A Compositional Resilience Index for Computationally Efficient Safety Analysis of Interconnected Systems

Luyao Niu[1], Abdullah Al Maruf[2], Andrew Clark[3], J. Sukarno Mertoguno[4], and Radha Poovendran[1]

***Abstract*— Interconnected systems such as power systems and chemical processes are often required to satisfy safety properties in the presence of faults and attacks. Verifying safety of these systems, however, is computationally challenging due to nonlinear dynamics, high dimensionality, and combinatorial number of possible faults and attacks that can be incurred by the subsystems interconnected within the network. In this paper, we develop a compositional resilience index to verify safety properties of interconnected systems under faults and attacks. The resilience index is a tuple serving the following two purposes. First, it quantifies how a safety property is impacted when a subsystem is compromised by faults and attacks. Second, the resilience index characterizes the needed behavior of a subsystem during normal operations to ensure safety violations will not occur when future adverse events occur. We develop a set of sufficient conditions on the dynamics of each subsystem to satisfy its safety constraint, and leverage these conditions to formulate an optimization program to compute the resilience index. When multiple subsystems are interconnected and their resilience indices are given, we show that the safety constraints of the interconnected system can be efficiently verified by solving a system of linear inequalities. We demonstrate our developed resilience index using a numerical case study on chemical reactors connected in series.**

I. Introduction

Safety-critical interconnected systems are widely seen in real-world applications such as power systems [1] and chemical processes [2]. Safety violations can lead to significant economic losses and severe damage to the system and/or human operators engaged with the system [1], [3]–[6]. Therefore, it is of critical importance to verify safety properties for such large-scale or even societal-scale systems.

One approach to verify safety is to use reachability analysis. Computing reachable sets for nonlinear systems is known to be undecidable [7]. Alternatively, solutions to safety verification by ensuring forward invariance of safety sets [8]–[11] or approximating reachable sets [12]–[14] have been developed. However, these approaches do not scale to interconnected systems of high dimensions. Large-scale systems such as power systems generally consist of multiple interconnected subsystems, motivating the development of compositional approaches [15]–[18]. These approaches decompose the safety verification problem into a set of problems of smaller scales formulated on the subsystems, and thus are more tractable.

The approaches in [15]–[18] assume that the systems are operated under benign environments, making the verified safety properties invalid for systems under faults and attacks. For interconnected systems, an error from one faulty or compromised subsystem could propagate and accumulate through interconnections and impact the safety of other subsystems. A naïve approach to safety verification for interconnected systems operated under adversarial environments is to enumerate all possible faulty or compromised subsystems, and perform safety analysis. However, the number of possible faults or attacks that can be incurred by the interconnected system is combinatorial. At present, scalable safety verification of large-scale interconnected systems under faults and attacks has been less studied.

In this paper, we develop a compositional safety verification approach for large-scale interconnected systems whose subsystems can be faulty or compromised by attacks. Each subsystem is subject to a safety constraint. We derive a set of conditions on the dynamics of a subsystem to guarantee its safety. We parameterize these conditions using a tuple of real numbers, termed resilience index. Our resilience index defines the amount of time that the system can safely remain in a faulty state, the amount of time required to recover from faults, and constraints on the system dynamics that must be satisfied during faulty as well as normal operation. The resilience index allows us to convert the problem of safety verification of large-scale interconnected systems to a set of algebraic computations, and thus makes safety verification feasible for large-scale systems. To summarize, this paper makes the following contributions.

- We formulate a resilient index for a subsystem that experiences faults or attacks. We prove safety guarantees for a subsystem based on the resilience index. We develop a sum-of-squares optimization to compute the resilience index for a subsystem.
- We derive a system of linear inequalities to quantify how the resilience index of a subsystem changes due to interconnections. Using the derived linear inequalities, we develop the conditions on the interconnections so that all subsystems are safe under faults and attacks.

[1]Luyao Niu and Radha Poovendran are with the Network Security Lab, Department of Electrical and Computer Engineering, University of Washington, Seattle, WA 98195-2500 {luyaoniu,rp3}@uw.edu

[2]Abdullah Al Maruf is with the Department of Electrical and Computer Engineering, California State University, Los Angeles, CA 90032 amaruf@calstatela.edu

[3]Andrew Clark is with the Electrical and Systems Engineering Department, McKelvey School of Engineering, Washington University in St. Louis, St. Louis, MO 63130 andrewclark@wustl.edu

[4]J. Sukarno Mertoguno is with the School of Cybersecurity and Privacy, Georgia Institute of Technology, Atlanta, GA 30332 karno@gatech.edu

This work was supported by the AFOSR grants FA9550-20-1-0074 and FA9550-22-1-0054, by the Office of Naval Research grants N00014-20-1-2636 and N00014-23-1-2386, by the National Science Foundation grant CNS-1941670, and by the BIRD Foundation: Israel-US Energy Center, Cyber Topic.

- We demonstrate the resilience indices and their usage using a case study on chemical process.

The rest of this paper is organized as follows. Section II presents related work. Section III describes the problem formulation. Section IV develops the compositional resilience index for each subsystem. In Section V, we derive the set of inequalities to compute resilience indices after interconnection. Section VI demonstrates the proposed approach using a numerical case study. We conclude the paper in Section VII.

II. Related Work

Safety verification [8], [11], [19] and safety-critical control [4], [20], [21] haven been investigated for systems operated in benign environments. To mitigate faults and attacks against safety-critical systems, various techniques have been developed. Attack detection and secure state estimation under attacks have been studied in [22], [23]. Fault-tolerant and resilient control schemes [9], [24]–[26] have been proposed to withstand the attacks and guarantee system safety. For interconnected systems consisting of multiple subsystems, the systems are of high dimensionality and the attack surface grows as interconnected systems involving more subsystems, making safety verification computationally expensive.

Compositional approaches have been adopted for safety verification of interconnected systems deployed in the absence of faults or attacks [15]–[18]. These approaches have utilized techniques including barrier certificates [15], [18], small-gain theorem [16], and dissipativity property [17]. When the system is operated under faulty or adversarial environments, these approaches become less effective.

The authors of [27], [28] re-configured the control laws of each subsystem and interconnection topology to guarantee safety. Such approach is computationally expensive when re-configuring the network topology and control laws. Furthermore, in applications such as power systems, re-designing interconnection topology is less desired or even impractical. In this paper, we develop a compositional resilience index and prove that the safety of each subsystem interconnected within a network can be analyzed by solving a system of linear inequalities derived using resilience index. Our developed approach does not require re-configuring the network topology or control laws, and hence is more computationally efficient. In [29], the authors decomposed the dynamics of each subsystem into intrinsic and coupled terms, where the former term is independent of the other subsystems and the latter one depends on interconnections. A resilience index was defined for each term of a compromised subsystem by bounding how fast a subsystem approaches the boundary of safety set. Such resilience indices were computed by sum-of-squares optimization, and allowed the synthesis of safe control law under fixed interconnections. When the interconnections change, the resilience indices and safe control law in [29] could not always guarantee safety property. In this paper, we propose a resilience index and derive a system of linear inequalities that can applied to verify safety when interconnections change. When the inequalities are feasible, the interconnected system can satisfy the safety constraints.

III. Problem Formulation

We first define the notations that will be used throughout this paper. Let $x \in \mathbb{R}^n$. We denote the k-th entry of x as $[x]_k$. A continuous function $\alpha : [-b, a) \to (-\infty, \infty)$ belongs to extended class $\mathcal{K}$ if it is strictly increasing and $\alpha(0) = 0$ for some $a, b > 0$. Linear functions $\alpha(x) = zx$ defined over $[-b, a)$ are extended class $\mathcal{K}$ functions when $z > 0$.

