IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 26 June 2023, accepted 10 July 2023, date of publication 14 July 2023, date of current version 24 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3295421

RESEARCH ARTICLE

A Novel Framework for the Design of Resilient Cyber-Physical Systems Using Control Theory and Formal Methods

KELVIN ANTO, (Member, IEEE), AKSHYA KUMAR SWAIN, (Senior Member, IEEE), AND PARTHA ROOP, (Member, IEEE)
Department of Electrical Computer and Software Engineering, The University of Auckland, Auckland 1010, New Zealand
Corresponding author: Kelvin Anto (kant366@aucklanduni.ac.nz)

ABSTRACT Cyber-Physical Systems (CPSs) intertwine distributed controllers, which control physical processes. As these systems require guarantees on their stability and safety, there is a need for systematic methods for integrated safety and stability analysis of CPSs. To this end, we have developed a novel approach for the design of resilient CPSs that combines formal methods and control theory. Our framework is suitable for CPS with real-time requirements, whose dynamics can be represented as a collection of Ordinary Differential Equations (ODEs). Hence, the developed approach suits a large class of CPSs. In addition to developing the framework, we demonstrate the practical applicability through a case study focused on mitigating *time-delay* attacks on CPS. Specifically, we investigate a two-area LFC system with electric vehicles (EVs) subjected to various types of delay attacks, including constant, variable, random, and cascaded delay attacks.

INDEX TERMS Cyber-physical system, time-delay switch attack, power grid, load frequency control (LFC), stability, safety, formal verification, UPPAAL.

I. INTRODUCTION

In Cyber-Physical Systems (CPSs), physical processes interact with cyber components through communication channels [1]. CPSs are used in wide-ranging applications such as power systems, medical devices, and intelligent transportation systems. The amalgamation of physical and computational elements in CPSs has introduced new challenges, which may undermine the safe operation of the system at all times. Two key classes of properties are essential for this, namely *stability* and *safety*. Stability ensures that the system's output remains within bounds under bounded inputs (BIBO stability) [2], while safety guarantees that the system never enters a "bad state" [3].

The stability of a controller used in a CPS is typically analyzed using control theory [4], [5]. In contrast, safety is often analyzed using formal methods [6], [7]. Due to the disciplinary diversity among researchers in these domains, the two classes of properties are often studied separately in the literature. Furthermore, scholarly publications pertaining to this topic predominantly focus on either the control theoretic aspect or the formal methods aspect, with limited integration of both disciplines.

Considering this gap, endeavors have been made to integrate formal methods and control theory in the context of Cyber-Physical Systems [8], [9], [10], [11], [12]. Formal methods for discrete-time dynamical systems, with an emphasis on hybrid systems, are exhaustively examined in [8]. However, this focuses on the application of formal methods from the standpoint of safety within a pre-established closed-loop system. Similarly, in [9], a verification framework is developed for unmanned aerial vehicles (UAVs) using theorem-proving techniques, albeit with a limitation that restricts its scope to analyzing the safety aspects of an already designed closed-loop system. A safe control strategy is proposed in [10] in the context of robotics.

The associate editor coordinating the review of this manuscript and approving it for publication was Youngjin Kim.

In [11], a comprehensive review of the application of formal methods for controller synthesis is undertaken. While the approaches [10] and [11] have explored the application of formal methods in control theory, their primary emphasis lies in synthesizing control strategies based on temporal logic specifications satisfying certain safety requirements. However, overall, there is a lack of comprehensive and cohesive approaches that seamlessly integrate both formal methods and control theory to conjointly ensure the stability and safety of CPSs, which is the focus of our work.

A. OVERVIEW OF THE PROPOSED APPROACH

Figure 1 provides an overview of the proposed approach. The approach is structured into two key parts: stability analysis (steps 1-3) and safety analysis (steps 4-6). Our formulation focuses exclusively on Linear Time-Invariant (LTI) systems [13] due to their inherent linearity and time-invariance properties which facilitate simplified mathematical modeling and controller design.

In step 1, the selected LTI CPS is described in state space representation. Step 2 encompasses a controller design that satisfies the stability and performance requirements of the system. Step 3 entails performing numerical simulations in MATLAB with an appropriate step size to validate and fine-tune the controller. Step 4 focuses on translating the closed-loop system from step 3 into formal models such as Timed Automata (TA) using a developed structural translation procedure. In step 5, safety properties are formulated as TCTL queries in UPPAAL, and formal verification is performed. If any of the properties fail, it necessitates system refinement, which involves revisiting step 2 for possible system or controller design refinements. These safety properties and refinement actions can be tailored to suit the specific characteristics of the LTI system under consideration. An illustration for our case study is provided in Section IV-D.

B. CONTRIBUTIONS OF THIS PAPER

The key contributions of this work are:-

i. We propose a novel unified framework for the conjoint stability and safety assurance of cyber-physical systems, where the system dynamics are restricted to LTI systems.

ii. We have developed a novel application of the proposed approach by illustrating the attack mitigation of *time-delay* attacks on CPS. The proposed approach exceeds in novelty relative to all known methods for detecting and mitigating *time-delay* attacks on CPS. This is further elaborated through the related work section.

The rest of the paper is organized as follows. Section I-C provides an overview of the related work. The methodology is partitioned into two main sections. Section II describes the system dynamics, attacker model, and resilient controller synthesis. The structural translation to translate state space models of the system into TA is presented in Section III. The simulations and results are shown in Section IV, considering a two-area LFC system. Finally, concluding remarks are presented in Section V.

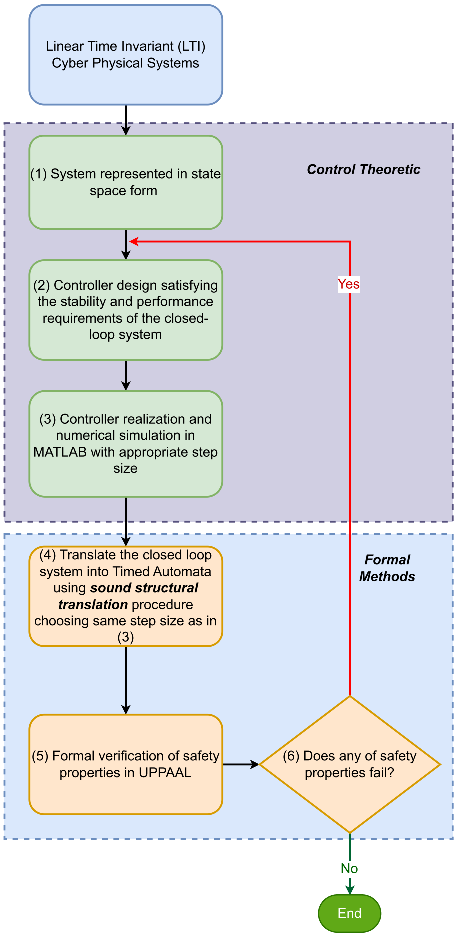
Linear Time Invariant (LTI) Cyber Physical Systems
Control Theoretic
(1) System represented in state space form
(2) Controller design satisfying the stability and performance requirements of the closed-loop system
(3) Controller realization and numerical simulation in MATLAB with appropriate step size
Yes
Formal Methods
(4) Translate the closed loop system into Timed Automata using ***sound structural translation*** procedure choosing same step size as in (3)
(5) Formal verification of safety properties in UPPAAL
(6) Does any of safety properties fail?
No
End

FIGURE 1. An overview of proposed approach.

