2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Temporal Logic Resilience for Cyber-Physical Systems

Adnane Saoud, Pushpak Jagtap, and Sadegh Soudjani

Abstract— **We consider the notion of resilience for cyber-physical systems, that is, the ability of the system to withstand adverse events while maintaining acceptable functionality. We use temporal logic to express the requirements on the acceptable functionality and define the resilience metric as the maximum disturbance under which the system satisfies the temporal requirements. We fix a parameterized template for the set of disturbances and form a robust optimization problem under the system dynamics and the temporal specifications to find the maximum value of the parameter. From the computational point of view, we show how this optimization can be solved for linear systems and provide under-approximations of the resilience metric for nonlinear systems using linear programs. The computations are demonstrated on the temperature regulation of buildings and adaptive cruise control.**

I. Introduction

Resilience has been studied by many research communities and it is broadly defined as *the ability of a system to withstand adverse events while maintaining an acceptable functionality.* For critical infrastructures, resilience is the main factor determining their reliability and is improved by continuously enhancing the prevention and absorption of disruptive events, and the recovery and adaptation for such events [1]. For IT systems, resilience is considered mainly against adverse cyber events, which are the cyber attacks that negatively impact the availability, integrity, or confidentiality of the system [2]. With the climate change increasing the extreme flood events, resilience metrics that consider the dynamical changes of the system have also received attention in the water research community to define and assess the resilience of water resource recovery facilities [3].

In this paper, we provide a notion of resilience for cyber-physical systems that integrates the time-evolution of the system with temporal logic to provide a quantitative measure on how the system can cope with disturbances. The temporal logic is used to encode formally the safety and other compliance requirements on the operation of the system and also express the expected behavior of the system to disturbances. We define resilience as the largest disturbance within a given (parameterized) set that can be applied to the system in its time evolution while still satisfying the temporal logic specification. This can also be interpreted as the minimum disturbance that needs to be applied to the system to falsify the specification. We focus on a discrete-time dynamical model of the system and express resilience requirements as linear temporal logic specifications over finite traces [4]. We show how the optimization for computing resilience can be solved exactly for linear systems and provide under approximations of the resilience metric for nonlinear systems using linear programs. We then provide numerical examples showing the merits of the proposed approach.

Our definition of resilience is substantially different from *robustness* for temporal specifications, which is defined as follows. Robustness of a system Σ with respect to a temporal specification ϕ is the largest value ε such that we still satisfy ϕ if we expand the solutions of Σ with a uniform ε over time and over trajectories [5], [6]. This definition does not take into account the dynamics of the system Σ and directly applies the expansion to the solution of Σ. In reality, disturbances and extreme events affect the time evolution of the system, and this needs to be integrated with any definition of resilience for dynamical systems.

Related work. The literature on defining quantitative semantics for different classes of temporal logic is relatively mature. These quantitative semantics study how well the system trajectories satisfy a given specification. The techniques include using discounting modalities that give less importance to distant events [7] and averaging modalities [8] where the semantics of standard modalities are extended using min, max, and a long-run average operator. The paper [5] considers real-valued signals and presents variants of robustness measures that indicate how far a given signal stands, in space and time, from satisfying or violating property and studies their sensitivity to the parameters of the system. The paper [6] considers the robust interpretation of Metric Temporal Logic to connect robust satisfaction of properties on discrete-time signals to their continuous-time counterparts. The authors in [9] present an efficient algorithm for computing the robustness degree in which a piecewise-continuous signal satisfies or violates a Signal Temporal Logic (STL) formula. Application of robustness metrics in specification-based monitoring of cyber-physical systems (CPS) is provided in [10] with a survey of theory and tools. The robustness metric is also used for temporal logic falsification of CPS [11]. STL is also used in [12] to study two important resilience properties of CPS, which are recoverability and durability.

All the works mentioned above study the robust satisfaction of properties for a given set of disturbances. In contrast,

Adnane Saoud is with College of Computing, University Mohammed VI Polytechnic, Benguerir, Morocco (e-mail: adnane.saoud@um6p.ma)

Pushpak Jagtap is with the Robert Bosch Center for Cyber-Physical Systems, Indian Institute of Science, Bangalore, India. His research is supported by the Google Research Grant, the SERB Start-up Research Grant, and the CSR Grants by Siemens and Nokia. (e-mail: pushpak@iisc.ac.in)

Sadegh Soudjani is with the School of Computing, Newcastle University, United Kingdom, and the Max Planck Institute for Software Systems, Germany. His research is supported by the following grants: EPSRC EP/V043676/1, EIC 101070802, and ERC 101089047. (e-mail: sadegh.soudjani@ncl.ac.uk)

we are looking at characterizing resilience to compute the largest disturbance within a given parameterized set. The work closest in spirit to our approach is the paper [13] that is limited to linear systems and safety specifications and studies properties of invariant sets when the size of the disturbance set changes with a scaling factor.

In summary, the main contributions of this paper are as follows. We provide a quantitative resilience metric by integrating the underlying dynamics with temporal logic specifications. We show how the related optimizations can be solved for linear systems and various types of specifications. We show that resilience with respect to convex or closed specifications enjoys some *nice* properties. Finally, we provide under-approximations of the resilience metric for nonlinear systems using linear programs. Due to space constraints, the proofs are omitted and will be published in an extended version.