We consider a collection of subsystems $\{\mathcal{S}_i\}_{i \in \mathcal{N}}$, where $\mathcal{N} = \{1, \ldots, N\}$. Each subsystem $\mathcal{S}_i$ individually follows dynamics given as

$$\mathcal{S}_i : \quad \dot{x}_i = f_i(x_i) + g_i(x_i)u_i, \tag{1}$$

where $x_i \in \mathcal{X}_i \subseteq \mathbb{R}^{n_i}$ is the state of subsystem i, and $u_i \in \mathcal{U}_i \subseteq \mathbb{R}^{p_i}$ is the external control input u_i applied to subsystem i. We consider that the external control input u_i will be chosen following a feedback control policy $\mu_i : \mathbb{R}^{n_i} \to \mathcal{U}_i$. Given the control policy μ_i and an initial state $x_i(0)$ at time $t = 0$, we denote the trajectory of subsystem $\mathcal{S}_i$ as $x_i(t; x_i(0), \mu_i)$. Functions $f_i : \mathbb{R}^{n_i} \to \mathbb{R}^{n_i}$ and $g_i : \mathbb{R}^{n_i} \to \mathbb{R}^{n_i \times p_i}$ are locally Lipschitz continuous.

We consider that each subsystem $\mathcal{S}_i$ is required to satisfy a safety constraint defined over a set $\mathcal{C}_i = \{x_i : h_i(x_i) \geq 0\}$, i.e., $x_i(t; x_i(0), \mu_i) \in \mathcal{C}_i$ is required to hold for all $t \geq 0$. Function $h_i : \mathbb{R}^{n_i} \to \mathbb{R}$ is continuously differentiable. We assume that the subsystem is initially safe, i.e., $x(0) \in \mathcal{C}_i$. For each subsystem $\mathcal{S}_i$, we assume that we are given a control law μ_i such that $x_i(t; x_i(0), \mu_i) \in \mathcal{C}_i$ holds for all $t \geq 0$. Such a safe control law μ_i can be synthesized by using approaches such as control barrier functions [20].

We assume that each subsystem can be faulty or compromised by an adversary. When the subsystem is faulty or under attack, the safe control law μ_i becomes offline, and the control input received by subsystem $\mathcal{S}_i$ can be arbitrarily altered to some $\tilde{u}_i \in \mathcal{U}_i$ that is chosen by the adversary and deviates from μ_i. To mitigate the persistence of faults and attacks, we consider that the subsystem recovers control law μ_i after the occurrence of faults and attacks leveraging fault/attack detection and isolation techniques [30].

To capture the fact that faults and attacks cause the control input to deviate from μ_i to arbitrary $\tilde{u}_i$, we represent each subsystem $\mathcal{S}_i$ under faults and attacks as a hybrid system $\mathcal{H}_i = (\mathcal{X}_i, \mathcal{U}_i, \mathcal{L}, \mathcal{Y}_i, \mathcal{Y}_i^{init}, Inv_i, \mathcal{F}_i, \Sigma_i, \mathcal{G}_i)$, where

- $\mathcal{X}_i \subseteq \mathbb{R}^{n_i}$ is the continuous state space of subsystem $\mathcal{S}_i$, and $\mathcal{U}_i \subseteq \mathbb{R}^{p_i}$ is the set of admissible control inputs.
- $\mathcal{L} = \{\texttt{offline}, \texttt{online}\}$ is a set of discrete locations capturing whether control law μ_i is available (`online`) or not (`offline`).
- $\mathcal{Y}_i = \mathcal{X}_i \times \mathcal{L}$ is the state space of hybrid system H, and $\mathcal{Y}_i^{init} \subseteq \mathcal{Y}_i$ is the set of initial states.
- $Inv_i : \mathcal{L} \to 2^{\mathcal{X}_i}$ is the invariant that maps from the set of locations to the power set of $\mathcal{X}_i$. That is, $Inv_i(l) \subseteq \mathcal{X}_i$ specifies the set of possible continuous states when the system is at location $l \in \mathcal{L}$.
- $\mathcal{F}_i$ is the set of vector fields. For each $F_i \in \mathcal{F}_i$ in the form of Eqn. (1), the continuous system state evolves as $\dot{x}_i = F_i(x_i, u_i, l)$, where F_i is jointly determined by

the system dynamics and the availability of control law μ_i, and $\dot{x}_i$ represents the time derivative of x_i.
- $\Sigma_i \subseteq \mathcal{Y}_i \times \mathcal{Y}_i$ is the set of transitions between the states of the hybrid system. A transition $\sigma_i = ((x_i, l), (x_i', l'))$ models the state transition from (x_i, l) to (x_i', l').

In applications such as power systems and vehicle platoons, multiple subsystems are interconnected as a network. The interconnections introduce couplings among subsystems, leading to the following dynamics for each subsystem

$$\dot{x}_i = f_i(x_i) + g_i(x_i)\mu_i(x_i) + \sum_{j\neq i} W_{ji}(x_j, x_i) - \sum_{j\neq i} W_{ij}(x_i, x_j), \quad (2)$$

where $W_{ij}(x_i, x_j)$ captures the interconnection between subsystems $\mathcal{S}_i$ and $\mathcal{S}_j$. Note that interconnections are not necessarily symmetric, i.e., $W_{ij}(x_i, x_j)$ and $W_{ji}(x_j, x_i)$ may not be identical.

We denote the state and joint control input of the interconnected system as $x = [x_1^\top, \ldots, x_N^\top]^\top$ and $u = [u_1^\top, \ldots, u_N^\top]^\top$, respectively. The interconnected system is therefore of high dimension and nonlinear. Furthermore, when each subsystem can possibly be compromised or faulty, the number of faults or attacks incurred by the interconnected system is combinatorial, making safety verification computationally intractable. In this paper, we investigate the following problem.

Problem 1. *Suppose that we are given a collection of subsystems $\{\mathcal{S}_i\}_{i=1}^N$ and their safe control laws μ_i with respect to their individual safety set $\mathcal{C}_i$, where $i \in \mathcal{N}$. The subsystems, which are potentially subject to faults and attacks, are interconnected within a network and each of them follows dynamics given in Eqn.* (2)*. The goal is to verify whether the interconnected system satisfies the set of safety constraints defined over $\mathcal{C}_i$ for all $i = 1, \ldots, N$.*

IV. Proposed Resilience Index

In this section, we propose a compositional resilience index for each subsystem to verify safety.

A. Definition of Resilience Index

We note that the discrete location set $\mathcal{L}$ is uniform to all subsystems, allowing us to develop a unified index to measure the resilience of any subsystem under faults and attacks. Our insight is as follows. At location `offline`, the safe control law μ_i is unavailable. To avoid violating the safety constraint, we require the subsystem to stay within a set $\mathcal{D}_i \subseteq \mathcal{C}_i$ so that $x_i \in \mathcal{C}_i$ for all time when the hybrid system is at location `offline`. When the hybrid system transitions from `offline` to `online`, the control law μ_i becomes available. Thereafter, the subsystem starts to *recover* from faults and attacks. To recover the control law and mitigate potential faults and attacks in the future, we let the control law μ_i to remain available for at least $\phi_i \geq 0$ amount of time. Furthermore, the system is required to reach set $\mathcal{D}_i$ within ϕ_i so that safety constraint will not be violated when attacks or faults occur in the future. Such insight allows us to define the following resilience index to capture each subsystem's resilience under faults and attacks.