C. RELATED WORK

Despite the advantages of CPSs, their vulnerabilities to cyber attacks have been increasing due to their reliance on cyber resources, including networking protocols. Consequently, CPSs are exposed to a broader range of attack vectors targeting either their physical domains, cyber domains, or the interconnections between them. Hence, attacks on such systems are classified as cyber-physical attacks (cp-attacks) [14]. Attacks on CPSs and their impacts are extensively discussed in [14], [15], [16], [17], and [18]. In this section, we provide a comprehensive review of existing methods related to our case study. Previous methods have focused on ensuring stability and performance of the CPS under *time-delay* attacks. We review them systematically in the following.

Time-delay attacks insidiously induce delays in the control or plant signals, often in an erratic or unpredictable manner. This malicious tampering may impair the performance of the system, including stability and safety. Notably, *time-delay* attacks encompass a broader range of scenarios relative to inherent time delays which occur in *time-delay* systems [19]. In particular, these attacks are modelled as *time-delay switch* attacks [20], which are applied to control signals. The impact of *time-delay* attacks on system stability is studied in [20] and [21]. The *time-delay attacks* have the potential to manifest in various guises, including but not limited to constant, variable, or random delay attack strategies. The dynamic and frequent changing behaviors of the *time-delay attacks* distinguish them from inherent *time-delay* systems, which operate under certain bounded delays without any switching conditions. Furthermore, [21] elucidates that while the natural delays in communications channels can be handled by controllers that dampen oscillations [22], *time-delay attacks* could cause more severe consequences and be more difficult to prevent. This is mainly because the devices employing open communication protocols are susceptible to DoS attacks, which hinder the timely exchange of crucial information, such as measurement data and control commands. To further comprehend the consequences of these attacks, an attack vector for a *time-delay* attack on the power grid is proposed in [21]. In [23], the robustness of the emotional learning control to control the Zeeman heart model under delay attacks is investigated. However, the performance of this controller degrades for large values of time delays [5].

To overcome the problems associated with larger time delays, researchers proposed various methods to estimate the delay. For example, a gradient-descent-based approach is proposed in [24], which estimates the delay while mitigating its effects. However, the stability and the safety of this controller are not investigated. A perturbation estimation-based approach is proposed in [4] to estimate the *time-delay*, mitigate its effects, and ensure stability. An alternate method for estimating delay is presented in [5], which is used to mitigate the impact of *time-delay* attacks. Although these techniques investigate stability, these approaches are not robust. Consequently, malicious alteration of delay estimation algorithms deployed in those approaches could lead to inaccurate results [25]. Recently, some researchers developed machine learning-based algorithms for mitigating the effects of delay attacks. For example, a deep learning-based approach is developed in [26] to detect and characterize the delay attacks. Another machine learning-based approach is proposed in [27] for stability and safety classifications under delay attacks. However, machine learning-based approaches are susceptible to attacks that maliciously alter the training or test data [5], [28].

To address this, in [29] we developed a formal approach based on *System Identification* and *Timed Automata (TAs)* to deal with delay attacks on the IEEE 1588 Precision Time Protocol (PTP). Likewise, a *Markov Chain-based modeling* and verification are proposed in [30] to detect and mitigate *time-delay* attacks in PTP. While the approaches [29] and [30] are interesting, these are specific to the PTP protocol and cannot be applied to a general class of attack mitigation on LTI systems. Moreover, the stability analysis of the system is not carried out in these.

II. PROBLEM FORMULATION AND PRELIMINARIES

In this section, we present modelling of a Linear Time-Invariant (LTI) Cyber-Physical System (CPS), formalize *time-delay* attacks, and diligently design a resilient controller to mitigate these attacks. Firstly, we construct a model of an LTI CPS using state-space representation, as detailed in Section II-A. Subsequently, we formalize *time-delay* attacks, which are modelled as switching actions, in Section II-B. In section II-C, we provide an in-depth explanation for the design of a resilient controller to ensure both stability and performance of the system in the face of *time-delay* attacks. The controller gains are obtained as a result of solving the optimization problem, which is articulated in Eqn(26), and the equation for computing controller gains is given by Eqn(8).

A. SYSTEM MODEL

Consider a cyber-physical system described as:-

$$\dot{x}(t) = Ax(t) + Bu(t) + Fw(t) \tag{1}$$

$$y = Cx(t) \tag{2}$$

where $x \in \mathcal{R}^n$ are the states of the system, $u \in \mathcal{R}^m$ denotes the input vector, $y \in \mathcal{R}^p$ is the output vector, and $w \in \mathcal{R}^l$ is the disturbance acting on the plant. The communication between the plant and the controller occurs through communication channels that are vulnerable to cyber-attacks.

B. FORMALIZING THE DELAY ATTACK

The *time-delay* attacks in the communication channel can either delay the actuator outputs or sensor outputs or both [20]. This study focuses on the *time-delay* attacks delaying the actuator outputs from the plant to the controller.

Therefore, the control law $u(t)$ under *time-delay* attacks can be expressed as:

$$u(t) = Kx(t - t_d), 0 \leq t_d \leq t \tag{3}$$

where t_d is the time-delay introduced by the attacker at $t = t_a$ and $K \in \mathcal{R}^{m \times n}$ is the controller gain. This attacker model is used to perform constant, random, and variable delay attacks. In order to perform cascading delay attacks, variable delay attacks are applied consecutively on x itself.

Following assumptions are made during the controller design:

Assumption 1: The time-delay t_d is bounded with the upper bound being d such that $0 \leq t_d \leq d$ and affects all the states of the system equally.

Assumption 2: The time-delay attack is applied at $t = t_a$ and persists till the end of the simulation.

In the design procedure, we use $t_d = d$, which is the upper bound of the delay.

C. H_∞ RESILIENT CONTROLLER SYNTHESIS

Let $T_{wy}(s)$ denote the transfer function between the disturbance vector $w(t)$ and the output $y(t)$. The objective is to design an H_∞ controller in the presence of *time-delay* attacks such that

$$\|T_{wy}\|_\infty = \frac{\|y\|_2}{\|w\|_2} = \frac{\sqrt{\int_0^\infty y^T(t)y(t)\,dt}}{\sqrt{\int_0^\infty w^T(t)w(t)\,dt}} \le \gamma, \gamma > 0 \quad (4)$$

where, γ is the disturbance rejection measure (also called as H_∞ performance index) [31]. Note that the introduction of *time-delay* into the system often impairs both the stability and the performance of the system.

The output of the H_∞ controller can be expressed as:

$$u(t) = K_\infty x(t-d) \quad (5)$$

where, K_∞ is the state feedback gain designed for stabilizing the system under *time-delay* attacks. Substituting (5) in (1) gives the closed-loop system as:

$$\dot{x}(t) = Ax(t) + BK_\infty x(t-d) + Fw(t) \quad (6)$$

The following theorem presents the solution of the system subjected to *time-delay* attacks by finding the suitable K_∞, leveraging the delay-dependent stability criterion and H_∞ performance criterion.

Theorem 1: If there exist positive-definite matrices Y, X, Q_t and Q_u such that

$$\begin{bmatrix} \psi_{11} & \psi_{12} & \psi_{13} & T_r & F & YC^T \\ * & \psi_{22} & \psi_{23} & T_s & F & 0 \\ * & * & \psi_{33} & 0 & F & 0 \\ * & * & * & -d^{-1}Q_u & 0 & 0 \\ * & * & * & * & -\gamma^2 I & 0 \\ * & * & * & * & * & -I \end{bmatrix} \le 0 \quad (7)$$

where,

$$\psi_{11} = AY^T + YA^T + Q_t + T_r + T_r^T$$
$$\psi_{12} = BS + YA^T - T_r + T_s^T, \quad \psi_{13} = -Y^T + YA^T + X$$
$$\psi_{22} = BS + S^TB^T - Q_t - T_s - T_s^T$$
$$\psi_{23} = -Y^T + S^TB^T, \ and \ \psi_{33} = -Y^T - Y + dQ_u$$

then under the time-delay attacks, the system (1) & (2) with controller (5) satisfies the H_∞ performance (4).

