \epsilon \mid a, \hat{a}, v \right]$$

$$= P \left[ \sup_{0 \leq k \leq T_d} \epsilon (\| x_{av}(k) - \hat{x}_{av}(k) \|) \geq \epsilon \epsilon \mid a, \hat{a}, v \right]$$

$$\leq P \left[ \sup_{0 \leq k \leq T_d} \phi(x_{av}(k), \hat{x}_{av}(k)) \geq \epsilon \epsilon \mid a, \hat{a}, v \right] \leq \theta.$$

The equality holds due to the fact that $\epsilon$ is a $K_{\epsilon}$ function. The second inequality holds based on the first condition of Definition 3.9, and the last inequality follows from the result in [43, Th. 1].

Proof: (Theorem 3.13) Given $a, \hat{a} \in X_d$, let us define the events $A_1 := \left\{ x_{av}(k) \in X \text{ for some } k \in [0, T_d] \right\}$, $A_2 := \left\{ \hat{x}_{av}(k) \in X_b \text{ for some } k \in [0, T_d] \right\}$, and $A_3 := \left\{ \sup_{0 \leq k \leq T_d} \| x_{av}(k) - \hat{x}_{av}(k) \| \leq \epsilon \right\}$. Then, we have

$$P \left[ \bar{A}_1 \right] \overset{(*)}{=} P \left[ A_2 \cap A_3 \right]$$

$$= P \left[ A_2 \mid A_3 \right] P \left[ A_3 \right] \overset{(**)}{\geq} (1 - \delta)(1 - \theta)$$

where $\bar{A}_i$ is the complement of event $A_i$ for $i \in \{1, 2\}$, and $P \left[ A_2 \mid A_3 \right]$ is conditional probability. The first equality comes from the definition of $X_b$ being an $\epsilon$-inflated version of $X_b$. Notice that in the last inequality (**), the term $P \left[ A_2 \mid A_3 \right]$ is lower bounded by $(1 - \delta)$, since if $A_3$ holds, $\varphi(\| x(k) - \hat{x}(k) \|)$ in Definition 3.12 will be upper bounded by $\varphi(\| \epsilon \|)$. Furthermore, the term $P \left[ A_3 \right]$ is lower
bounded by \( (1 - \theta) \) by Theorem 3.10. This concludes the proof.

**Proof:** (Theorem 5.4) We first show that conditions (10) and (11) in Definition 3.3 hold. For any \((x, \hat{x}) \in X_a \times X_a\), with \(X_a = \prod_{i=1}^{N} X_{a_i}\), and from (7), we have

\[
B(x, \hat{x}) = \max_i \{ \sigma_i^{-1}(B_i(x_i, \hat{x}_i)) \} \leq \max_i \{ \sigma_i^{-1}(\tilde{\gamma}_i) \} = \gamma
\]

and simply for any \((x, \hat{x}) \in X_b \times X_b\), with \(X_b = \prod_{i=1}^{N} X_{b_i}\),

\[
X = \prod_{i=1}^{N} X_i\), and from (8), we have

\[
B(x, \hat{x}) = \max_i \{ \sigma_i^{-1}(B_i(x_i, \hat{x}_i)) \} \geq \max_i \{ \sigma_i^{-1}(\tilde{\lambda}_i) \} = \lambda
\]

satisfying conditions (7) and (8) with \(\gamma = \max_i \{ \sigma_i^{-1}(\tilde{\gamma}_i) \}\) and \(\lambda = \max_i \{ \sigma_i^{-1}(\tilde{\lambda}_i) \}\). Moreover, \(\lambda > \gamma\), according to (26). Now we show that condition (12) holds, as well. Let \(\kappa(s) = \max_{i,j} \{ \sigma_j^{-1} \circ \tilde{\kappa}_{ij} \circ \sigma_j(s) \}\). It follows from (25) that \(\kappa < \mathcal{I}\).

Since \(\max_i \sigma_i^{-1}\) is concave, one can readily acquire the chain of inequalities in (A.2) shown at the bottom of this page using Jensen’s inequality. Hence, \(B\) is a CBF for the augmented system \(\hat{\Sigma} = [\Sigma; \tilde{\Sigma}]\), which completes the proof.

**B. Computation of LCBF**

In this subsection, we provide a systematic approach to search for LCBFs and the corresponding control policies for subsystems. The proposed approach is based on the sum-of-squares (SOS) optimization problem [45], in which LCBF is restricted to be nonnegative, which can be written as a SOS of different polynomials. To do so, we need to raise the following assumption.