Definition 1 (Resilience Index of a Subsystem)**.** *Consider a subsystem $\mathcal{S}_i$ that uses a feedback control law μ_i and is under a safety constraint defined on set $\mathcal{C}_i = \{x_i : h_i(x_i) \geq 0\}$. Let subsystem $\mathcal{S}_i$ be formulated as hybrid system $\mathcal{H}_i$ and $d_i, \eta_i \geq 0$, $\tau_i, \phi_i > 0$. We say subsystem $\mathcal{S}_i$ is $(d_i, \tau_i, \phi_i, \eta_i)$-resilient if the following conditions hold*

- *Set $\mathcal{D}_i$ defined as $\mathcal{D}_i = \{x_i : h_i(x_i) - d_i \geq 0\}$ is forward invariant if control law μ_i is used and the hybrid system $\mathcal{H}_i$ in at location* `online`*.*
- *After reaching location* `offline`*, hybrid system $\mathcal{H}_i$ remains at location* `offline` *for at most τ_i amount of time before transition from* `offline` *to* `online` *occurs for any x_i.*
- *Following the transition from* `offline` *to* `online`*, hybrid system $\mathcal{H}_i$ remains at location* `online` *for at least ϕ_i amount of time.*
- *When x_i is at the boundary of $\mathcal{D}_i$ and the hybrid system $\mathcal{H}_i$ in at location* `online`*, the time derivative of x_i is lower bounded by η_i. Furthermore, given any state $x_i' \in \mathcal{C}_i \setminus \mathcal{D}_i$, the continuous state x_i reaches $\mathcal{D}_i$ within ϕ_i amount of time when $\mathcal{H}_i$ is at location* `online` *and control law μ_i is used.*

The quadruple $(d_i, \tau_i, \phi_i, \eta_i)$ is the resilience index of $\mathcal{S}_i$.

In what follows, we derive a set of conditions to compute the resilience index of a subsystem.

Proposition 1. *Consider a subsystem in Eqn.* (1) *under attack and a safety set $\mathcal{C}_i$. Let $h_i^d(x_i) = h_i(x_i) - d_i$ and $\mathcal{D}_i = \{x_i : h_i^d(x_i) \geq 0\} \subseteq \mathcal{C}_i$. Suppose $x_i(0) \in \mathcal{D}_i$. If there exist constants $d_i, \eta_i \geq 0$, $\tau_i, \phi_i > 0$, and an extended class $\mathcal{K}$ function $\alpha_i(\cdot)$ such that*

$$\frac{\partial h_i^d}{\partial x_i}(x_i)[f_i(x_i) + g_i(x_i)u_i] \geq -\frac{d_i}{\tau_i}, \ \forall (x_i, u_i) \in \mathcal{C}_i \times \mathcal{U}_i \quad (3a)$$

$$\frac{\partial h_i^d}{\partial x_i}(x_i)[f_i(x_i) + g_i(x_i)\mu_i(x_i)] \geq \frac{d_i}{\phi_i}, \ \forall x_i \in \mathcal{C}_i \setminus \mathcal{D}_i \quad (3b)$$

$$\frac{\partial h_i^d}{\partial x_i}(x_i)[f_i(x_i) + g_i(x_i)\mu_i(x_i)] \geq -\alpha_i(h_i^d(x_i)) + \eta_i, \quad \forall x \in \mathcal{D}_i \quad (3c)$$

then subsystem $\mathcal{S}_i$ is safe with respect to $\mathcal{C}_i$.

Proof. Without loss of generality, we assume that the subsystem is compromised by attack at some arbitrary time $t_0 \geq 0$. For any $t \in [t_0, t_0 + \tau_i]$ and control input $u_i \in \mathcal{U}_i$, we have $h_i(x_i(t)) = h_i(x_i(t_0)) + \int_{s=t_0}^t \dot{h}_i \, \mathrm{d}s \geq d_i - \frac{d_i}{\tau_i}(t - t_0) \geq 0$, where $\dot{h}_i$ represents the time derivative of function h_i, the equality holds by the definition of $h_i(x_i(t))$, the first inequality holds by Eqn. (3a) and the observation that $\dot{h}_i^d = \dot{h}_i$, and the last inequality holds by $t \in [t_0, t_0 + \tau]$. Therefore, hybrid system $\mathcal{H}_i$ satisfies $x_i(t; x_i(t_0), u_i) \in \mathcal{C}_i$ for all $u_i \in \mathcal{U}_i$ when $x_i(t_0) \in \mathcal{D}_i$, $\mathcal{H}_i$ is at location $l =$ `offline` for at most τ_i amount of time, and Eqn. (3a) holds.

We next consider some arbitrary time $t \in [t_0+\tau_i, t_0+\tau_i+\phi_i]$ when the hybrid system is at location `online`. We show that $x_i(t; x_i(t_0+\tau_i), \mu_i) \in \mathcal{C}_i$ for all $t \in [t_0+\tau_i, t_0+\tau_i+\phi_i]$ when the hybrid system remains at location `online` and control law μ_i is used. We further show that there exists $t' \in [t_0+\tau_i, t_0+\tau_i+\phi_i]$ such that $x_i(t''; x_i(t_0+\tau_i), \mu_i) \in \mathcal{D}_i$ for all $t'' \in [t', t_0+\tau_i+\phi_i]$ when the hybrid system remains at location `online` and control law μ_i is used.

We prove $x_i(t; x_i(t_0+\tau_i), \mu_i) \in \mathcal{C}_i$ for all $t \in [t_0+\tau_i, t_0+\tau_i+\phi_i]$ when the hybrid system remains at location `online` and μ_i is used by contradiction. Suppose that the subsystem leaves the safety set. Since the trajectory of $\mathcal{S}_i$ is continuous, then there exists time $t \in [t_0+\tau_i, t_0+\tau_i+\phi_i]$ such that $h(x(t)) = 0$ and $\dot{h}(x(t)) < 0$. If such $x(t) \in \mathcal{C}_i \setminus \mathcal{D}_i$, we then have contradiction to Eqn. (3b) since $\frac{d_i}{\phi_i} > 0$ and thus $\dot{h}(x(t)) > 0$. If such $x(t) \in \mathcal{D}_i$, we also have contradiction since Eqn. (3c) implies that $\dot{h}(x(t)) > \eta_i \geq 0$. Therefore, we can claim that $x_i(t; x_i(t_0+\tau_i), \mu_i) \in \mathcal{C}_i$ for all $t \in [t_0+\tau_i, t_0+\tau_i+\phi_i]$ when the hybrid system remains at location `online` and μ_i is used.

We now prove that there exists $t' \in [t_0+\tau_i, t_0+\tau_i+\phi_i]$ such that $x_i(t''; x_i(t_0+\tau_i), \mu_i) \in \mathcal{D}_i$ for all $t'' \in [t', t_0+\tau_i+\phi_i]$ when the hybrid system remains at location `online` and control law μ_i is used. Suppose no such $t' \in [t_0+\tau_i, t_0+\tau_i+\phi_i]$ exists. We then have that $x_i(t_0+\tau_i+\phi_i) \in \mathcal{C}_i \setminus \mathcal{D}_i$ and hence $h_i(x_i(t_0+\tau_i+\phi_i)) < d_i$. By Eqn. (3b), we have $h_i(x_i(t_0+\tau_i+\phi_i)) = h_i(x_i(t_0+\tau_i)) + \int_{s=t_0+\tau_i}^{t} \dot{h}_i \, \mathrm{d}s \geq \frac{d_i}{\phi_i}(t-t_0-\tau_i) \geq d_i$, leading to contradiction. Therefore, such t' must exist. Finally, by Eqn. (3c) and [20], we have that if $x_i(t'; x_i(t_0+\tau_i), \mu_i) \in \mathcal{D}_i$, then set $\mathcal{D}_i$ if forward invariant when the hybrid system remains at location `online` and control law μ_i is used, indicating that $x_i(t''; x_i(t_0+\tau_i), \mu_i) \in \mathcal{D}_i$ for all $t'' \in [t', t_0+\tau_i+\phi_i]$. $\square$

We remark that the tuple $(d_i, \tau_i, \phi_i, \eta_i)$ is unordered. When employing it to evaluate and compare the resilience of multiple subsystems, one may adopt the weighted average of d_i, τ_i, ϕ_i, and η_i. Alternatively, d_i, τ_i, ϕ_i, and η_i can be ordered based on their importance, allowing comparison of resilience indices in lexicographical order.