The corresponding H_∞ controller is given by

$$K_\infty = SY^{-1} \quad (8)$$

Proof: Define the Lyapunov-Krasovskii functional

$$V(t) = x^T(t)Px(t) + \int_{t-d}^{t} x^T(s)Qx(s)\,ds + \int_{-d}^{0}\int_{t+\alpha}^{t} \dot{x}^T(s)R\dot{x}(s)\,ds\,d\alpha \quad (9)$$

where P, Q, R are symmetric positive definite matrices. The derivative of (9) w.r.t time gives

$$\dot{V}(t) = \dot{x}^T(t)Px(t) + x^T(t)P\dot{x}(t) + x^T(t)Qx(t) - x^T(t-d)Qx(t-d) + d\dot{x}^T(t)R\dot{x}(t) - \int_{t-d}^{t} \dot{x}^T(s)R\dot{x}(s)\,ds \quad (10)$$

The last term in the Eqn (10) can be expressed using the Newton-Leibnitz formula:

$$x(t) - x(t-d) - \int_{t-d}^{t} \dot{x}^T(s)\,ds = 0 \quad (11)$$

Then, with the selection of appropriate matrices T_1 and T_2, we can write

$$2\left[x^T(t)\ x^T(t-d)\right]\begin{bmatrix} T_1 \\ T_2 \end{bmatrix}(x(t) - x(t-d) - \int_{t-d}^{t} \dot{x}^T(s)\,ds) = 0 \quad (12)$$

This equation form the foundation for the subsequent analysis and derivation of the mathematical proofs.

Eqn(12) can be further expressed as:

$$\begin{bmatrix} x(t) \\ x(t-d) \end{bmatrix}^T \begin{bmatrix} T_1 + T_1^T & -T_1 + T_2^T \\ * & -T_2 - T_2^T \end{bmatrix} \begin{bmatrix} x(t) \\ x(t-d) \end{bmatrix} - \int_{t-d}^{t} 2[x^T(t)T_1 + x^T(t-d)T_2]\dot{x}^T(s)\,ds = 0 \quad (13)$$

Using the Bounding Lemma in [32] and expanding Eqn (13), we obtain,

$$-2\int_{t-d}^{t} \left[x^T(t)\ x^T(t-d)\right]\begin{bmatrix} T_1 \\ T_2 \end{bmatrix}\dot{x}^T(s)\,ds \le d\begin{bmatrix} x(t) \\ x(t-d) \end{bmatrix}^T \times \begin{bmatrix} T_1 \\ T_2 \end{bmatrix} R^{-1} \begin{bmatrix} T_1 \\ T_2 \end{bmatrix}^T \begin{bmatrix} x(t) \\ x(t-d) \end{bmatrix} + \int_{t-d}^{t} \dot{x}^T(s)R\dot{x}(s)\,ds \quad (14)$$

Substituting Eqn (14) into Eqn (13) yields

$$-\int_{t-d}^{t} \dot{x}^T(s)R\dot{x}(s)\,ds \le \begin{bmatrix} x(t) \\ x(t-d) \end{bmatrix}^T \begin{bmatrix} T_1 + T_1^T & -T_1 + T_2^T \\ * & -T_2 - T_2^T \end{bmatrix} \times \begin{bmatrix} x(t) \\ x(t-d) \end{bmatrix} + d\begin{bmatrix} x(t) \\ x(t-d) \end{bmatrix}^T \begin{bmatrix} T_1 \\ T_2 \end{bmatrix} R^{-1} \times \begin{bmatrix} T_1 \\ T_2 \end{bmatrix}^T \begin{bmatrix} x(t) \\ x(t-d) \end{bmatrix} \quad (15)$$

This equation establishes an inequality relationship that relates the integral of the state variable derivatives multiplied by the matrix R and a quadratic form involving the state variables and the matrices T_1 and T_2.

Considering any matrix $G \in \mathcal{R}^{n\times n}$ and using Eqn (6) one may write,

$$2[x^T(t)G + x^T(t-d)G + \dot{x}^T(t)G][-\dot{x}(t) + Ax(t) + BK_\infty x(t-d) + Fw(t)] = 0 \quad (16)$$

This equation establishes a zero equality relationship between the terms within the brackets, involving state variables $x(t)$, delayed state variables $x(t-d)$, derivative of state variables $\dot{x}(t)$, and the matrices G, A, B, K_∞, and F.

Let $\zeta(t) = \left[x^T(t)\ x^T(t-d)\ \dot{x}^T(t)\right]^T$

Therefore, eqn(16) can be rewritten as,

$$\zeta^T(t)\begin{bmatrix} \theta_{11} & \theta_{12} & \theta_{13} \\ * & \theta_{22} & \theta_{23} \\ * & * & \theta_{33} \end{bmatrix}\zeta(t) + 2\zeta^T(t)\begin{bmatrix} GF \\ GF \\ GF \end{bmatrix} w(t) = 0 \quad (17)$$

where

$$\theta_{11} = GA + A^T G^T, \quad \theta_{12} = GBK_\infty + A^T G^T$$
$$\theta_{13} = -G + A^T G^T, \quad \theta_{22} = GBK_\infty + K_\infty^T B^T G^T$$
$$\theta_{23} = -G + K_\infty^T B^T G^T, \; and \; \theta_{33} = -G - G^T$$

Using the Bounding Lemma in [32] and further matrix manipulation of eqn(17) gives

$$\zeta^T(t)\begin{bmatrix}\theta_{11} & \theta_{12} & \theta_{13}\\ * & \theta_{22} & \theta_{23}\\ * & * & \theta_{33}\end{bmatrix}\zeta(t) + \zeta^T(t)\begin{bmatrix}GF\\ GF\\ GF\end{bmatrix}\gamma^{-2}\begin{bmatrix}GF\\ GF\\ GF\end{bmatrix}^T\zeta(t)$$
$$+\gamma^2 w^T(t)w(t) \geq 0 \tag{18}$$

Next, substitute Eqn(15) into Eqn(10) yields,

$$\begin{aligned}\dot{V}(t) &\leq \dot{x}^T(t)Px(t) + x^T(t)P\dot{x}(t) + x^T(t)Qx(t)\\ &\quad -x^T(t-d)Qx(t-d) + d\dot{x}^T(t)R\dot{x}(t)\\ &\quad + \begin{bmatrix}x(t)\\ x(t-d)\end{bmatrix}^T\begin{bmatrix}T_1 + T_1^T & -T_1 + T_2^T\\ * & -T_2 - T_2^T\end{bmatrix}\begin{bmatrix}x(t)\\ x(t-d)\end{bmatrix}\\ &\quad + d\begin{bmatrix}x(t)\\ x(t-d)\end{bmatrix}^T\begin{bmatrix}T_1\\ T_2\end{bmatrix}R^{-1}\begin{bmatrix}T_1\\ T_2\end{bmatrix}^T\begin{bmatrix}x(t)\\ x(t-d)\end{bmatrix}\end{aligned} \tag{19}$$