**Assumption 1.1:** For the POMDP \(\Sigma = (X, U, W, \varsigma_1, f, Y_1, \lambda_1, \beta, h_1, h_2, \varsigma_2)\), the transition map \(f : X \times U \times W \rightarrow X\) is a polynomial function of its arguments. Furthermore, the internal output map \(h_1 : X \rightarrow Y_1\) and \(\mathcal{K}_\infty\) functions \(\alpha\) and \(\rho\) are polynomial.

Under Assumption 1.1, one can reformulate conditions of Definitions 3.2 and 3.11 to an SOS optimization problem in order to search for a polynomial LCBF \(\hat{B}(\cdot, \cdot)\) and \(B(\cdot, \cdot)\), and their corresponding control policies. In the following lemmas, SOS formulations are provided.

**Lemma 1.2:** Suppose Assumption 1.1 holds and sets \(X_a, X_b, W\) can be defined by vectors of polynomial inequalities \(X_a = \{ x \in \mathbb{R}^n \mid g_a(x) \geq 0 \}, \)

\(X_b = \{ x \in \mathbb{R}^n \mid g_b(x) \geq 0 \}, \)

\(X = \{ x \in \mathbb{R}^n \mid g(x) \geq 0 \}, \)

\(W = \{ w \in \mathbb{R}^p \mid g_w(w) \geq 0 \}, \)

\(U = \{ u(k) \in \mathbb{R}^m \mid g_u(u(k)) \geq 0 \}\), where the inequalities are defined element-wise. Suppose there exists an SOS polynomial \(B(x, \hat{x})\), constants \(\gamma, \psi \in \mathbb{R}_{\geq 0}, \lambda, \hat{\lambda} \in \mathbb{R}_{> 0}, 0 < \kappa < 1\), functions \(\alpha \in \mathcal{K}_\infty, \hat{\alpha} \in \mathcal{K}_\infty \cup \{0\}\), polynomials \(l_{ij}(\hat{x}, \hat{w})\) corresponding to the \(j\)th input in \(u(k) = (v_1(k), v_2(k), \ldots, v_m(k)) \in U \subseteq \mathbb{R}^m\), and vectors of SOS polynomials \(l_z(x), \tilde{l}_z(\hat{x})\) for \(z \in \{0, 1, 2, 3\}\), and \(l_v(u(\hat{x})), l_w(\hat{w}), \tilde{l}_w(\hat{w})\), of appropriate dimensions such that the following expressions are SOS polynomials:

\[
B(x, \hat{x}) = B^T(x, \hat{x})\left[ f(x, \hat{x}) - \alpha \left( \begin{array}{c} h_1(x) \\ h_1(\hat{x}) \end{array} \right) \right] - \alpha \left( \begin{array}{c} h_1(x) \\ h_1(\hat{x}) \end{array} \right) \right)^T B(x, \hat{x})
\]

(A.3)
\(- B(x, \hat{x}) - [\tilde{T}_x^T(x)] \left[ \frac{g_a(x)}{g_a(\hat{x})} \right] + \tilde{\lambda} \) \hspace{1cm} (A.4)
\[ B(x, \hat{x}) - [\tilde{T}_w^T(x)] \left[ \frac{\tilde{g}(x)}{\tilde{g}(\hat{x})} \right] + \tilde{\gamma} \] \hspace{1cm} (A.5)
\[ - \mathbb{E} [\mathcal{B}(f(x(k), v(k), w(k), e(k)))], \] \[ \hat{f}(\hat{x}(k), v(k), w(k), g_2(k)) \] \[ |x(k), \hat{x}(k), v(k), w(k), \hat{w}(k)| + \kappa \mathcal{B}(x(k), \hat{x}(k)) + \psi \] \[ + \tilde{\rho} \left( \begin{array}{c} \left[ \frac{w(k)}{\hat{w}(k)} \right]^T \frac{[w(k)]}{[\hat{w}(k)]} \\ \frac{2p}{m} \end{array} \right) \sum_{j=1}^{m} (v_j(k) - l_{v_j}(\hat{x}(k), \hat{w}(k))) \] \[ - [\tilde{T}_w^T(x(k)) \frac{[\tilde{w}(k)]}{[\tilde{w}(\hat{x}(k))]} \left[ \frac{g_w(x(k))}{g_w(\hat{x}(k))} \right] - \tilde{T}_w^T(x(k))g_v(v(k)) \] \[ - [\tilde{T}_w^T(w(k)) \frac{[\tilde{w}(w(k))]}{[\tilde{w}(\hat{w}(w(k)))]} \left[ \frac{g_w(x(k))}{g_w(\hat{x}(k))} \right] - \tilde{T}_w^T(w(k))g_v(v(k)) \] \[ (A.6) \]
where \( p \) is the dimension of the internal inputs \( w \) and \( \hat{w} \). Then, \( B(x, \hat{x}) \) satisfies conditions (6)–(20) in Definition 3.2 and \( v(k) = [l_{v_1}(\hat{x}(k), \hat{w}(k)); \ldots ; l_{v_m}(\hat{x}(\hat{w}(w(k))))] \) is the corresponding safety controller, where \( \kappa, \rho, \tilde{\rho} \) can be acquired based on \( \kappa, \tilde{\rho}, \tilde{\gamma} \) similar to Lemma 1.2.