B. Computation of Resilience Index

In the following, we formulate a sum-of-squares (SOS) optimization program to compute the resilience index for any subsystem $\mathcal{S}_i$. Under certain assumptions on the dynamics (1), function $h_i(x)$, and control input set $\mathcal{U}_i$, we formulate the SOS program by converting the conditions in Eqn. (3) into SOS constraints. We make the following assumption.

Assumption 1. *For any subsystem $\mathcal{S}_i$, we assume that functions $f_i(x_i)$, $g_i(x_i)$, and $h_i(x_i)$ are polynomial in x_i. In addition, we assume that $\mathcal{U}_i = \prod_{k=1}^{p_i}[u_{k,min}, u_{k,max}]$ with $u_{k,min} < u_{k,max}$.*

In the following, we present the set of SOS constraints. We show that any $d_i, \eta_i \geq 0$ and $\tau_i, \phi_i > 0$ satisfying the SOS constraints constitute the resilience index of $\mathcal{S}_i$.

Proposition 2. *Assume that control law μ_i is polynomial in x_i. Suppose there exist $d_i, \eta_i \geq 0$, and $\tau_i, \phi_i > 0$ such that the following expressions are SOS:*

$$\begin{aligned}
&\frac{\partial h_i^d}{\partial x_i}(x_i)[f_i(x_i) + g_i(x_i)u_i] + d_i\theta_i - q(x_i,u_i)h_i^d(x_i) \\
&\qquad - \sum_{k=1}^{p_i}(w_k(x_i,u_i)([u]_k - [u]_{k,min}) \\
&\qquad\qquad + v_k(x_i,u_i)([u]_{k,max} - [u]_k)), \quad (4a)\\
&\frac{\partial h_i^d}{\partial x_i}(x_i)[f_i(x_i) + g_i(x_i)\mu_i(x_i)] - d_i\beta_i \\
&\qquad\qquad - l(x_i)h_i^d(x) + m(x_i)h_i(x_i), \quad (4b)\\
&\frac{\partial h_i^d}{\partial x_i}(x_i)[f_i(x_i) + g_i(x_i)\mu_i(x_i)] \\
&\qquad\qquad + \alpha(h_i^d(x)) - r(x_i)h_i(x_i) - \eta_i, \quad (4c)
\end{aligned}$$

where $l(x_i), m(x_i), q(x_i,u_i), r(x_i)$ are SOS, and $w_k(x_i,u_i)$ as well as $v_k(x_i,u_i)$ are SOS for each $k = 1,\ldots,p_i$. Then d_i, $\tau_i = \frac{1}{\theta_i}$, $\phi_i = \frac{1}{\beta_i}$, and η_i satisfy Eqn. (3)*.*

Proof. We prove that Eqn. (4a) implies Eqn. (3a). The other SOS constraints can be proved in a similar manner. Consider $x_i \in \mathcal{C}_i$ and $[u]_{k,min} \leq [u]_k \leq [u]_{k,max}$ for all $k = 1,\ldots,p_i$. We thus have that $h_i^d(x_i) \geq 0$ since $\mathcal{D}_i \subseteq \mathcal{C}_i$. In addition, we have that $[u]_k - [u]_{k,min} \geq 0$, and $[u]_{k,max} - [u]_k \geq 0$. When expression (4a) is SOS, $q(x_i,u_i)$, $w_k(x_i,u_i)$, and $v_k(x_i,u_i)$ are SOS for all $k = 1,\ldots,p_i$, we have that the expression in Eqn. (4a) is non-negative. Therefore, if expression (4a) is SOS and τ_i is chosen as $\tau_i = 1/\theta_i$, then Eqn. (3a) holds. $\square$

We observe that the SOS constraints derived in Proposition 2 are bilinear (see the terms $d_i\theta_i$ and $d_i\beta_i$). Hence the resilience index cannot be readily computed by implementing these SOS constraints. We overcome this challenge by developing an alternating optimization procedure, as shown in Algorithm 1. In Algorithm 1, parameters τ_{max} and ϕ_{min} are the upper and lower bounds for τ_i and ϕ_i, respectively. If there exist no bound for τ_i and ϕ_i, then parameters τ_{max} and ϕ_{min} can be set as infinity and zero, respectively.

Algorithm 1 Algorithm for computing resilience index

Input: $\mathcal{S}_i$, τ_{max}, ϕ_{min}, and $\epsilon > 0$
Output: d_i, τ_i, ϕ_i, η_i
Initialization: $d_i = 0$
while $d_i \leq \sup_{x_i}\{h_i(x_i)\}$ **do**
  Solve for θ_i, β_i, η_i such that (4) is feasible with d_i fixed.
  if Eqn. (4) is feasible, $\frac{1}{\theta_i} \leq \tau_{max}$, $\frac{1}{\beta_i} \geq \phi_{min}$ **then**
    return d_i, $\tau_i = \frac{1}{\theta_i}$, $\phi_i = \frac{1}{\beta_i}$, and η_i
  else
    $d_i = d_i + \epsilon$
  end if
end while

V. Resilience Index After Interconnection

In this section, we consider a setting where multiple subsystems, with each being formulated by a hybrid system $\mathcal{H}_i$, are interconnected within a network. Suppose that a collection of subsystems $\{\mathcal{S}_i\}_{i=1}^N$ are interconnected within a network. In the network, each subsystem $\mathcal{S}_i$ follows the dynamics as given by Eqn. (2).

We note that the interconnected system can be formulated as a hybrid system $\mathcal{H}$ as defined in Section IV-A. In this case, the continuous state space is $\mathcal{X} = \prod_{i=1}^N \mathcal{X}_i$, and the discrete location is $\mathcal{L} = \{\texttt{offline}, \texttt{online}\}^N$. We observe that the continuous state is of dimension $n = \sum_{i=1}^N n_i$. Furthermore, the transitions among the discrete locations are the Cartesian product of discrete transitions of all subsystems, which is combinatorial in nature to capture all possible faults and attacks that can be incurred by the subsystems. Therefore, safety verification on $\mathcal{H}$ is computationally intractable for large-scale interconnected systems. In what follows, we derive how the resilience index of each subsystem changes due to interconnections. We further show how our proposed resilience index can be applied to efficiently verify safety constraints of the interconnected system.

A. Computation of Resilience Index After Interconnection

In the following, we first characterize the behaviors of any subsystem $\mathcal{S}_j$ when being interconnected. We define

$$\delta_j = \inf_x \Big\{ \frac{\partial h_j^d}{\partial x_j} \big[\sum_{i\neq j} W_{ij}(x_i, x_j) - \sum_{i\neq j} W_{ji}(x_j, x_i) \big] \Big\}. \quad (5)$$

We will show that the resilience index of a subsystem $\mathcal{S}_j$ after being interconnected can be bounded using one of the following two sets of inequalities

$$R_1 : \begin{cases} 0 \leq d_j' \leq d_j \leq \sup_{x_j}\{h_j(x_j)\} \\ -\frac{d_j'}{\tau_j'} \leq -\frac{d_j}{\tau_j} + \delta_j \\ \frac{\phi_j}{d_j + \phi_j \delta_j} d_j' - \phi_j' \leq 0 \\ \eta_j' \leq \delta_j + \min\{\frac{d_j}{\phi_j}, \eta_j + \inf_{x_j \in \mathcal{D}_j}\{\alpha_j(h_j(x_j) - d_j') \\ \qquad -\alpha_j(h_j(x_j) - d_j)\}\} \end{cases} \quad (6)$$

$$R_2 : \begin{cases} 0 \leq d_j \leq d_j' \leq \sup_{x_j}\{h_j(x_j)\} \\ -\frac{d_j'}{\tau_j'} \leq -\frac{d_j}{\tau_j} + \delta_j \\ \frac{d_j'}{\phi_j'} \leq \delta_j + \min\{\frac{d_j}{\phi_j}, \inf_{x_j \in \mathcal{D}_j}\{-\alpha_j(h_j^d(x_j))\} + \eta_j\} \\ \eta_j' \leq \delta_j + \eta_j - \sup_{x_j \in \mathcal{D}_j}\{\alpha_j(h_j(x_j) - d_j') \\ \qquad -\alpha_j(h_j(x_j) - d_j)\}\} \end{cases} \quad (7)$$