II. Preliminaries

Notation: The symbols $\mathbb{R}$, $\mathbb{R}_{\geq 0}$, $\mathbb{N}$, and $\mathbb{N}_{\geq n}$ denote the set of real, nonnegative real numbers, nonnegative integer, and integers greater than or equal to $n \in \mathbb{N}$, respectively. We use $\mathbb{R}^{n\times m}$ to denote a vector space of real matrices with n rows and m columns. For a matrix $A \in \mathbb{R}^{n\times m}$, A^T represent transpose of matrix A. For a vector $x \in \mathbb{R}^n$, we use $\|x\|$ and $\|x\|_\infty$ to denote the Euclidean and infinity norm, respectively. We use $\mathbb{I}$ to denote the identity matrix. For a set of p points $C = \{c_1, c_2, \ldots, c_p\}$, $c_i \in \mathbb{R}^n$, the convex hull of C is represented by $\text{conv}(c_1, c_2, \ldots, c_p) := \{\alpha_1 c_1 + \alpha_2 c_2 + \ldots + \alpha_p c_p \mid c_i \in C, \alpha_i \geq 0, i \in \{1, 2, \ldots, p\}, \sum_{i=1}^{p} \alpha_i = 1\}$. An interval in $\mathbb{R}^n$ is a set denoted by $X = [\underline{x}_1, \overline{x}_1] \times [\underline{x}_2, \overline{x}_2] \times \ldots [\underline{x}_n, \overline{x}_n]$ and defined as $X = \{x \in \mathbb{R}^n \mid \underline{x}_i \leq x \leq \overline{x}_i,\ i \in \{1, 2, \ldots, n\}\}$. In particular, when $\underline{x}_i = \underline{x}$ and $\overline{x}_i = \overline{x}$ for all $i \in \{1, 2, \ldots, n\}$, then the interval X can be written in a compact form as: $X = [\underline{x}, \overline{x}]^n$. Given $x \in \mathbb{R}^n$ and $\varepsilon \geq 0$, $\Omega_\varepsilon(x) = \{z \in \mathbb{R}^n \mid \|z - x\|_\infty \leq \varepsilon\}$.

A. Discrete-Time Dynamical Systems

A discrete-time system is a tuple $\Sigma = (X, D, f)$, where $X \subset \mathbb{R}^n$ is the state space and $D \subset \mathbb{R}^n$ is the disturbance space which is assumed to be a compact set containing the origin. The evolution of the state of Σ is given by

$$x(k+1) = f(x(k)) + d(k), \quad k \in \mathbb{N}, \tag{1}$$

where $d(k) \in D$ represents the additive disturbance. The trajectory of system Σ of length $N+1$ is represented by $w_x = (x_0, x_1, \ldots, x_{N-1}) \in X^N$, where x_k represents the value of trajectory starting from a state $x(0) = x_0 \in X$ at k^{th} instance (i.e., $x(k)$).

Linear temporal logic (LTL) provides a high-level language for describing the desired behavior of a dynamical system. Formulas in this logic are constructed inductively using a set of atomic propositions and combining them via Boolean operators [14]. Consider a finite set of atomic propositions AP that defines the alphabet $\Sigma_a := 2^{\mathsf{AP}}$. Each letter of this alphabet evaluates a subset of the atomic propositions as true. In this work, we consider LTL specifications over finite words, referred to as LTL_F, where the letters form finite words defined as $\boldsymbol{\omega} = (\omega_0, \omega_1, \omega_2, \ldots, \omega_{N-1}) \in \Sigma_a^N$ for some $N \in \mathbb{N}$. These words are connected to trajectories of the system Σ via a measurable labeling function $\mathsf{L} : X \to \Sigma_a$ that assigns letters $\alpha = \mathsf{L}(x)$ to state $x \in X$. That is, any finite trajectory $w_x = (x_0, x_1, \ldots, x_{N-1})$ is mapped to the set of finite words Σ_a^N, as $\boldsymbol{\omega} = \mathsf{L}(w_x) := (\mathsf{L}(x_0), \mathsf{L}(x_1), \mathsf{L}(x_2), \ldots \mathsf{L}(x_{N-1}))$.

Definition 2.1: An LTL_F formula over a set of atomic propositions AP is constructed inductively as

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

with $p \in \mathsf{AP}$, and ψ_1, ψ_2, ψ being LTL_F formulas.

Given a finite word $\boldsymbol{\omega}$ of length N and an LTL_F formula ψ, we inductively define when an LTL_F formula is true at the n^{th} step $(n < N)$ and denoted by $\boldsymbol{\omega}_n \models \psi$, as follows:

- $\boldsymbol{\omega}_n \models \mathsf{true}$ always hold and $\boldsymbol{\omega}_n \models \mathsf{false}$ does not hold.
- An atomic proposition, $\boldsymbol{\omega}_n \models p$ for $p \in \mathsf{AP}$ holds if $p \in \boldsymbol{\omega}_n$.
- A negation, $\boldsymbol{\omega}_n \models \neg p$, holds if $\boldsymbol{\omega}_n \not\models p$.
- A logical conjunction, $\boldsymbol{\omega}_n \models \psi_1 \wedge \psi_2$, holds if $\boldsymbol{\omega}_n \models \psi_1$ and $\boldsymbol{\omega}_n \models \psi_2$.
- A logical disjunction, $\boldsymbol{\omega}_n \models \psi_1 \vee \psi_2$, holds if $\boldsymbol{\omega}_n \models \psi_1$ or $\boldsymbol{\omega}_n \models \psi_2$.
- A temporal next operator, $\boldsymbol{\omega}_n \models \bigcirc\psi$, holds if $\boldsymbol{\omega}_{n+1} \models \psi$. Similarly, for $0 \leq j < N - n$, $\boldsymbol{\omega}_n \models \bigcirc^j\psi$, holds if $\boldsymbol{\omega}_{n+j} \models \psi$.
- A temporal until operator, $\boldsymbol{\omega}_n \models \psi_1 \,\mathsf{U}\, \psi_2$, holds if for some m such that $n \leq m < N$, we have $\boldsymbol{\omega}_m \models \psi_2$ and for all $n \leq k < m$, we have $\boldsymbol{\omega}_k \models \psi_1$.
- A temporal always operator, $\boldsymbol{\omega}_n \models \Box\psi$, holds if for all m such that $n \leq m < N$, we have $\boldsymbol{\omega}_n \models \psi$. Similarly, for $0 \leq j < N - n$, $\boldsymbol{\omega}_n \models \Box^j\psi$ holds if for all $n \leq m \leq n + j$, we have $\boldsymbol{\omega}_m \models \psi$.
- A temporal eventually operator, $\boldsymbol{\omega}_n \models \Diamond\psi$, holds if for some m such that $n \leq m < N$, we have $\boldsymbol{\omega}_n \models \psi$. Similarly, for $0 \leq j < N - n$, $\boldsymbol{\omega}_n \models \Diamond^j\psi$, holds if for some m such that $n \leq m < n + j$, we have $\boldsymbol{\omega}_{n+j} \models \psi$.

For trajectory $w_x = (x_0, x_1, \ldots, x_{N-1}) \in X^N$, we say that $w_x \models \psi$ if for $\boldsymbol{\omega} = \mathsf{L}(w_x) := (\mathsf{L}(x_0), \mathsf{L}(x_1), \ldots, \mathsf{L}(x_{N-1}))$, we have $\boldsymbol{\omega} \models \psi$. Similarly, for a set of trajectories $\mathcal{X} \subseteq X^N$, we say that $\mathcal{X} \models \psi$, if $w_x \models \psi$ for all $w_x \in \mathcal{X}$.

Remark 1: Our notion of resilience is general, but for computational purposes, we restrict ourselves to the following specifications over words of length N: $\Box p$, $\bigcirc p$, $\Diamond p$, with $p \in \mathsf{AP}$, and conjunctions over them. Note that all LTL_F can be represented using Deterministic Finite Automata (DFA) [15] and effectively, one can represent them using sequences of reach and avoid specifications (i.e., $\psi = \Diamond p \wedge \Box\neg q$, where $p, q \in \Sigma_a$) [16, Section III.b]. Thus, one can easily use the results provided in the paper for any LTL_F specification using the properties provided in Proposition 3.1.

III. Characterizations of Resilience

The goal of the paper is to provide characterizations and algorithmic procedures for computing resilience with respect to different classes of systems and specifications.

A. Resilience for LTL$_F$ Specifications

Consider the system Σ in (1), with a set of disturbances given by ball with respect to infinity norm centered at zero: $D := \Omega_\varepsilon(0)$. We denote by $\xi(x,\varepsilon)$ the set of trajectories starting from some $x \in X$ with such a disturbance set:

$$\xi(x,\varepsilon) := \{(x_0, x_1, x_2, \ldots) \,|\, x_0 = x,\, x_{k+1} \in f(x_k) + D\}\,. \quad (2)$$

Note that $\xi(x,0)$ contains only the disturbance-free trajectory of the system (nominal trajectory).

Definition 3.1: Consider the dynamical system Σ in (1), an LTL$_F$ specification ψ and a point $x \in X$. We define the *resilience* of the system Σ with respect to the initial condition x and the specification ψ as a function $g_\psi : X \to \mathbb{R}_{\geq 0} \cup \{+\infty\}$ with:

$$g_\psi(x) = \begin{cases} \sup\{\varepsilon \geq 0 \,|\, \xi(x,\varepsilon) \vDash \psi\}\,, & \text{if } \xi(x,0) \vDash \psi \\ 0 & \text{if } \xi(x,0) \nvDash \psi. \end{cases} \quad (3)$$

where $\xi(x,\varepsilon) \vDash \psi$ indicates that all trajectories in $\xi(x,\varepsilon)$ satisfies the specification.

B. Structural Properties of Resilience

In this subsection, we prove the structural properties of the resilience metric in Definition. 3.1 utilizing the inductive definition of temporal specifications.

Proposition 3.1: Consider the dynamical system Σ in (1), an LTL$_f$ specification ψ, a set $X \subseteq \mathbb{R}^n$ and a point $x \in X$. The following properties hold:

(i) When ψ is the true specification, $g_\psi(x) = +\infty \;\forall x \in X$.
(ii) When ψ is the false specification, $g_\psi(x) = 0 \;\forall x \in X$.
(iii) For any specification $\psi = \psi_1 \wedge \psi_2$, we have that $g_\psi(x) = \min\{g_{\psi_1}(x), g_{\psi_2}(x)\} \;\forall x \in X$.
(iv) For any specification $\psi = \psi_1 \vee \psi_2$, we have that $g_\psi(x) \geq \max\{g_{\psi_1}(x), g_{\psi_2}(x)\} \;\forall x \in X$.
(v) For any specification $\psi = \neg\phi$, we have that $g_\psi(x) g_\phi(x) = 0 \;\forall x \in X$.
(vi) For $X \subset \mathbb{R}^n$, $g_\psi(X) = \inf_{x \in X} g_\psi(x)$.