**Remark 1.3:** Inequalities (6) and (9) consider infinity norms over \( \| h_1(x) ; h_2(x) \| \) and \( \| w ; \hat{w} \| \), respectively. Since such norms cannot be expressed as polynomials, we convert infinity norms to Euclidean ones and that is the reason constant \( 2p \) appears as a denominator in (A.6).

**Remark 1.4:** Note even if the functions mentioned in Assumption 1.1 are not polynomials, one can still use the proposed results in the article by searching for LCBFs via CEGIS.

We now state another lemma for the computation of LCBF as in Definition 3.11.

**Lemma 1.5:** Suppose Assumption 1.1 holds and sets \( X_a, X_b, X_r, X_w, Y_2 \) can be defined by vectors of polynomial inequalities \( X_a = \{ x \in \mathbb{R}^n \mid g_a(x) \geq 0 \}, X_b = \{ x \in \mathbb{R}^n \mid g_b(x) \geq 0 \}, X_r = \{ x \in \mathbb{R}^n \mid \gamma(x) \geq 0 \}, U = \{ v(k) \in \mathbb{R}^m \mid g_v(v(k)) \geq 0 \}, \) and \( W = \{ w \in \mathbb{R}^p \mid g_w(w) \geq 0 \} \), where the inequalities are defined element-wise. Suppose there exists an SOS polynomial \( B(x) \), constants \( \gamma, \psi \in \mathbb{R}_{20}, \tilde{\lambda} \in \mathbb{R}_{0}, 0 < \tilde{\kappa} < 1 \), functions \( \alpha, \omega \in \mathcal{K}_{\infty}, \tilde{\rho} \in \mathcal{K}_{\infty} \cup \{ 0 \} \), polynomials \( l_{v_j}(\hat{x}, \hat{w}) \) corresponding to the \( j \)-th input in \( v(k) = (v_1(k), v_2(k), \ldots, v_m(k)) \in U \subseteq \mathbb{R}^m \), and vectors of SOS polynomials \( l_z(x) \) for \( z \in \{ 0, 1, 2, 3 \} \), \( l_{\hat{x}}(\hat{x}), l_{\hat{w}}(v(k)) \), and \( l_{\hat{w}}(\hat{w}) \) of appropriate dimensions such that the following expressions are sum-of-square polynomials:
\[ B(x) - T_0^T(x)g(x) - \alpha(h_1(x)^T h_1(x)) \] \[ - B(x) - T_1^T(x)g_a(x) + \tilde{\lambda} \] \[ (A.7) \]
\[ B(x) - T_2^T(x)g_1(x) + \gamma \] \[ - \mathbb{E} [B(f(x(k), v(k), w(k), e(k)))] \] \[ |x(k), v(k), w(k), \hat{w}(k)| + \kappa B(x(k), \hat{x}(k)) + \tilde{\rho} \frac{(\tilde{w}(\tilde{k}))}{p} \] \[ \tilde{\psi} + \tilde{\kappa} \mathcal{B}(x(k), \hat{x}(k)) + \tilde{\kappa} \mathcal{B}(x(k), \hat{x}(k)) + \tilde{\rho} \frac{(\tilde{w}(\tilde{k}))}{p} \] \[ (A.9) \]
where \( p \) and \( n \) are the dimensions of the internal input \( w \) and state \( x \), respectively. Then, \( B(x, \hat{x}) \) satisfies conditions (17)–(20) in Definition 3.11 and \( v(k) = [l_{v_1}(\hat{x}(k), \hat{w}(k)); \ldots ; l_{v_m}(\hat{x}(\hat{w}(w(k))))] \) is the corresponding safety controller, where \( \kappa, \rho, \psi \) can be acquired based on \( \gamma, \kappa, \rho, \psi \) similar to Lemma 1.2.