We define $\mathcal{D}_j' = \{x_j : h_j(x_j) - d_j' \geq 0\}$. The inequalities in R_1 and R_2 specify sets $\mathcal{D}_j'$ differently. The inequalities in R_1 specify that $\mathcal{D}_j' \supseteq \mathcal{D}_j$, whereas R_2 defines $\mathcal{D}_j' \subseteq \mathcal{D}_j$, which further leads to distinct behaviors when $x_j \in \mathcal{C}_j \setminus \mathcal{D}_j'$. In what follows, we show how the behavior of each subsystem following dynamics in Eqn. (2) can be characterized by the solutions to R_1 or R_2. This allows us to further verify the safety constraints for the interconnected system.

Theorem 1. *Consider that a collection of subsystems $\{\mathcal{S}_j\}_{j=1}^N$ are interconnected, and each $\mathcal{S}_j$ follows dynamics as given in Eqn. (2) for all $j = 1, \ldots, N$. We denote their resilience indices before being interconnected as $(d_k, \tau_k, \phi_k, \eta_k)$, where $k = 1, \ldots, N$. Define $\mathcal{D}_j' = \{x_j : h_j(x_j) - d_j' \geq 0\}$. If parameters d_j', τ_j', ϕ_j', and η_j' render either R_1 or R_2 to be feasible, then the following conditions hold for $\mathcal{S}_j$ after being interconnected:*

$$\frac{\partial h_j^d}{\partial x_j}(x_j)[f_j(x_j) + g_j(x_j)u_j + \sum_{i\neq j} W_{ij}(x_i, x_j) - \sum_{i\neq j} W_{ji}(x_j, x_i)] \geq -\frac{d_j'}{\tau_j'},\ \forall (x_j, u_j) \in \mathcal{C}_j \times \mathcal{U}_j \quad (8a)$$

$$\frac{\partial h_j^d}{\partial x_j}(x_j)[f_j(x_j) + g_j(x_j)\mu_j(x_j) + \sum_{i\neq j} W_{ij}(x_i, x_j) - \sum_{i\neq j} W_{ji}(x_j, x_i)] \geq \frac{d_j'}{\phi_j'},\ \forall x_j \in \mathcal{C}_j \setminus \mathcal{D}_j' \quad (8b)$$

$$\frac{\partial h_j^d}{\partial x_j}(x_j)[f_j(x_j) + g_j(x_j)\mu_j(x_j) + \sum_{i\neq j} W_{ij}(x_i, x_j) - \sum_{i\neq j} W_{ji}(x_j, x_i)] \geq -\alpha_j(h_j(x_j) - d_j') + \eta_j',\ \forall x \in \mathcal{D}_j' \quad (8c)$$

Proof. We first verify that if d_j', τ_j', ϕ_j', and η_j' satisfy R_1, then Eqn. (8) holds. We denote $\dot{h}_j^d$ as

$$\dot{h}_j^d = \frac{\partial h_j^d}{\partial x_j}(x_j)[f_j(x_j) + g_j(x_j)\mu_j(x_j) + \sum_{i\neq j} W_{ij}(x_i, x_j) - \sum_{i\neq j} W_{ji}(x_j, x_i)].$$

Suppose that d_j', τ_j', ϕ_j', and η_j' yield R_1 to be feasible. In this case, we have that $\mathcal{D}_j = \{x_j : h_j(x_j) - d_j \geq 0\} \subseteq \mathcal{D}_j' = \{x_j : h_j(x_j) - d_j' \geq 0\}$ due to $d_j' \leq d_j$. When $\mathcal{H}_j$ is at location $\texttt{offline}$, we have

$$\dot{h}_j^d \geq \frac{\partial h_j^d}{\partial x_j}(x_j)[f_j(x_j) + g_j(x_j)u_j] + \delta_j \quad (9)$$

$$\geq -\frac{d_j}{\tau_j} + \delta_j \geq -\frac{d_j'}{\tau_j'},\ \forall (x_j, u_j) \in \mathcal{C}_j \times \mathcal{U}_j \quad (10)$$

where inequality (9) holds Eqn. (5), the second inequality holds by Eqn. (3a), and the last inequality holds by the assumption that R_1 is feasible under $(d_j', \tau_j', \phi_j', \eta_j')$.

Consider the case where hybrid system $\mathcal{H}_j$ is at location $\texttt{online}$ and control law $\mu_j(x_j)$ is available. We have

$$\dot{h}_j^d \geq \frac{d_j}{\phi_j} + \delta_j \geq \frac{d_j'}{\phi_j'} \quad (11)$$

holds for all $x_j \in \mathcal{C}_j \setminus \mathcal{D}_j'$, where the first inequality holds by Eqn. (3b) and (5), and the second inequality holds by $(\mathcal{C}_j \setminus \mathcal{D}_j') \subseteq (\mathcal{C}_j \setminus \mathcal{D}_j)$ given the feasibility of R_1.

We finally consider the case where $x_j \in \mathcal{D}_j'$ by dividing our discussion into two scenarios. When $x_j \in \mathcal{D}_j' \setminus \mathcal{D}_j$, Eqn. (11) yields $\dot{h}_j^d \geq \frac{d_j}{\phi_j} + \delta_j \geq \eta_j'$, where the last inequality holds by the feasibility of R_1. When $x_j \in \mathcal{D}_j \subseteq \mathcal{D}'_j$, we have that $\dot{h}_j^d \geq -\alpha(h_j^d(x_j)) + \eta_j + \delta_j \geq -\alpha(h_j(x_j) - d'_j) + \eta'_j$ holds for all $x_j \in \mathcal{D}_j$, where the last inequality holds by the feasibility of R_1, i.e., $\eta'_j \leq \delta_j + \eta_j + \inf_{x_j \in \mathcal{D}_j}\{\alpha(h_j(x_j) - d'_j) - \alpha(h_j(x_j) - d_j)\}$.

We next verify that if d'_j, τ'_j, ϕ'_j, and η'_j satisfy R_2, then Eqn. (8) holds. Note that in this case, $\mathcal{D}'_j = \{x_j : h_j(x_j) - d'_j \geq 0\} \subseteq \mathcal{D}_j = \{x_j : h_j(x_j) - d_j \geq 0\}$. When hybrid system $\mathcal{H}_j$ is at location `offline`, Eqn. (8a) can be derived using Eqn. (9) and (10) given that d'_j, τ'_j, ϕ'_j, and η'_j satisfy R_2. We next consider that hybrid system $\mathcal{H}_j$ is at location `online`. We discuss two possible scenarios that can occur when $x_j \in \mathcal{C}_j \setminus \mathcal{D}'_j$. If $x_j \in \mathcal{C}_j \setminus \mathcal{D}_j$, we have

$$\dot{h}_j^d \geq \frac{d_j}{\phi_j} + \delta_j \geq \frac{d'_j}{\phi'_j}, \ \forall x_j \in \mathcal{C}_j \setminus \mathcal{D}_j \tag{12}$$

where the first inequality holds by Eqn. (3b) and the definition of δ_j, and the second inequality holds by the feasibility of R_2. If $x_j \in \mathcal{D}_j \setminus \mathcal{D}'_j$, we have that

$$\dot{h}_j^d \geq -\alpha(h_j^d(x_j)) + \delta_j + \eta_j \geq \frac{d'_j}{\phi'_j}, \ \forall x_j \in \mathcal{D}_j \setminus \mathcal{D}'_j, \tag{13}$$

where the first inequality holds by Eqn. (3c) and the definition of δ_j, and the second inequality holds by the feasibility of R_2. Combining Eqn. (12) and (13) yields Eqn. (8b).