Now, we provide sufficient conditions on the dynamics of the system Σ and the specification ψ allowing us to replace the $\sup$ operator with the $\max$ operator in the definition of g_ψ in (3), which makes the computation of the resilience metric computationally tractable. To do this, we introduce the class of closed specifications defined below. Given a sequence of trajectories $w_{x,i}$, $i \in \mathbb{N}$, with $w_{x,i} = x_{0,i}, x_{1,i}, x_{2,i} \ldots$, the limit of $w_{x,i}$ is defined by $w_x = \lim_{i\to\infty} w_{x,i} = x_0, x_1, x_2 \ldots$, where for all $j \in \mathbb{N}$, $x_j = \lim_{i\to\infty} x_{j,i}$. The sequence $w_{x,i}$ is called converging whenever w_x exists. Hence, the limit of a sequence of trajectories can be seen as an element-wise limit of its components.

Definition 3.2 (Closed specification): Consider a metric space X, an LTL$_F$ formula ψ is said to be closed if the following holds: for any converging sequence of trajectories $w_{x,i}$, $i \in \mathbb{N}$, if for all $i \in \mathbb{N}$, $w_{x,i} \vDash \psi$, then $w_x = \lim_{i\to\infty} w_{x,i} \vDash \psi$.

Intuitively, the closedness property states that a specification is preserved when going from a sequence of trajectories to its element-wise limit. The complete characterization of the fragment of LTL$_F$ specifications that are closed is out of the scope of this paper and will be explored in future research. An example of closed specifications is reported below.

Example 3.1: Consider a set $A \subseteq \mathbb{R}^n$ and $N \in \mathbb{N}_{>0}$. If the set A is a closed subset of $\mathbb{R}^n$, then the LTL$_F$ formulas $\psi_1 = \Box^N A$, $\psi_2 = \bigcirc^N A$ and $\psi_3 = \Diamond^N A$ are closed.

Proposition 3.2: Consider the discrete-time system Σ in (1) defined on a metric space X. Consider $x \in X$ and an LTL$_F$ specification ψ. If the map $f : \mathbb{R}^n \to \mathbb{R}^n$ is continuous and if the specification ψ is closed, then:

$$g_\psi(x) = \begin{cases} \max\{\varepsilon \geq 0 \,|\, \xi(x,\varepsilon) \vDash \psi\}\,, & \text{if } \xi(x,0) \vDash \psi, \\ 0, & \text{if } \xi(x,0) \nvDash \psi. \end{cases}$$

We also provide sufficient conditions under which the map $g_\psi(x)$ remains bounded for an $x \in X$.

Proposition 3.3: Consider the dynamical system Σ in (1), an LTL$_F$ specification ψ and a point $x \in X$. If the set $\mathsf{L}^{-1}(\psi) \subseteq \{\mathbb{R}^n\}^N$ is a bounded[1] subset of $\{\mathbb{R}^n\}^N$, then $g_\psi(x)$ is bounded, where N represents the length of the trajectories corresponding to the LTL$_F$ specification ψ.

C. Resilience Properties for Linear Systems

In this part, we introduce the concept of convex specifications and present an efficient approach for the computation of the resilience metric for the class of linear systems and convex specifications.

Definition 3.3 (Convex specification): Consider a vector space C, an LTL$_F$ formula ψ is said to be convex if the following holds: for trajectories $w_{x,i}$, $i \in \{1,2\}$, if $w_{x,i} \vDash \psi$, then for any trajectory $w_x = \lambda w_{x,1} + (1-\lambda) w_{x,2}$, $\lambda \in [0,1]$, we have that $w_x \vDash \psi$.

Intuitively, the convexity property states that the specification is preserved under a convex hull operator. The complete characterization of the fragment of LTL$_F$ specifications that are convex is out of the scope of this paper and will be explored in future research. An example of convex specifications is reported next.

Example 3.2: Consider a set $A \subseteq \mathbb{R}^n$ and $N \in \mathbb{N}_{>0}$. If the set A is convex, then the specifications $\psi_1 = \Box^N A$, $\psi_2 = \bigcirc^N A$ are convex.

Now, consider the case where the objective is to compute $g_\psi(X)$ for a set $X \subset \mathbb{R}^n$. A straightforward approach that was mentioned earlier in the property (vi) of Proposition 3.1 is to use the fact that $g_\psi(X) = \inf_{x\in X} g_\psi(x)$, which requires computing $g_\psi(x)$ for all $x \in X$ and that can be computationally infeasible for continuous sets. In this part, we present an efficient approach to compute $g_\psi(X)$

[1]A set $Z \subseteq \{\mathbb{R}^n\}^N$ is said to be bounded if there exists $\gamma \geq 0$ such that for any finite trajectory $z_0 z_1 z_2 \ldots z_{N-1} \in Z$, we have $\|z_i\| \leq \gamma$ for all $0 \leq i < N$.

for the case where the set X can be written as a convex closure of a finite number of points. Our result relies on the superposition principle for linear systems and the introduced class of convex specifications.

Theorem 3.4: Consider the discrete-time linear system in (1). Consider $X = \text{conv}(c_1, c_2, \ldots, c_p) \subset \mathbb{R}^n$ and a convex specification ψ. We have $g_\psi(X) = \min_{i=1,2,\ldots,p} g_\psi(c_i)$.