Grouping and re-arranging the terms will give,

$$\begin{aligned}\dot{V}(t) &\leq \begin{bmatrix}x^T(t)\\ x^T(t-d)\\ \dot{x}^T(t)\end{bmatrix}\begin{bmatrix}Q + T_1 + T_1^T & -T_1 + T_2^T & P\\ * & -Q - T_2 - T_2^T & 0\\ * & * & dR\end{bmatrix}\\ &\quad\times\begin{bmatrix}x(t)\\ x(t-d)\\ \dot{x}(t)\end{bmatrix} + d\begin{bmatrix}x(t)\\ x(t-d)\end{bmatrix}^T\begin{bmatrix}T_1\\ T_2\end{bmatrix}R^{-1}\\ &\quad\times\begin{bmatrix}T_1\\ T_2\end{bmatrix}^T\begin{bmatrix}x(t)\\ x(t-d)\end{bmatrix}\end{aligned} \tag{20}$$

Then substitute Eqn(18) into Eqn(20) and grouping the terms gives,

$$\begin{aligned}\dot{V}(t) &\leq \zeta^T(t)\left\{\begin{bmatrix}\xi_{11} & \xi_{12} & \xi_{13}\\ * & \xi_{22} & \xi_{23}\\ * & * & \xi_{33}\end{bmatrix} + \begin{bmatrix}T_1\\ T_2\\ 0\end{bmatrix}dR^{-1}\begin{bmatrix}T_1\\ T_2\\ 0\end{bmatrix}^T\right.\\ &\quad\left. +\gamma^{-2}\begin{bmatrix}GF\\ GF\\ GF\end{bmatrix}\begin{bmatrix}GF\\ GF\\ GF\end{bmatrix}^T\right\}\zeta(t) + \gamma^2 w^T(t)w(t)\end{aligned} \tag{21}$$

where $\xi_{11} = \theta_{11} + Q + T_1 + T_1^T$, $\xi_{12} = \theta_{12} - T_1 + T_2^T$
$\xi_{13} = \theta_{13} + P$, $\xi_{22} = \theta_{22} - Q - T_2 - T_2^T$
$\xi_{23} = \theta_{23}$, *and* $\xi_{33} = \theta_{33} + dR$
Next, let us consider the following cost function to study the H_∞ performance criterion:

$$J_{wy} = \int_0^\infty [y^T(t)y(t) - \gamma^2 w^T(t)w(t)]\,dt \tag{22}$$

where, γ is the H_∞ performance index. Note that, if $J_{wy} \leq 0$, then the closed loop system satisfies the Eqn (4). Therefore, the objective is to ensure $J_{wy} \leq 0$ so that the H_∞ controller guarantees the performance index γ.

With zero initial conditions, $V(0) = 0$ and $V(\infty) \geq 0$, we can write,

$$J_{wy} \leq \int_0^\infty [y^T(t)y(t) - \gamma^2 w^T(t)w(t) + \dot{V}(t)]\,dt \tag{23}$$

We know from the Eqn(2) that $y(t) = Cx(t)$ and therefore $y^T(t) = x^T(t)C^T$. Substituting Eqn(21) into Eqn(23) and using Eqn(2) gives,

$$J_{wy} \leq \int_0^\infty \zeta^T(t)\Lambda\zeta(t)\,dt \tag{24}$$

where,

$$\begin{aligned}\Lambda &= \begin{bmatrix}\xi_{11} & \xi_{12} & \xi_{13}\\ * & \xi_{22} & \xi_{23}\\ * & * & \xi_{33}\end{bmatrix} + \begin{bmatrix}T_1\\ T_2\\ 0\end{bmatrix}dR^{-1}\begin{bmatrix}T_1\\ T_2\\ 0\end{bmatrix}^T\\ &\quad + \gamma^{-2}\begin{bmatrix}GF\\ GF\\ GF\end{bmatrix}\begin{bmatrix}GF\\ GF\\ GF\end{bmatrix}^T + \begin{bmatrix}C^T\\ 0\\ 0\end{bmatrix}\begin{bmatrix}C^T\\ 0\\ 0\end{bmatrix}^T\end{aligned} \tag{25}$$

So, $\Lambda \leq 0$ implies $J_{wy} \leq 0$. Let us apply the Schur complement [33] to Eqn(23). Pre-multiply and post-multiply Λ with diag$\{G^{-1}, G^{-1}, G^{-1}, G^{-1}, I, I\}$ and its transpose respectively. With appropriate change of variables: $\mathbf{Y = G^{-1}}$, $\mathbf{K_\infty G^{-T} = K_\infty Y^T = S}$, $\mathbf{G^{-1}QG^{-T} = Q_t}$, $\mathbf{G^{-1}RG^{-T} = Q_u}$, $\mathbf{G^{-1}T_1G^{-T} = T_r}$, $\mathbf{G^{-1}T_2G^{-T} = T_s}$ and $\mathbf{G^{-1}PG^{-T} = X}$ gives the LMI (7). This completes the proof. ■

Define $\bar{\gamma} = \gamma^2$. To obtain the solution of (7), we aim to minimize $\bar{\gamma}$, Frobenius norm of S and trace of Y. Frobenius norm of S represents the square root of the sum of the squares of the elements of the matrix S, which provides a measure of its magnitude and plays a significant role in the optimization process.

This yields a H_∞ controller that effectively constrains the control effort within practical limits, while also achieving a lower γ value due to the additional constraints on S and Y. This can be expressed as the following LMI optimization problem.

Optimization Problem:-

$$\begin{aligned}&\min \quad \bar{\gamma} + \bar{s} + 0.01 * trace(Y)\\ &\text{subject to} \quad (7), Y \geq 0, X \geq 0, Q_t \geq 0, Q_u \geq 0, \bar{\gamma} \geq 0\end{aligned} \tag{26}$$

where $\bar{s} = \sqrt{\sum_{i=1}^{a}\sum_{j=1}^{b}\|s_{ij}\|^2}$. Here, a and b represent the number of rows and columns of the S matrix respectively, and s_{ij} are the elements of S.

III. STRUCTURAL TRANSLATION TO TIMED AUTOMATA

In order to examine the safety-related aspects of the system under delay attack, we employ model checking and formal verification in UPPAAL [34], which is an integrated tool suite for formal verification of real-time systems and is proven to be efficacious in modelling and verifying systems [35] modelled as Timed Automata (TA).

Therefore, to facilitate this analysis, it is necessary to translate the system described in state-space form into formal models represented as timed automata. The syntax of a Timed Automaton in UPPAAL is defined below:-

Definition 1 (Timed Automaton): A Timed Automaton $\mathcal{A}$ in UPPAAL is a tuple $\langle\, L, l_0, C, A, \Sigma, E, I, Q \,\rangle$ where: L is a set of all locations in $\mathcal{A}$, $l_0 \in L$ is the initial location, C is a finite set of all real-valued clocks, and A is a finite set of variables. Σ is a set of actions and co-actions. The actions and co-actions are of the form $z!$ and $z?$ (channel synchronizations here). $E \subseteq L \times G \times \Sigma \times U \times L$ is the set of edges and $I : L \rightarrow \Phi(C)$ specifies the invariants to locations, where $\Phi(C)$ is the set of clock constraints. $Q : L \rightarrow \{Nr, Ur, Cm\}$ specifies each location as either Nr - Normal, Ur - Urgent and Cm - Committed.