We finally consider that $x_j \in \mathcal{D}'_j$. We have that $\dot{h}_j^d \geq -\alpha(h_j^d(x_j)) + \eta_j + \delta_j \geq -\alpha(h_j(x_j) - d'_j) + \eta'_j$ holds for all $x_j \in \mathcal{D}'_j$, where the first inequality holds by Eqn. (3c) and the definition of δ_j, and the second inequality holds by $\mathcal{D}'_j \subseteq \mathcal{D}_j$ along with the feasibility of R_2.

Combining the discussion above completes the proof. □

We observe that when function α_j is linear, computing the resilience indices after interconnection reduces to solving a linear system. In the following, we show that given the resilience indices of $\mathcal{S}_j$ before it is interconnected along with its control law μ_i, we can efficiently quantify how its resilience index changes due to interconnections by solving a set of inequalities given in Eqn. (6) and (7).

Theorem 2. *Consider that a collection of subsystems $\{\mathcal{S}_j\}_{j=1}^N$ are interconnected, and each $\mathcal{S}_j$ follows dynamics as given in Eqn.* (2) *for all $j = 1, \ldots, N$. We denote their resilience indices before being interconnected as $(d_k, \tau_k, \phi_k, \eta_k)$, where $k = 1, \ldots, N$. If parameters $d'_j, \eta'_j \geq 0$ and $\tau'_j, \phi'_j > 0$ satisfy either R_1 in Eqn.* (6) *or R_2 in Eqn.* (7)*, then $\mathcal{S}_j$ is $(d'_j, \tau'_j, \phi'_j, \eta'_j)$-resilient under dynamics* (2)*. Furthermore, $\mathcal{S}_j$ is safe with respect to $\mathcal{C}_j$ after being interconnected within the network.*

Proof. When parameters d'_j, τ'_j, ϕ'_j, and η'_j render either R_1 or R_2 to be feasible, we have that Eqn. (8) holds by using Theorem 1. By using Proposition 1 and Definition 1, we have that when $d'_j, \eta'_j \geq 0$ and $\tau'_j, \phi'_j > 0$, subsystem $\mathcal{S}_j$ is $(d'_j, \tau'_j, \phi'_j, \eta'_j)$-resilient and safe with respect to $\mathcal{C}_j$. □

Computing δ_j for each subsystem $\mathcal{S}_j$ requires to solve an optimization problem over joint system state $x \in \mathbb{R}^n$, where $n = \sum_{i=1}^N n_i$. To alleviate the computations in high dimensional state space, we approximate parameter δ_j as

$$\delta_j \geq \sum_{i \neq j} \inf_{(x_i, x_j) \in \mathcal{C}_i \times \mathcal{C}_j} \{\frac{\partial h_j^d}{\partial x_j}[W_{ij}(x_i, x_j) - W_{ji}(x_j, x_i)]\} := \tilde{\delta}_j.$$

By replacing δ_j with $\tilde{\delta}_j$ in Eqn. (8), we can apply similar approach to show that Theorem 1 and 2 still hold.

B. Feasibility of Resilience Index for Interconnected System

Consider an interconnected system consisting of N subsystems. We need to determine whether the inequalities in R_1 or R_2 need to be solved to apply Theorem 1 and 2 for safety verification of the interconnected system. One approach is to combine the inequalities in R_1 and R_2 by using a set of mixed integer constraints and big M-method [31], where the integer variable $y \in \{0, 1\}$ models whether R_1 or R_2 is solved. In this subsection, we show that we can determine whether R_1 or R_2 is feasible given the value of δ_j, and hence avoid solving the mixed integer program.

Theorem 3. *Consider a subsystem $\mathcal{S}_j$ whose resilience index is given as $(d_j, \tau_j, \phi_j, \eta_j)$ before being interconnected. Assume that $\alpha_j(h_j(x_j)) = zh_j(x_j)$ for some coefficient $z > 0$. If δ_j satisfies*

$$\delta_j \geq \max\{-\frac{d_j}{\phi_j}, -\eta_j - zd_j\}, \tag{14}$$

then there exist $d'_j, \eta'_j \geq 0$ and $\tau'_j, \phi'_j > 0$ such that the inequalities in R_1 are satisfied. If δ_j satisfies

$$\delta_j \geq \max\{-\frac{d_j}{\phi_j}, -\eta_j + z(\sup_{x_j}\{h_j(x_j)\} - d_j)\}, \tag{15}$$

then there exist $d'_j, \eta'_j \geq 0$ and $\tau'_j, \phi'_j > 0$ such that the inequalities in R_2 are satisfied.

Proof. Suppose that Eqn. (14) holds. We rewrite R_1 in the matrix form $A_j v_j \leq b_j$, where $v_j = [d'_j, \tau'_j, \phi'_j, \eta'_j]^\top$, $d'_j, \eta'_j \geq 0$, $\tau'_j, \phi'_j > 0$,

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & -\frac{d_j}{\phi_j} + \delta_j & 0 \\ z & 0 & 0 & 1 \\ -1 & \frac{d_j}{\tau_j} - \delta_j & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, b = \begin{bmatrix} d_j \\ 0 \\ \delta_j + \eta_j + zd_j \\ 0 \\ \delta_j + \frac{d_j}{\phi_j} \end{bmatrix}$$

When Eqn. (14) holds, we have that there exists no $r_j \geq 0$ such that $b_j^\top r_j < 0$. Using Farkas' Lemma [32], there must exist some $v_j \geq 0$ such that $A_j v_j \leq b_j$, and thus satisfies R_1. Similar proof technique can be applied to show that when Eqn. (15) holds, there must exist non-negative $(d'_j, \tau'_j, \phi'_j, \eta'_j)$ such that R_2 is satisfied. Noticing that $\phi'_j, \eta'_j = 0$ will make A_j and b_j ill-defined completes our proof. □

Using Theorem 3, we can decide whether we need to solve the inequalities given by R_1 or R_2 according to the value of δ_j. Therefore, we mitigate the computational complexity by solving N sets of inequalities. By observing that $-\eta_j - zd_j \leq$

$-\eta_j + z(\sup_{x_j}\{h_j(x_j) - d_j\})$, we further have that if there exist non-negative $(d_j', \tau_j', \phi_j', \eta_j')$ such that R_2 is satisfied, then there must also exist some non-negative solution to the inequalities in R_1. Finally, the sign of δ_j can be used to reason whether interconnections improve the resilience.