In Sections IV-V, we provide results on the computation of the resilience metric for linear and a class of nonlinear systems for various specifications.

IV. Computation of Resilience for Linear Systems

In this section, we show how the resilience metric can be computed exactly for some classes of specifications, such as the exact time reachability and finite-horizon safety. Moreover, we show how it can be approximated arbitrarily closed for finite-horizon reachability properties.

A. Exact-Time Reachability

Consider the linear discrete-time system Σ defined by:

$$x_{k+1} = Ax_k + d_k, \tag{4}$$

with $x_k, d_k \in \mathbb{R}^n, k \in \mathbb{N}$ and reachability at a specific time $N \in \mathbb{N}$ as $\psi = \bigcirc^N \Gamma$, for some polytopic set Γ. We have the following result showing that the computation of the resilience metric for linear systems and reachability at a specific time point specification boils down to a linear optimization problem.

Theorem 4.1: Consider the linear system Σ in (4) and the specification $\psi = \bigcirc^N \Gamma$, for $N \in \mathbb{N}$, where Γ is a polytope $\Gamma = \{x \in X \,|\, Gx \leq H\}$ with $G \in \mathbb{R}^{q \times n}$ and $H \in \mathbb{R}^q$, $q \in \mathbb{N}$. We have

$$g_\psi(x) = \min\{\varepsilon \geq 0 \,|\, P \geq 0, PA_b = E, PB_b \leq \varepsilon F(x)\} \tag{5}$$

with

- $A_b := \begin{bmatrix} \mathbb{I} \\ -\mathbb{I} \end{bmatrix} \in \mathbb{R}^{2nN \times nN}$ and $B_b := \begin{bmatrix} \mathbf{1} \\ \mathbf{1} \end{bmatrix} \in \mathbb{R}^{2nN}$
- $E = [GA^{N-1}, GA^{N-2}, \ldots, GA, G] \in \mathbb{R}^{q \times nN}$
- $F(x) = H - GA^N x \in \mathbb{R}^q$.

B. Finite-Horizon Safety Specifications

In this section, we provide a closed-form expression of the resilience metric for the case of linear systems and finite-horizon safety specifications.

Theorem 4.2: Consider the linear system Σ in (4) with finite-horizon safety specification $\psi = \square^N \Gamma$, where $\Gamma = \{x \in X \,|\, Gx \leq H\}$, for some $N \in \mathbb{N}$. We have

$$g_\psi(x) = \max\{\varepsilon \geq 0 \mid P \geq 0, PA_b = E, PB_b \leq \varepsilon F(x)\},$$

$$E = \begin{bmatrix} G & 0 & 0 & \ldots & 0 & 0 \\ GA & G & 0 & \ldots & 0 & 0 \\ GA^2 & GA & G & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ GA^{N-1} & GA^{N-2} & GA^{N-3} & \ldots & GA & G \end{bmatrix},$$

$$F(x) = [H - GAx \; H - GA^2x \; \ldots \; H - GA^N x].$$

Let us remark that by defining $\psi_i = \bigcirc^i \Gamma$, one gets $\psi = \wedge_{i=0}^N \psi_i$. Therefore, it follows from (iii) in Proposition 3.1 that $g_\psi(x) = \min_i g_{\psi_i}(x)$. Hence, one can state the previous result in terms of reachability with exact time, with g_{ψ_i} computed previously in Theorem 4.1.

C. Finite-Horizon Reachability

In this section, we provide an approach to compute the resilience metric for linear systems and finite-horizon reachability specifications, by resorting to the the exact time reachability approach in Section IV-A.

Consider the linear system Σ in (4) with finite-horizon reachability specification $\psi = \Diamond^N \Gamma$ for some set Γ as a polytope $\Gamma := \{x \in X \,|\, Gx \leq H\}$. Then, we have

$$g_\psi(x) = \max \varepsilon \geq 0, \; s.t. \text{ for all } d_0, \ldots, d_{N-1} \in \Omega_\varepsilon(0)$$
$$\begin{cases} Gx \leq H \text{ or} \\ G(Ax + d_0) \leq H \text{ or} \\ G(A^2x + Ad_0 + d_1) \leq H \text{ or} \\ \vdots \\ G(A^N x + A^{N-1}d_0 + \ldots + d_{N-1}) \leq H. \end{cases} \tag{6}$$

in view of (v) in Proposition 3.1, one can select $\psi_i = \bigcirc^i \Gamma$, to get $\psi = \vee_{i=0}^N \psi_i$. Therefore, we can use the results of reachability in an exact time presented in Section IV-A to obtain a lower bound on the resilience metric given by $g_\psi(x) \geq \max_i g_{\psi_i}(x)$.

V. Computation of Resilience for Nonlinear Systems

In this section, we extend the approaches to compute the resilience metric to the case of nonlinear systems. Since the computation of resilience for different types of specifications relies on reachability with the exact time as a building block, in this section, we focus on reachability with an exact time specification. The extension to other specifications can be done following the approaches presented in the previous section.

Consider the reachability at a specific time point: $\psi = \bigcirc^N \Gamma$, for some set Γ defined as a polytope $\Gamma = \{x \in X \,|\, Gx \leq H\}$. We provide a linear optimization-based solution for computing $g_\psi(x)$ for nonlinear systems.