The detailed explanation of labels each location as either (Nr) Normal, (Ur) Urgent or (Cm) Committed can be found in [36]. Here, G is a set of guards representing conjunctions of predicates of the form $x \sim n$ or $x - y \sim n$ or $v \sim n$ for $x, y \in C$, $v \in A$, $\sim \in \{\leq, <, =, >, \geq\}$ and $n \in \mathbb{N}$. U denotes the set of updates representing a sequence of assignments to variables of the form $v := exp$ and/or clock resets of the form $x := 0$ where $v \in \{A \cup \varepsilon\}$, $x \in C$ and exp is an arithmetic expression. The edge $(l, g, \Sigma, u, l') \in E$ is denoted as $l \xrightarrow{g,\Sigma,u} l'$. An example of TA is illustrated below following the syntax defined in the Definition 1.

Example 1 (Timed Automaton): Consider the following example of the attacker TA depicted in Figure 2, which models a time-delay attacker. The attacker adds a certain delay t_d to the control signals starting from time $t = t_a$. This TA has three locations, and the set of locations $L = \{S_0, S_1, S_2\}$. The locations, S_0 and S_2, are normal locations (Nr) and the location S_1 is committed location(Cm). The initial location l_0 is S_0, denoted by a double circle in UPPAAL. The set of real-valued clocks in this example is $C = \{ca\}$. The finite set of variables $A = \{t_d, time\_count, t_a\}$ and the finite set of actions and co-actions $\Sigma = \{output\_to\_controller, output\_from\_plant\}$ which serve as synchronization channels. The set of guards $G = \{time\_count < t_a, time\_count >= t_a\}$.

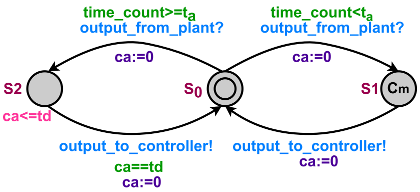

FIGURE 2. **Attacker TA used to perform constant, variable, and random delay attacks.**

Upon the receipt of the synchronization message/channel *output_from_plant* and guard condition $time\_count < t_a$ being satisfied, this TA undergoes a transition from S_0 to S_1 while resetting the clock ca to 0. The set of updates is $U = \{ca := 0\}$. This transition is an element of set of edges E and can be represented as $(S_0, time\_count < t_a, output\_from\_plant, ca := 0, S_1)$. Notably, S_1 is a committed location (Cm), prompting an immediate transition from S_1 to S_0 (without any delay in time). During this transition, it sends *output_to_controller* as well as resets the clock ca to 0. Furthermore, if the guard condition $time\_count >= t_a$ is fulfilled and the synchronization message/channel *output_from_plant* is received, the TA takes a transition from S_0 to S_2 while resetting the clock ca to 0. The set of updates is $U = \{ca := 0\}$. The automaton can remain in the location S_1 as long as $ca <= td$ and when $ca == td$, it moves S_0 from S_2. During this transition, it sends *output_to_controller* as well as resets the clock ca to 0.

The attacker model depicted in Figure 2 is used to perform constant, random, and variable delay attacks by having td constant, random, and variable, respectively. Subsequently, a timed automaton model, as depicted below in Figure 3, is developed to perform cascading delay attacks.

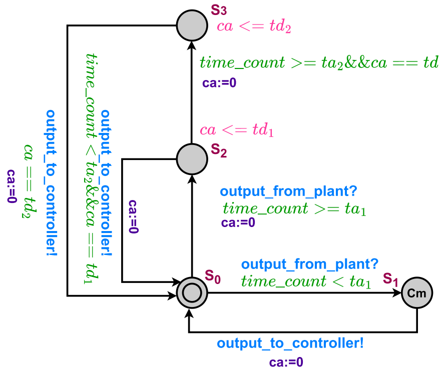

FIGURE 3. **Cascading delay attacker TA used to perform cascading delay attacks.**

A. MODELING STATE SPACE SYSTEM AS UPDATE FUNCTIONS

Using any numerical methods of discretization such as in [37], the system (1) can be described as update function:

$$x(t + \tau_0) = x(t) + A\tau_0 x(t) + B\tau_0 u(t) + F\tau_0 w(t) \qquad (27)$$

where τ_0 is a very small time-step. In this study, a time-step of 0.01s is chosen.

B. FORMALIZATIONS

The closed-loop CPS under consideration is split into two parts: plant and controller. We define J, K and W as arbitrary index sets on $\mathbb{N}$. This system whose dynamics can be expressed by first order ODEs can be formally represented as following 2-tuples:

a. **Plant** - $\mathcal{P} = (\{\mathcal{F}_i\}_{i \in J}, \{\mathcal{H}_h\}_{h \in W}, A, \Sigma, \tau)$
b. **Controller** - $\mathcal{C} = (\{\mathcal{G}_j\}_{j \in K}, A, \Sigma)$

where each component of above are described as:

- $\{\mathcal{F}_i\}_{i \in J}$ are functions representing the discretized ODEs of plant dynamics which updates the state variables

$\{x_i\}_{i\in J}$ and updated set of state variables are denoted as $\{x_i^{\text{next}}\}_{i\in J}$. Here $|J| = n \in \mathbb{N}$ is an index set which counts such number of functions. For example, in this study, $\mathcal{F}_1$ is $x_1^{\text{next}} := x_1 + \tau(a_{11}x_1 + a_{12}x_2 + a_{14}x_4 + a_{15}x_5 + f_{11}Pd_1)$ which uses a set of parameters and maps x_1 to x_1^{next}. The plant under consideration has 12 state variables and 12 ODEs. Hence, 12 update functions which updates those state variables, therefore, $|J| = 12$.

- $\{\mathcal{H}_h\}_{h\in W}$ are the functions updating the disturbance vector $\{w_h\}_{h\in W}$. Here $|W| = h \in \mathbb{N}$ is an index set which counts such number of functions. For example, in this study $|W| = 2$ and this implies the disturbance vector $\{w\} = \{w_1, w_2\}$. Here, in the LFC case study, w_1 refers to load disturbance in Area-1 denoted as Pd_1 and w_2 refers to load disturbance in Area-2 denoted as Pd_2. The $\{\mathcal{H}_h\}_{h\in W}$ is represented here by "updateW()" which updates w_1 and w_2.
- $A = A_{\mathcal{P}} \cup A_{\mathcal{C}}$ where $A_{\mathcal{P}}, A_{\mathcal{C}}$ denote global variables used by the Plant and Controller respectively.
- τ denotes update time-period, which is set to 0.1s.
- Σ is a set of action and co-action. Here, Σ stands for synchronization channel between the plant and the controller.
- $\{\mathcal{G}_j\}_{j\in K}$ are functions which updates the control signals. Here $|K| = m \in \mathbb{N}$ is an index set which counts such number of functions.

C. ALGORITHMS FOR TA GENERATION

The following algorithms structurally convert the models of the plant and the controller to their respective UPPAAL TA counterparts.