Proposition 3. *Consider a subsystem $\mathcal{S}_j$ whose resilience index is given as $(d_j, \tau_j, \phi_j, \eta_j)$ before being interconnected. If $\delta_j \geq 0$, then there exists a resilience index $(d_j', \tau_j', \phi_j', \eta_j')$ such that the set of inequalities given by R_1 is feasible. Furthermore, the interconnections improve the resilience of $\mathcal{S}_j$ in the sense that $\eta_j' \geq \eta_j$ holds when $x_j \in \mathcal{D}_j$ and*

$$d_j' \leq d_j, \quad \tau_j' = \tau_j, \quad \phi_j' \leq \phi_j.$$

Proof. We prove the proposition by giving a choice of non-negative $(d_j', \tau_j', \phi_j', \eta_j')$ that satisfies R_1. We first note that $\tau_j' = \tau_j \geq 0$ is a valid choice for parameter τ_j'. In this case, if $\delta_j \geq 0$, we have that d_j' can be chosen as $d_j' = d_j - \delta_j \tau_j \leq d_j$. Given this choice of d_j', we have that $0 \leq \phi_j' = \frac{d_j'}{d_j + \phi_j \delta_j}\phi_j \leq \phi_j$. Since α is an extended class $\mathcal{K}$ function, we have that $\alpha(h_j(x_j) - d_j') \geq \alpha(h_j(x_j) - d_j)$ for all x_j. Therefore, $\inf_{x_j \in \mathcal{D}_j}\{\alpha(h_j(x_j) - d_j') - \alpha(h_j(x_j) - d_j)\} \geq 0$ and $\inf_{x_j \in \mathcal{D}_j}\{\alpha(h_j(x_j) - d_j') - \alpha(h_j(x_j) - d_j) + \eta_j \geq \eta_j$. Thus $\eta_j' = \inf_{x_j \in \mathcal{D}_j}\{\alpha(h_j(x_j) - d_j') - \alpha(h_j(x_j) - d_j)\}\} + \delta_j + \eta_j \geq 0$. Let $\eta_j'' = \min\{\frac{d_j}{\phi_j}, \inf_{x_j \in \mathcal{D}_j}\{\alpha(h_j(x_j) - d_j') - \alpha(h_j(x_j) - d_j) + \eta_j\}\} + \delta_j > 0$. We have $(d_j', \tau_j', \phi_j', \eta_j')$ is a valid resilience index for $\mathcal{S}_j$ after interconnection. □

VI. Case Study

In this section, we demonstrate how the proposed resilience index can be used to analyze safety constraints of interconnected systems.

We consider two well-mixed, nonisothermal continuous stirred-tank reactors (CSTRs), denoted as $\mathcal{S}_1$ and $\mathcal{S}_2$. We assume that three parallel elementary irreversible exothermic reactions of the form $A \xrightarrow{r_1} B$, $B \xrightarrow{r_2} E$, and $A \xrightarrow{r_3} Q$ occurs, where A is the reactant species, B is the desired product, and E as well as Q are undesired byproducts. The states of $\mathcal{S}_1$ and $\mathcal{S}_2$ are denoted as $x_1 = [T_1, c_1]^\top$ and $x_2 = [T_2, c_2]^\top$, where T_i and c_i respectively represent temperature of the reactor and concentration of $\mathcal{S}_i$ with $i \in \{1, 2\}$. Each CSTR utilizes a jacket to remove or provide heat to the reactor to control the chemical reaction.

When the CSTRs are interconnected in series, their dynamics are given as

$$\dot{x}_1 = \begin{bmatrix} \frac{F_{e,1}}{V_1}(T_{0,1} - T_1) - \sum_{r=1}^{3} \frac{H_r}{\rho p} R_r(c_1, T_1) \\ \frac{F_{e,1}}{V_i}(c_{0,1} - c_1) - \sum_{r=1}^{3} R_r(c_1, T_1) \end{bmatrix} + \begin{bmatrix} \frac{u_1}{\rho p V_1} \\ 0 \end{bmatrix} \tag{16}$$

$$\dot{x}_2 = \begin{bmatrix} \frac{F_{e,2}}{V_2}(T_{0,2} - T_2) - \sum_{r=1}^{3} \frac{H_r}{\rho p} R_r(c_2, T_2) \\ \frac{F_{e,2}}{V_2}(c_{0,2} - c_2) - \sum_{r=1}^{3} R_r(c_2, T_2) \end{bmatrix} + \begin{bmatrix} \frac{u_1}{\rho p V_1} \\ 0 \end{bmatrix} + \frac{F_1}{V_2}\begin{bmatrix} T_1 - T_2 \\ c_1 - c_2 \end{bmatrix} \tag{17}$$

where $F_{e,i}$ is the flow rate, $R_r(c_i, T_i) = k_i \exp(-E_i / l T_i) c_i$, V_i is the volume, u_i is the rate of heat input/ removal. We

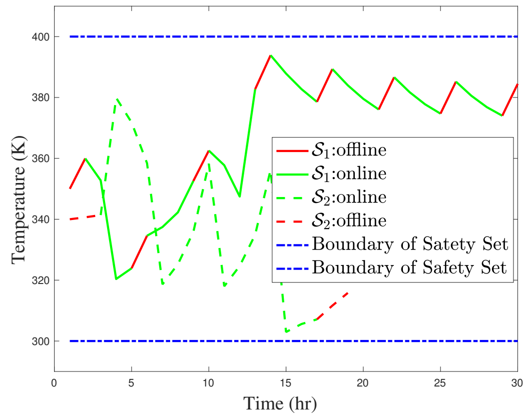

Fig. 1: This figure presents the temperature in CSTRs $\mathcal{S}_1$ and $\mathcal{S}_2$ after they are interconnected in series. The temperature of $\mathcal{S}_1$ and $\mathcal{S}_2$ are represented in solid and dashed lines. The portion plotted in red represents that the CSTR is faulty or compromised, whereas the portion plotted in green denotes that the desired rate of heat input is available.

follow the choices of process parameters given in [2] and summarize them in Table I. The set of admissible inputs is set as $|u_1| \leq 2.7 \times 10^6$ KJ/hr and $|u_2| \leq 2.8 \times 10^6$ KJ/hr. In Eqn. (17), we have that $W_{12}(x_1, x_2) = \frac{F_1}{V_2}\begin{bmatrix} T_1 - T_2 \\ c_1 - c_2 \end{bmatrix}$.

We assume that the safety constraints defined for CSTRs $\mathcal{S}_1$ and $\mathcal{S}_2$ are $\mathcal{C}_1 = \{T_1 : h_1(T_1) \geq 0\}$ and $\mathcal{C}_2 = \{T_2 : h_2(T_2) \geq 0\}$, where $h_i(T_i) = (T_i - 300)(400 - T_i)$ for all $i \in \{1, 2\}$. That is, the temperature in both CSTR needs to be within range $[300, 400]$K. Both CSTRs can be faulty or compromised, leading to manipulated rate of heat input $\tilde{u}_i$, where $i \in \{1, 2\}$.

TABLE I: Values of parameters used in Eqn. (16) and (17).

Parameter Value	Unit
$F_{e,1} = 4.998$, $F_{e,2} = 30.0$, $F_1 = 4.998$	m^3/hr
$V_1 = 1.0$, $V_2 = 3.0$	m^3
$T_{0,1} = 300.0$, $T_{0,2} = 300.0$	K
$E_1 = 5.0$, $E_2 = 7.53$, $E_3 = 7.53$	$\times 10^4$ KJ/kmol
$H_1 = -5.0$, $H_2 = -5.2$, $H_3 = -5.4$	$\times 10^4$ KJ/kmol
$\rho = 1000.0$	kg/m^3
$k_1 = 3.0 \times 10^6$, $k_2 = 3.0 \times 10^5$, $k_3 = 3.0 \times 10^5$	hr^{-1}
$l = 8.314$	KJ/kmol·K
$p = 0.231$	KJ/kg· K
$c_{0,1} = 4.0$, $c_{0,2} = 2.0$	kmol/m^3

We first compute the resilience indices of CSTRs $\mathcal{S}_1$ and $\mathcal{S}_2$ when they are not interconnected. Their resilience indices are given as $(d_1, \tau_1, \phi_1, \eta_1) = (2100, 0.0146, 0.308, 0)$ and $(d_2, \tau_2, \phi_2, \eta_2) = (500, 0.0292, 0.0222, 0)$. Following dynamics Eqn. (16) and (17), we have that the δ_2 defined in Eqn. (5) is negative, and hence we aim to solve R_2 to compute the resilience index of CSTR $\mathcal{S}_2$ after interconnection. We have that $(d_2', \tau_2', \phi_2', \eta_2') = (800, 0.0237, 0.1368, 0)$. We simulate the temperature in both CSTRs in Fig. 1. We plot the time period when the control input is compromised in red color, and the time period when the desired control law is online in green color. We observe that the fault or attack could manipulate the temperature in both CSTRs by changing the rate of heat input u_i. We further demonstrate that safety constraints defined on the temperature of $\mathcal{S}_1$ and $\mathcal{S}_2$ are met. We plot the boundaries of the safety set $\mathcal{C}_1$ and $\mathcal{C}_2$ using dash-dotted blue lines. We observe that T_1 and T_2 remain within $[300, 400]$K for all time $t \geq 0$, and hence safety constraint is satisfied if we can find a feasible resilience index, which demonstrates Theorem 2.