Theorem 5.1: Consider the nonlinear system Σ given by

$$x(k+1) = f(x(k)) + d(k), \; x(k) \in X \subseteq \mathbb{R}^n, \; k \in \mathbb{N} \tag{7}$$

and the specification $\psi = \bigcirc^N \Gamma$, where Γ is the polytope $\Gamma = \{x \in X \,|\, Gx \leq H\}$. Assume the existence of $\overline{\alpha}_{i,j}$, $\underline{\alpha}_{ij}$, $i, j \in \{1, 2, \ldots, n\}$, such that for all $x \in X$:

$$\underline{\alpha}_{ij} \leq \frac{\partial f_i}{\partial x_j} \leq \overline{\alpha}_{ij}, \; i, j \in \{1, 2, \ldots, n\}, \tag{8}$$

Consider the matrices $B_1, B_2, \ldots, B_N \in \mathbb{R}^{n \times n}$ defined as

$$B_{k,ij} = \max\left(\sum_{h=1}^{n} G_{ih} \underline{D}_{k,hj}, \sum_{h=1}^{c} G_{ih} \overline{D}_{k,hj} \right),$$

where $B_{k,ij}$ represents the coefficient corresponding to the position (i,j) of the matrix B_k, $k \in \{1,2,\ldots,N\}$, and the matrices $\underline{D}_k, \overline{D}_k$ are given with $\underline{D}_k = \underline{A}^k$ and $\overline{D}_k = \overline{A}^k$, with $\underline{A}, \overline{A}$ defined for $i,j \in \{1,2,\ldots,n\}$ by $\underline{A}_{ij} = \underline{\alpha}_{ij}$ and $\overline{A}_{ij} = \overline{\alpha}_{ij}$. Then, we have

$$g_\psi(x) \geq \max\{\varepsilon \geq 0 \,|\, B_N x + B_{N-1} d_0 + \ldots + d_{N-1} \leq H \text{ for all } d(0),\ldots,d(N-1) \in \Omega_\varepsilon(0)\}, \quad (9)$$

Theorem 5.1 shows how to transform the problem of computing the resilience metric for nonlinear systems and exact-time reachability, into a problem for a linear system that can be resolved using the approach proposed in Section IV-A.

VI. Case Studies

Temperature Regulation. We consider the problem of regulating the temperature in a circular building of 9 rooms. The dynamics of the room temperatures are given by

$$T_i(k+1) = T_i(k) + \alpha(T_{i+1}(k) + T_{i-1}(k) - 2T_i(k)) + \beta(T_e + \delta T_e - T_i(k)), \qquad i \in \{1,2,\ldots,9\},$$

where T_{i+1} and T_{i-1} are the temperatures of the neighbor rooms (here $T_0 = T_9$ and $T_{9+1} = T_1$), $T_e = 0°C$ is the outside temperature, considered as a disturbance and α and β are the conduction factors. The numerical parameters are taken from [17] and given by $\alpha = 0.45$ and $\beta = 0.045$.

The desired behavior of the system is as follows: The temperatures of the 9 rooms initiated in the set $X_0 = [24,25]^9$ should reach the target set $X_T = [21,22]^9$ exactly at $N = 3$ steps while remaining in the safe set $X_S = [20.5,25]^9$. This behavior can be described by the LTL$_F$ formula:

$$\psi = \psi_1 \wedge \psi_2, \text{ with } \psi_1 = \Box^3 X_S \text{ and } \psi_2 = \bigcirc^3 X_T. \quad (10)$$

The objective is to compute the range of admissible external disturbances δT_e under which any trajectory of the system initiated in the set X_0 satisfies ψ. Since the system is linear and the set of initial states X_0 is convex, we rely on Theorems 4.1, 4.2 and 3.4 to compute the resilience metric. The numerical implementations show that the resilience metric is given by the set $\Delta_{T_e} = [-2.23, 2.23]°C$.

Figure 1 (top) shows the nominal trajectories (with $\delta T_e = 0$) of the system for the 9 rooms. Figure 1 (bottom) shows the trajectories of the system for the 9 rooms with a disturbance δT_e randomly chosen in the set $\Delta_{T_e} = [-2.23, 2.23]°C$. In order to show the satisfaction of ψ by the nine rooms, we also represent in green the boundaries of the target set X_T and in red the boundaries of the safe set X_S.

Adaptive Cruise Control. Consider a vehicle moving along a straight road. The dynamics of the vehicle is adapted from [17] and given by the following difference equation:

$$v(k+1) = v(k) + \frac{\tau}{m}(f_0 - f_1 v - f_2 v^2), \quad (11)$$

where $m > 0$ is the mass of the vehicle, $v \geq 0$ represents the velocity of the vehicle and the term $f_0 - f_1 - f_2 v^2$ includes the rolling resistance and aerodynamics and τ represents a