Algorithm 1 Plant TA Construction

```
1:  procedure Plant ($\mathcal{P}$)
2:      parse $\mathcal{P} = (\{\mathcal{F}_i\}_{i\in J}, \{\mathcal{H}_h\}_{h\in W}, A, \Sigma, \tau)$   ▷ Initialize parameters
3:      $n \leftarrow |J|$; $h \leftarrow |W|$; $L \leftarrow \{S_0, S_1\}$; $l^0 \leftarrow \{S_0\}$; $C \leftarrow \{t\}$;
4:      $A \leftarrow \{\{x_i\}_{i\in[n]}, \{x_i^{\text{next}}\}_{i\in[n]}, \{w_i\}_{i\in[h]}\}$; $E \leftarrow \{\}$;
5:      $I(S_0) = \{t \le \tau\}$, $I(S_1) = \{\phi\}$;
6:      $Q(S_0) = N_r$, $Q(S_1) = C_m$;
7:      $U^1 \leftarrow \{\}$, $U^2 \leftarrow \{\}$;
8:      for $i \in [n]$ do
9:          $U^1 \leftarrow U^1 \cup \{x_i^{\text{next}} := \mathcal{F}_i(\{x_i\}_{i\in[n]})\}$
10:         $U^2 \leftarrow U^2 \cup \{x_i := x_i^{\text{next}}\}$
11:     end for
12:     E $\leftarrow$ $E \cup \{S_0 \xrightarrow{\{t==\tau\}, \Sigma!, U^1} S_1\}$
13:     E $\leftarrow$ $E \cup \{S_1 \xrightarrow{\phi, \phi, U^2 \cup (\{\mathcal{H}_h\}_{h\in W}, \{t:=0\})} S_0\}$
14:     return $\mathcal{P}_{TA} := (L, l_0, C, A, \Sigma, E, I, Q)$
15: end procedure
```

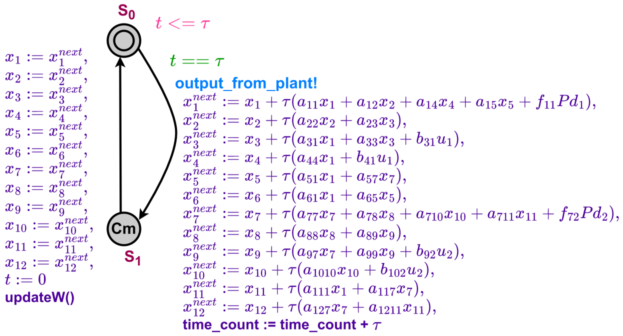
S_0
$t <= \tau$
$t == \tau$
output_from_plant!
$x_1^{next} := x_1 + \tau(a_{11}x_1 + a_{12}x_2 + a_{14}x_4 + a_{15}x_5 + f_{11}Pd_1),$
$x_2^{next} := x_2 + \tau(a_{22}x_2 + a_{23}x_3),$
$x_3^{next} := x_3 + \tau(a_{31}x_1 + a_{33}x_3 + b_{31}u_1),$
$x_4^{next} := x_4 + \tau(a_{44}x_1 + b_{41}u_1),$
$x_5^{next} := x_5 + \tau(a_{51}x_1 + a_{57}x_7),$
$x_6^{next} := x_6 + \tau(a_{61}x_1 + a_{65}x_5),$
$x_7^{next} := x_7 + \tau(a_{77}x_7 + a_{78}x_8 + a_{710}x_{10} + a_{711}x_{11} + f_{72}Pd_2),$
$x_8^{next} := x_8 + \tau(a_{88}x_8 + a_{89}x_9),$
$x_9^{next} := x_9 + \tau(a_{97}x_7 + a_{99}x_9 + b_{92}u_2),$
$x_{10}^{next} := x_{10} + \tau(a_{1010}x_{10} + b_{102}u_2),$
$x_{11}^{next} := x_{11} + \tau(a_{111}x_1 + a_{117}x_7),$
$x_{12}^{next} := x_{12} + \tau(a_{127}x_7 + a_{1211}x_{11}),$
time_count := time_count + τ
$x_1 := x_1^{next},$
$x_2 := x_2^{next},$
$x_3 := x_3^{next},$
$x_4 := x_4^{next},$
$x_5 := x_5^{next},$
$x_6 := x_6^{next},$
$x_7 := x_7^{next},$
$x_8 := x_8^{next},$
$x_9 := x_9^{next},$
$x_{10} := x_{10}^{next},$
$x_{11} := x_{11}^{next},$
$x_{12} := x_{12}^{next},$
$t := 0$
updateW()
Cm
S_1

FIGURE 4. Plant TA $\mathcal{P}$.

The plant TA is constructed from the formalized representation of the plant($\mathcal{P}$) using Algorithm (1). In this algorithm, lines 1 to 7 initialize a UPPAAL tuple according to Definition 1. Subsequently, lines 8 to 10 encompass the update functions responsible for updating the state variables of the plant ($\{x_i, x_i^{\text{next}}\}_{i\in[n]}$). The update time period of τ is captured by setting the invariant $I(S_0) = \{t \le \tau\}$ on the initial location S_0 and the other state is kept committed by setting $Q(S_1) = C_m$. Lines 12 and 13 add edges that denote the transition between two locations, S_0 and S_1. The edge transitions E update the system state variable exactly at $t = \tau$ and updates the synchronization channel Σ (here, the plant is the sender). Finally, the constructed TA is returned in line 14.

Algorithm 2 Controller TA Construction

```
1:  procedure Controller ($\mathcal{C}$)
2:      parse $\mathcal{C} = (\{\mathcal{G}_j\}_{j\in K}, A, \Sigma)$   ▷ Initialize parameters
3:      $m \leftarrow |K|$; $L \leftarrow \{S_0\}$; $l^0 \leftarrow \{S_0\}$;$C \leftarrow \{\}$;
4:      $A \leftarrow \{\{u_j\}_{j\in[m]}, \{x_i\}_{i\in[n]}\}$; $E \leftarrow \{\}$;
5:      $I(S_0) = \phi$; $Q(S_0) = N_r$; $U^1 \leftarrow \{\}$;
6:      for $j \in [m]$ do
7:          $U^1 \leftarrow U^1 \cup \{u_j := \mathcal{G}_j(\{x_i\}_{i\in K})\}$
8:      end for
9:      E $\leftarrow$ $E \cup \{S_0 \xrightarrow{\phi, \Sigma?, U^1} S_0\}$
10:     return $\mathcal{C}_{TA} := (L, l_0, C, A, \Sigma, E, I, Q)$
11: end procedure
```

The Algorithm 2 is used for constructing the controller TA. Lines 1 to 5 in this algorithm initialize blue a UPPAAL tuple for the controller. Lines 6 to 8 refer to the update function, which updates the control signals $\{u_j\}_{j\in[m]}$ on the receipt of synchronization signal Σ. Line 9 adds edge, which denotes the transition in the self-loop at location S_0. Line 10 returns the constructed controller TA.

D. MODELING THE PLANT AND CONTROLLER AS TAs

Using the algorithms(1) and (2), we model the plant and the controller TAs illustrated in the Figures 4 and 5 respectively.

IV. TWO AREA LFC WITH EV AS CASE STUDY

The effectiveness of the proposed framework is demonstrated considering an example of two-area Load Frequency Control (LFC) system with EVs subjected to *time-delay* attacks. The fleet of EVs is modelled using a first-order system having a time constant of Tev_i and a gain of Ke_i. The participation

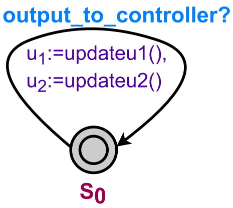

FIGURE 5. Controller TA $\mathcal{C}$.

factors of EVs and generating units are given by αe_i and αg_i respectively.

The dynamics of this system can be described by state equations of the form eqn(1) and (2) where the state vector of area i is defined as: $x_i = [\Delta f_i, \Delta Pm_i, \Delta Pv_i, \Delta Pe_i, \Delta Ptie_{ij}, \Delta E_i]^T$ (the explanation of these state variables can be found in [38] and [39]). For a two-area interconnected power system ($i = 2$), the state vector, input vector and disturbance vectors are defined as: $x(t) = [x_1, x_2]^T$, $u(t) = [u_1, u_2]^T$ and $w(t) = [\Delta Pd_1, \Delta Pd_2]^T$.