**References**

[1] J. Lygeros et al., “Hierarchical, hybrid control of large scale systems,” Ph.D. dissertation, Citeeseer, 1996.
[2] H.-D. Tran, L. V. Nguyen, W. Xiang, and T. T. Johnson, “Order-reduction abstractions for safety verification of high-dimensional linear systems,” *Discrete Event Dyn. Syst.*, vol. 27, no. 2, pp. 443–461, 2017.
[3] K. Mallik, S. E. Z. Soudjani, A.-K. Schmuck, and R. Majumdar, “Compositional construction of finite state abstractions for stochastic control systems,” in *Proc. IEEE 56th Annu. Conf. Decis. Control*, 2017, pp. 550–557.
[4] J.-P. Katoen, D. Klink, and M. R. Neuhäusler, “Compositional abstraction for stochastic systems,” in *Proc. Int. Conf. Formal Model. Anal. Timed Syst.*, 2009, pp. 195–211.
[5] X. Chen, S. Mover, and S. Sankaranarayanan, “Compositional relational abstraction for nonlinear hybrid systems,” *ACM Trans. Embedded Comput. Syst.*, vol. 16, no. 5, pp. 1–19, 2017.

J. Berendsen and F. Vaandrager, “Compositional abstraction in real-time model checking,” in *Proc. Int. Conf. Formal Model. Anal. Timed Syst.*, 2008, pp. 233–249.
[7] K. Mallik, A.-K. Schmuck, S. Soudjani, and R. Majumdar, “Compositional synthesis of finite-state abstractions,” *IEEE Trans. Autom. Control*, vol. 64, no. 6, pp. 3820–3826, Jun. 2019.
[8] P.-J. Meyer and D. V. Dimarogonas, “Compositional abstraction refinement for control synthesis,” *Nonlinear Anal.: Hybrid Syst.*, vol. 27, pp. 437–451, 2018.
[9] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, “Control barrier function based quadratic programs for safety critical systems,” *IEEE Trans. Autom. Control*, vol. 62, no. 8, pp. 3861–3876, Aug. 2017.
[10] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, “Control barrier functions: Theory and applications,” in *Proc. 18th Eur. Control Conf.*, 2019, pp. 3420–3431.
[11] A. D. Ames, J. W. Grizzle, and P. Tabuada, “Control barrier function based quadratic programs with application to adaptive cruise control,” in *Proc. IEEE 53rd Conf. Decis. Control*, 2014, pp. 6271–6278.
[12] L. Wang, A. D. Ames, and M. Egerstedt, “Safety barrier certificates for collisions-free multirobot systems,” *IEEE Trans. Robot.*, vol. 33, no. 3, pp. 661–674, Jun. 2017.
[13] Z. Lyu, X. Xu, and Y. Hong, “Small-gain theorem for safety verification of interconnected systems,” *Automatica*, vol. 139, 2022, Art. no. 110178.
Abolfazl Lavaei (Member, IEEE) received the M.Sc. degree in aerospace engineering, with a specialization in flight dynamics and control from the University of Tehran (UT), Tehran, Iran, in 2014 and the Ph.D. degree in electrical engineering from the Technical University of Munich (TUM), Munich, Germany, in 2019.

He is a Postdoctoral Associate with the Institute for Dynamic Systems and Control, ETH Zurich, Switzerland. From 2019 to 2020, he was a Postdoctoral Researcher with the Department of Computer Science, LMU Munich. His line of research focuses mainly on theoretical and practical aspects of “formal verification, learning and control of large-scale stochastic cyber-physical systems” with application to “autonomous systems”. His research interests revolve around the intersection of control theory, computer science, machine learning, and data science.

Dr. Lavaei is the recipient of several international awards, including Best Demo/Poster Award at the ACM HSCC 2022, Best Repeatability Prize at the IFAC ADHS 2021, Best Demo/Poster Award at the ACM HSCC 2020, IFAC Young Author Award Finalist at the IFAC LSS 2019, Best Graduate Student Award at the University of Tehran with the full GPA (20/20), and several prestigious Ph.D. scholarships from different top-ranked universities.

Majid Zamani (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from the Isfahan University of Technology, Isfahan, Iran, in 2005, the M.Sc. degree in electrical engineering from the Sharif University of Technology, Tehran, Iran, the M.A. degree in mathematics and the Ph.D. degree in electrical engineering from the University of California, Los Angeles, CA, USA, both in 2012.

He is currently an Assistant Professor with the Computer Science Department, University of Colorado Boulder, Boulder, CO, USA, and a Guest Professor with the Computer Science Department, LMU Munich. From 2012 to 2013, he was a Postdoctoral Researcher with the Delft Center for Systems and Control, Delft University of Technology, The Netherlands, where he was an Assistant Professor with Design Engineering Department, from 2013 to 2014. From 2014 to 2019, he was an Assistant Professor with the Department of Electrical and Computer Engineering, Technical University of Munich, Germany. His research interests include verification and control of hybrid systems, embedded control software synthesis, networked control systems, and incremental properties of nonlinear control systems.

Dr. Zamani received the NSF Career award in 2022 and an ERC Starting Grant Award from the European Research Council in 2018.