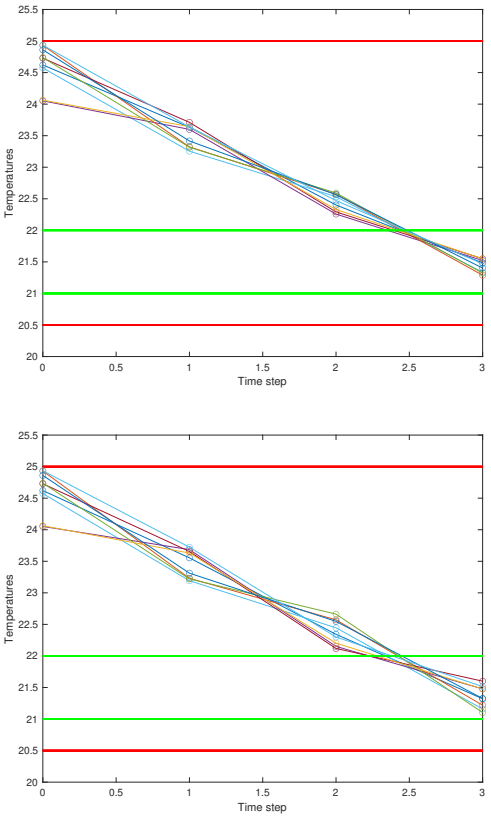

Fig. 1. Evolution of the temperatures in the nine rooms with a disturbance $\delta T_e = 0$ (top) and with a disturbance δT_e randomly chosen in the set $\Delta_{T_e} = [-2.23, 2.23]°C$ (bottom). The green and red boundaries represent target set X_T and safe set X_s, respectively.

sampling period. Moreover, we include a lead vehicle whose velocity $v_0 \geq 0$ is constant. The dynamics of the system are

$$\begin{cases} h(k+1) &= h(k) + \tau(v_0 + \delta v_0 - v(k)) \\ v(k+1) &= v(k) + \frac{\tau}{m}(f_0 + \delta f_0 - f_1 v(k) - f_2 v(k)^2), \end{cases}$$

where δv_0 is the uncertainty on the velocity v_0 of the lead vehicle and δf_0 is the uncertainty on the parameter f_0. The desired behavior can be described by the following LTL$_F$ formula: $\psi := \psi_1 \wedge \psi_2 \wedge \psi_3$ with $\psi_1 := \Box^{15} X_S$, $\psi_2 := X_1 \rightarrow \bigcirc^3 X_{T_1}$, and $\psi_3 := X_2 \rightarrow \bigcirc^{11} X_{T_2}$. This behavior can be interpreted as follows: the relative position should remain in the safe set $X_S = [h_{S,\min}, h_{S,\max}] \times [v_{S,\min}, v_{S,\max}]$, whenever the state of the vehicle belongs to the set $X_1 = [h_{1,\min}, h_{1,\max}] \times [0, +\infty)$, i.e, the relative distance is between $h_{1,\min}$ and $h_{1,\max}$, the relative position and velocity should reach the set $X_{T_1} = [h_{T_1,\min}, h_{T_1,\max}] \times [v_{T_1,\min}, v_{T_1,\max}]$ in 3 steps, and whenever the state of the vehicle belongs to the set $X_2 = [h_{1,\min}, h_{1,\max}] \times [0, +\infty)$, i.e, the relative distance is between $h_{2,\min}$ and $h_{2,\max}$, the relative position and velocity should reach the set $X_{T_2} = [h_{T_2,\min}, h_{T_2,\max}] \times [v_{T_2,\min}, v_{T_2,\max}]$ in 11 steps.

The objective is to compute the resilience metric under which the trajectory of the system initiated from $x_0 = (60, 2)$ satisfies ψ. The numerical values of the vehicle parameters and the considered specifications are given in Table I.

To deal with this nonlinear system, we use the approach developed in Section V. First, one can easily check that

TABLE I

VEHICLE AND SAFETY PARAMETERS

Parameter	Value	Unit
M	1370	Kg
f_0	51.0709	N
f_1	5	Ns/m
f_2	0.4161	Ns^2/m^2
$h_{1,\min}$	61	m
$h_{1,\max}$	61.5	m
$h_{2,\min}$	62.75	m
$h_{2,\max}$	63	m
$h_{T_1,\min}$	62.75	m
$h_{T_1,\max}$	63.5	m
$v_{T_1,\min}$	13	m/s
$v_{T_1,\max}$	14	m/s
$h_{T_2,\min}$	61.75	m
$h_{T_2,\max}$	62.5	m
$v_{T_2,\min}$	16.5	m/s
$v_{T_2,\max}$	17.5	m/s
$h_{S,\min}$	59.5	m
$h_{S,\max}$	64.5	m
$v_{S,\min}$	1	m/s
$v_{S,\max}$	18	m/s

the values of the parameters $\alpha_{i,j}$, $i,j \in \{1,2\}$, given by $\underline{\alpha}_{11} = \overline{\alpha}_{11} = 1$, $\underline{\alpha}_{12} = \overline{\alpha}_{12} = -1$, $\underline{\alpha}_{21} = \overline{\alpha}_{21} = 0$, $\underline{\alpha}_{22} = 1 - \frac{\tau}{m} - 2f_2 v_{S,\max}$ and $\overline{\alpha}_{22} = 1 - \frac{\tau}{m} - 2f_2 v_{S,\min}$ satisfy the inequalities in (8), where the bounds on $\underline{\alpha}_{22}$ and $\overline{\alpha}_{22}$ follows from the fact that we are interested in dealing with velocities of the following vehicle within the interval $[v_{S,\min}, v_{S,\max}]$. Hence, in view of Theorem 5.1, one can use the linear program in (9) to compute an approximation of the resilience metric g_ψ. The numerical implementations show that the value of the resilience metric is given by $\Delta v_0 = [-0.8, 0.8]$ and $\Delta f_0 = [-1096, 1096]$.

Figure 2 shows examples of 4 trajectories under disturbances chosen randomly within the admissible resilience metric set, i.e., with $\delta v_0 \in [-0.8, 0.8]$ and $\delta f_0 \in [-1096, 1096]$, together with the nominal trajectory (in blue). In order to show the satisfaction of ψ by the vehicle, we also represent in blue the boundaries of the first target set X_{T_1}, in green the boundary of the second target set X_{T_2} and in red the boundaries of the safe set X_S.