The system matrix A, input matrix B, load disturbance matrix F and the output matrix C for the complete two area system can be expressed as:

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}, \quad B = diag[B_1, B_2]$$

$$C = diag[C_1, C_2], \quad F = diag[F_1, F_2] \;\; where,$$

$$A_{ii} = \begin{bmatrix} \frac{-D_i}{M_i} & \frac{1}{M_i} & 0 & \frac{1}{M_i} & -\frac{1}{M_i} & 0 \\ 0 & \frac{-1}{Tch_i} & \frac{1}{Tch_i} & 0 & 0 & 0 \\ \frac{-1}{R_1 Tg_i} & 0 & -\frac{1}{Tg_i} & 0 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{Tev_i} & 0 & 0 \\ 2\pi \sum_{j=1, j\neq i}^{n} T_{ij} & 0 & 0 & 0 & 0 & 0 \\ \beta_i & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$A_{ij} = \begin{bmatrix} 0 & 0\,0\,0\,0\,0 \\ 0 & 0\,0\,0\,0\,0 \\ 0 & 0\,0\,0\,0\,0 \\ 0 & 0\,0\,0\,0\,0 \\ -2\pi T_{ij} & 0\,0\,0\,0\,0 \\ 0 & 0\,0\,0\,0\,0 \end{bmatrix}, B_i = \begin{bmatrix} 0 \\ 0 \\ \frac{\alpha g_i}{Tg_i} \\ \frac{Ke_i \alpha e_i}{Tev_i} \\ 0 \\ 0 \end{bmatrix}$$

$$F_i = \begin{bmatrix} -\frac{1}{M_i} & 0\,0\,0\,0\,0 \end{bmatrix}^T, C_i = \begin{bmatrix} 1\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,1\,0 \end{bmatrix}$$

The parameters of the system considered in this study are taken from [38] and [39] and are as follows: $D_1 = 1.5$, $D_2 = 1$, $\beta_1 = 21.5$, $\beta_2 = 21$, $M_1 = 10$, $M_2 = 12$, $Tch_1 = 0.2s$, $Tch_2 = 0.45s$, $Tg_1 = 0.12s$, $Tg_2 = 0.18s$, $Tev_1 = 0.12s$, $Tev_2 = 0.20s$, $Ke_1 = 3.00$, $Ke_2 = 2.00$, $\alpha g_1 = \alpha g_2 = 0.9$, $\alpha e_1 = \alpha e_2 = 0.1$, $R_1 = 0.05$, $R_2 = 0.05$ and $T_{12} = 0.198$ p.u/rad.

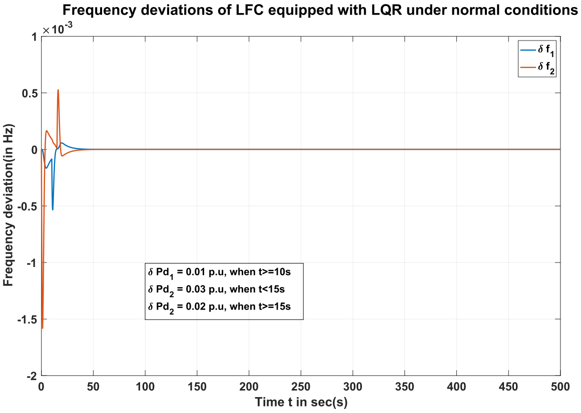

FIGURE 6. Frequency deviations of LFC system in the normal scenario.

A. LFC SYSTEM UNDER NORMAL SCENARIO

Initially, the simulation is carried out considering the normal situation i.e. when the LFC system is not subjected to *time-delay* attacks. To evaluate the performance of the closed-loop system, as a standard procedure followed in the literature, a step load disturbance of 1% is applied to Area-1 starting at $t = 10s$. Similarly, for Area-2, a step load disturbance of 3% is applied initially until $t = 15s$, and it is reduced to 2% thereafter. The frequency deviations are regulated by designing a standard Linear Quadratic Regulator (LQR), whose gains are given in Eqn (28), as shown at the bottom of the page.

From the results of the simulation, depicted in Figure 6, it is observed that the LQR could effectively regulate the frequency in the absence of *time-delay* attacks. This scenario serves as a baseline for comparing the performance of the closed-loop system under various subsequent scenarios, which includes *time-delay* attacks.

B. LFC SYSTEM SUBJECTED TO TIME-DELAY ATTACK

In the subsequent phase of the investigation, the system was subjected to *time-delay* attacks applied at $t = 20s$ and varying the delay from $t_d = 0.1s$ to $t_d = 0.7s$. Notably, the results revealed that when the delay exceeds $0.55s$, the LQR failed to regulate the frequency deviations and exhibited an unstable response. Figure 7 vividly illustrates the response when subjected to a delay of $t_d = 0.7s$.

C. LFC SYSTEM EMBEDDED WITH H_∞ RESILIENT CONTROLLER SUBJECTED TO DELAY ATTACKS

In order to get a stable response during *time-delay* attacks, H_∞ based controller was designed following the procedure described in Section II-C. Due to the limited feasibility region, multiple solvers were deployed, ultimately utilizing YALMIP and MOSEK to obtain the solution. The H_∞ controller gain matrix is given in Eqn (29), as shown at the bottom of the next page, which achieves the performance

$$K_{\text{Lqr}} = \begin{bmatrix} 18.1183 & 0.548 & 0.5698 & 0.355 & -0.1029 & 0.9992 & 0.0837 & -0.0066 & -0.0024 & -0.0017 & 0.0741 & 0.0396 \\ -0.3955 & -0.0037 & -0.0008 & -0.0031 & -0.0722 & -0.0396 & 22.3036 & 0.9343 & 0.6038 & 0.4738 & -0.3072 & 0.9992 \end{bmatrix} \tag{28}$$

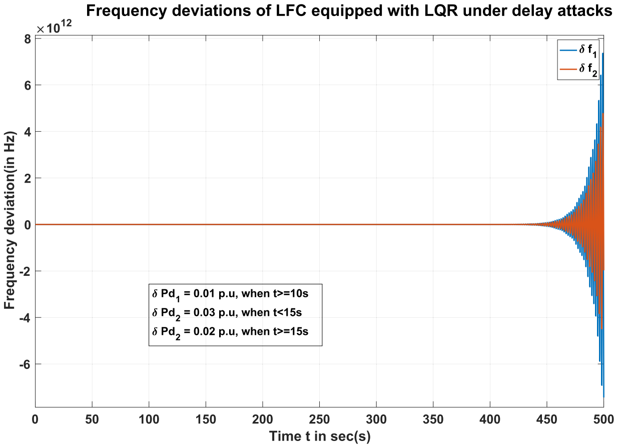

FIGURE 7. Frequency deviations of LFC system under delay attacks.