VII. Conclusion

In this paper, we investigated the problem of efficient safety verification for large-scale interconnected systems under faults and attacks. We developed a compositional resilience index for each subsystem to characterize its capability on tolerating faults and attacks without violating safety constraints. We showed that if a subsystem possessed a resilience index, then it satisfies the given safety constraint regardless of the faults and attacks. We formulated a sum-of-squares optimization program to compute the resilience index. When the resilience index and a safe control law of a subsystem were given, we proved that the resilience index of the subsystem after being interconnected could be computed by solving a system of linear inequalities. We further developed the sufficient conditions over the interconnections to guarantee the derived linear inequalities to be feasible. We demonstrated the proposed approach using a case study on interconnected chemical reactors.

References

[1] J. E. Sullivan and D. Kamensky, "How cyber-attacks in Ukraine show the vulnerability of the US power grid," *The Electricity Journal*, vol. 30, no. 3, pp. 30–35, 2017.

[2] N. H. El-Farra, A. Gani, and P. D. Christofides, "Fault-tolerant control of process systems using communication networks," *AIChE Journal*, vol. 51, no. 6, pp. 1665–1682, 2005.

[3] A. Greenberg, "Hackers remotely kill a Jeep on the highway–with me in it," 2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[4] C. Fan, K. Miller, and S. Mitra, "Fast and guaranteed safe controller synthesis for nonlinear vehicle models," in *International Conference on Computer Aided Verification*. Springer, 2020, pp. 629–652.

[5] K. Koscher, S. Savage, F. Roesner, S. Patel, T. Kohno, A. Czeskis, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," in *IEEE Symposium on Security and Privacy*. IEEE, 2010, pp. 447–462.

[6] Y. Chen, A. Singletary, and A. D. Ames, "Guaranteed obstacle avoidance for multi-robot operations with limited actuation: A control barrier function approach," *IEEE Control Systems Letters*, vol. 5, no. 1, pp. 127–132, 2020.

[7] N. Fijalkow, J. Ouaknine, A. Pouly, J. Sousa-Pinto, and J. Worrell, "On the decidability of reachability in linear time-invariant systems," in *22nd ACM International Conference on Hybrid Systems: Computation and Control*, 2019, pp. 77–86.

[8] S. Prajna, A. Jadbabaie, and G. J. Pappas, "A framework for worst-case and stochastic safety verification using barrier certificates," *IEEE Transactions on Automatic Control*, vol. 52, no. 8, pp. 1415–1428, 2007.

[9] L. Niu, D. Sahabandu, A. Clark, and P. Radha, "Verifying safety for resilient cyber-physical systems via reactive software restart," in *ACM/IEEE 13th International Conference on Cyber-Physical Systems (ICCPS)*. ACM/IEEE, 2022, pp. 104–115.

[10] A. Clark, "Verification and synthesis of control barrier functions," in *60th IEEE Conference on Decision and Control (CDC)*, 2021, pp. 6105–6112.

[11] Z. Manna and A. Pnueli, *Temporal Verification of Reactive Systems: Safety*. Springer Science & Business Media, 2012.

[12] I. M. Mitchell, A. M. Bayen, and C. J. Tomlin, "A time-dependent Hamilton-Jacobi formulation of reachable sets for continuous dynamic games," *IEEE Transactions on Automatic Control*, vol. 50, no. 7, pp. 947–957, 2005.

[13] D. P. Bertsekas and I. B. Rhodes, "On the minimax reachability of target sets and target tubes," *Automatica*, vol. 7, no. 2, pp. 233–247, 1971.

[14] J. F. Fisac, A. K. Akametalu, M. N. Zeilinger, S. Kaynama, J. Gillula, and C. J. Tomlin, "A general safety framework for learning-based control in uncertain robotic systems," *IEEE Transactions on Automatic Control*, vol. 64, no. 7, pp. 2737–2752, 2018.

[15] C. Sloth, G. J. Pappas, and R. Wisniewski, "Compositional safety analysis using barrier certificates," in *Proceedings of the 15th ACM International Conference on Hybrid Systems: Computation and Control*, 2012, pp. 15–24.

[16] Z. Lyu, X. Xu, and Y. Hong, "Small-gain theorem for safety verification of interconnected systems," *Automatica*, vol. 139, p. 110178, 2022.

[17] S. Coogan and M. Arcak, "A dissipativity approach to safety verification for interconnected systems," *IEEE Transactions on Automatic Control*, vol. 60, no. 6, pp. 1722–1727, 2014.

[18] M. Anand, A. Lavaei, and M. Zamani, "From small-gain theory to compositional construction of barrier certificates for large-scale stochastic systems," *arXiv preprint arXiv:2101.06916*, 2021.

[19] E. M. Clarke, "Model checking," in *International Conference on Foundations of Software Technology and Theoretical Computer Science*. Springer, 1997, pp. 54–56.

[20] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs for safety critical systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 8, pp. 3861–3876, 2016.

[21] X. Xu, "Constrained control of input–output linearizable systems using control sharing barrier functions," *Automatica*, vol. 87, pp. 195–201, 2018.

[22] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic control*, vol. 59, no. 6, pp. 1454–1467, 2014.

[23] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, and G. J. Pappas, "Robustness of attack-resilient state estimators," in *ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*, 2014, pp. 163–174.

[24] L. Sha, "Using simplicity to control complexity," *IEEE Software*, vol. 18, no. 4, pp. 20–28, 2001.

[25] F. Abdi, C.-Y. Chen, M. Hasan, S. Liu, S. Mohan, and M. Caccamo, "Guaranteed physical security with restart-based design for cyber-physical systems," in *2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS)*. ACM/IEEE, 2018, pp. 10–21.

[26] J. S. Mertoguno, R. M. Craven, M. S. Mickelson, and D. P. Koller, "A physics-based strategy for cyber resilience of CPS," in *Autonomous Systems: Sensors, Processing, and Security for Vehicles and Infrastructure 2019*, vol. 11009. International Society for Optics and Photonics, 2019, p. 110090E.

[27] H. Yang, B. Jiang, M. Staroswiecki, and Y. Zhang, "Fault recoverability and fault tolerant control for a class of interconnected nonlinear systems," *Automatica*, vol. 54, pp. 49–55, 2015.

[28] H. Yang, C. Zhang, Z. An, and B. Jiang, "Exponential small-gain theorem and fault tolerant safe control of interconnected nonlinear systems," *Automatica*, vol. 115, p. 108866, 2020.

[29] A. Al Maruf, L. Niu, A. Clark, J. S. Mertoguno, and R. Poovendran, "A compositional approach to safety-critical resilient control for systems with coupled dynamics," in *61st Conference on Decision and Control (CDC)*. IEEE, 2022, pp. 910–917.

[30] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[31] S. Boyd, S. P. Boyd, and L. Vandenberghe, *Convex Optimization*. Cambridge university press, 2004.

[32] S.-C. Fang and S. Puthenpura, *Linear Optimization and Extensions: Theory and Algorithms*. Prentice-Hall, Inc., 1993.