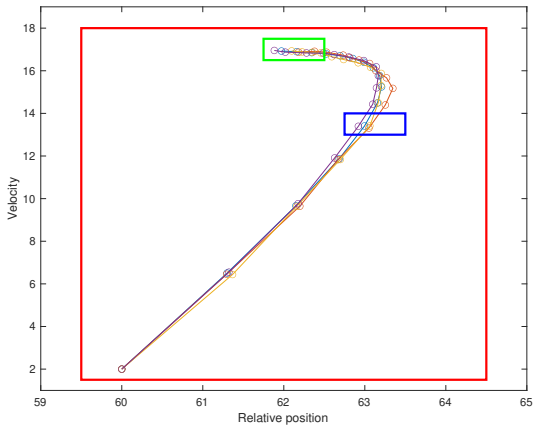

Fig. 2. Evolution of the nominal (blue) and perturbed trajectories of the system. The green, blue and red boundaries represent the first target set X_{T_1}, the second target set X_{T_2} and the safe set X_S, respectively.

VII. CONCLUSIONS AND DISCUSSION

We provided a new resilience metric for cyber-physical systems that integrates the dynamical evolution of the system with temporal logic requirements. We showed how this resilience metric can be computed for discrete-time models of the system and instances of linear temporal logic specifications. In the future, we plan to develop techniques for enhancing resilience (i.e., maximizing resilience over decision variables) and extending the ideas to continuous-time dynamical systems. We also plan to use the proposed resilience metric for the design of contracts for large-scale networked systems [18] by specifying the largest class of disturbances that a subsystem in the network can tolerate.

REFERENCES

[1] D. Rehak, P. Senovsky, M. Hromada, and T. Lovecek, "Complex approach to assessing resilience of critical infrastructure elements," *International journal of critical infrastructure protection*, vol. 25, pp. 125–138, 2019.

[2] V. Y. Pillitteri, "Developing cyber resilient systems: A systems security engineering approach," *National Institute of Standards and Technology*, vol. 2, pp. 800–160, 2019.

[3] T. G. Holloway, J. B. Williams, D. Ouelhadj, and G. Yang, "Exploring the use of water resource recovery facility instrument data to visualise dynamic resilience to environmental stressors," *Water Research*, p. 118711, 2022.

[4] S. Zhu, L. M. Tabajara, J. Li, G. Pu, and M. Y. Vardi, "Symbolic LTLf synthesis," in *IJCAI'17*, pp. 1362–1369, 2017.

[5] A. Donzé and O. Maler, "Robust satisfaction of temporal logic over real-valued signals," in *International Conference on Formal Modeling and Analysis of Timed Systems*, pp. 92–106, Springer, 2010.

[6] G. E. Fainekos and G. J. Pappas, "Robustness of temporal logic specifications for continuous-time signals," *Theoretical Computer Science*, vol. 410, no. 42, pp. 4262–4291, 2009.

[7] S. Almagor, U. Boker, and O. Kupferman, "Discounting in LTL," in *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pp. 424–439, Springer, 2014.

[8] P. Bouyer, N. Markey, and R. M. Matteplackel, "Averaging in LTL," in *Concurrency Theory*, pp. 266–280, Springer, 2014.

[9] A. Donzé, T. Ferrere, and O. Maler, "Efficient robust monitoring for STL," in *CAV'13*, pp. 264–279, Springer, 2013.

[10] E. Bartocci, J. Deshmukh, A. Donzé, G. Fainekos, O. Maler, D. Ničković, and S. Sankaranarayanan, "Specification-based monitoring of cyber-physical systems: a survey on theory, tools and applications," in *Lectures on Runtime Verification*, pp. 135–175, 2018.

[11] A. Aerts, B. Tong Minh, M. R. Mousavi, and M. A. Reniers, "Temporal logic falsification of cyber-physical systems: An input-signal-space optimization approach," in *ICSTW*, pp. 214–223, IEEE, 2018.

[12] H. Chen, S. A. Smolka, N. Paoletti, and S. Lin, "An STL-based approach to resilient control for cyber-physical systems," in *Hybrid Systems: Computation and Control (HSCC)*, pp. 1–12, 2023.

[13] M. Schulze Darup, R. Schaich, and M. Cannon, "How scaling of the disturbance set affects robust positively invariant sets for linear systems," *International Journal of Robust and Nonlinear Control*, vol. 27, no. 16, pp. 3236–3258, 2017.

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

[15] S. Zhu, G. Pu, and M. Y. Vardi, "First-order vs. second-order encodings for-to-automata translation," in *Theory and Applications of Models of Computation (TAMC'19)*, pp. 684–705, Springer, 2019.

[16] J. Wang, S. Kalluraya, and Y. Kantaros, "Verified compositions of neural network controllers for temporal logic control objectives," in *CDC'22*, pp. 4004–4009, IEEE, 2022.

[17] A. Saoud, A. Girard, and L. Fribourg, "Contract-based design of symbolic controllers for safety in distributed multiperiodic sampled-data systems," *IEEE TAC*, vol. 66, no. 3, pp. 1055–1070, 2020.

[18] A. Saoud, A. Girard, and L. Fribourg, "Assume-guarantee contracts for continuous-time systems," *Automatica*, vol. 134, p. 109910, 2021.