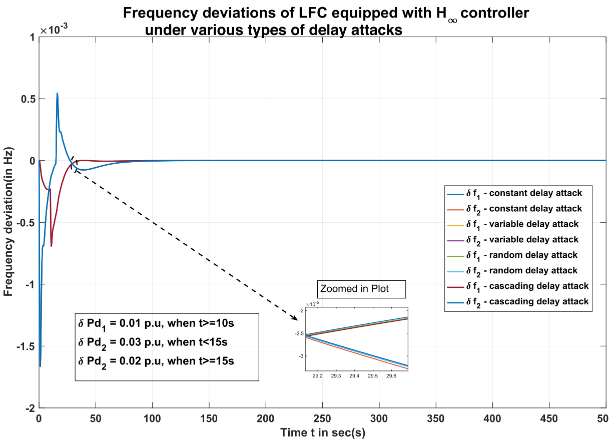

FIGURE 8. Frequency deviations of LFC system with H_∞ controller under various delay attacks.

index $\gamma_{min} = 1.8273$. To evaluate the effectiveness of the designed controller, various simulations were conducted that simulated different types of *time-delay* attacks including constant, variable, random, and cascading each applied at $t = 20s$. The results of the simulation for these types of *time-delay* attacks are shown in Figure 8.

From the results, it is evident that the proposed controller could regulate the frequency deviations and stabilizes the system under *time-delay* attacks. For constant delay, a constant value of 0.7s is set for t_d. The applied variable time delays are visually represented in Figure 9. The random delays are assumed to be uniformly distributed pseudo-random numbers between 0.3 and 0.7.

On the other hand, cascaded delay attacks involve a series of delay elements that are connected/cascaded in series.

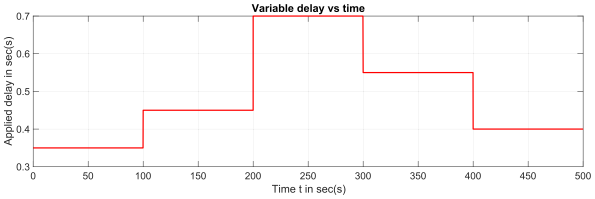

FIGURE 9. Applied variable delay attacks.

To create such cascading delay attacks, variable delay attacks are applied on x itself, resulting in $x(t - t_{d1})$. Subsequently, another variable delay attack is applied on $x(t-t_{d1})$, resulting in $x(t-t_{d2})$. It is worth noting that both cascading and variable delay attacks deploy the same variable delay attack scheme.

D. FORMAL VERIFICATION OF TWO-AREA LFC SYSTEM

From the security perspective, we investigate the safety aspects of the system using formal verification in UPPAAL. One crucial aspect to address is the physical limitations of the turbine in a load frequency controller; the rate of power generation has to be within practical limits, which is termed as Generation Rate Constraint (GRC). In this study, a GRC limit (r) of $\pm 3\%/min$ [40], [41] is considered. Furthermore, it is equally important to ensure that the frequency of the system lies within $\pm 1.5\%$ of the nominal value (50 Hz in countries such as New Zealand). Therefore, these aspects can be corroborated provided some of the properties defined below are satisfied:

i. *P1* - Frequency deviation of the system does not exceed the lower bound(low).
ii. *P2* - Frequency deviation of the system does not exceed the upper bound(up).
iii. *P3* - The rate of change in generating power of the system does not exceed the lower bound(-r).
iv. *P4* - The rate of change in generating power of the system does not exceed the upper bound(+r).

To facilitate the verification of the properties P1–P2, a *Frequency deviation monitor* has been developed, as depicted in Figure 10.

Similarly, a *GRC monitor* was developed to aid the verification of properties P3–P4 and shown in the Figure 11.

We resorted to statistical model checking due to the limitations of symbolic model checking in handling floating point operations in UPPAAL. The results of verifying the properties P1–P2 as tabulated in Table 1 demonstrate that the probability of frequency deviations exceeding the upper and lower bound is very minimal (0.299%). Subsequently, the properties P3–P4 were also verified, and the results are tabulated in Table 1. This shows that it is 99.7% certain that

$$K_\infty = \begin{bmatrix} -4.5635 & -0.05 & -0.0978 & 0.0414 & -0.0649 & -0.0398 & 0.1979 & 0.0004 & 0.0084 & -0.0235 & 0.0357 & 0.0044 \\ -0.0204 & 0.0003 & -0.0026 & 0.0036 & 0.0977 & 0.0008 & -8.5123 & -0.0476 & -0.2876 & 0.6941 & -0.1228 & -0.122 \end{bmatrix} \tag{29}$$

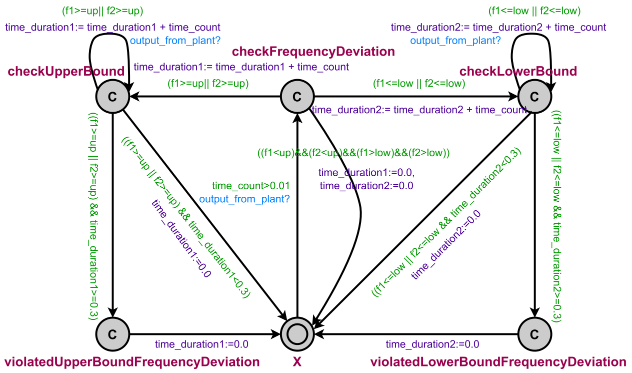
(f1>=up|| f2>=up)
time_duration1:= time_duration1 + time_count
output_from_plant?
checkFrequencyDeviation
(f1<=low || f2<=low)
time_duration2:= time_duration2 + time_count
output_from_plant?
checkUpperBound
time_duration1:= time_duration1 + time_count
(f1>=up|| f2>=up)
checkLowerBound
(f1<=low || f2<=low)
C
C
C
time_duration2:= time_duration2 + time_count
((f1<up)&&(f2<up)&&(f1>low)&&(f2>low))
time_duration1:=0.0,
time_duration2:=0.0
time_count>0.01
output_from_plant?
((f1>=up || f2>=up) && time_duration1>=0.3)
((f1>=up || f2>=up) && time_duration1<0.3)
time_duration1:=0.0
((f1<=low || f2<=low && time_duration2<0.3)
time_duration2:=0.0
((f1<=low || f2<=low && time_duration2>=0.3)
C
C
time_duration1:=0.0
time_duration2:=0.0
violatedUpperBoundFrequencyDeviation
X
violatedLowerBoundFrequencyDeviation

FIGURE 10. Timed Automaton model of Frequency deviation monitor.

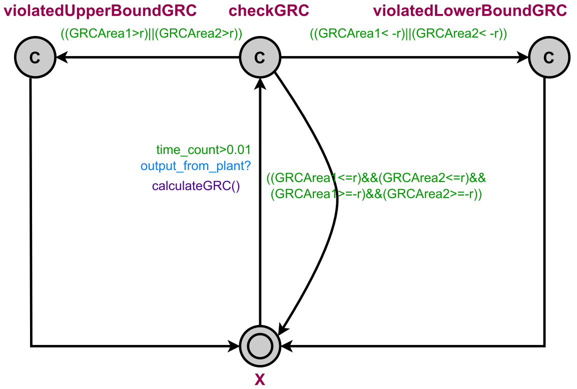
violatedUpperBoundGRC
checkGRC
violatedLowerBoundGRC
((GRCArea1>r)||(GRCArea2>r))
((GRCArea1< -r)||(GRCArea2< -r))
C
C
C
time_count>0.01
output_from_plant?
calculateGRC()
((GRCArea1<=r)&&(GRCArea2<=r)&&
(GRCArea1>=-r)&&(GRCArea2>=-r))
X

FIGURE 11. Timed Automaton model of GRC monitor.

TABLE 1. Verification results for the properties P1-P4.

Property	Query used	Probability
P1	*Pr[<=500;1000](<>Frequency_monitor.violated LowerBoundFrequencyDeviation)*	0.299 %
P2	*Pr[<=500;1000](<>Frequency_monitor.violated UpperBoundFrequencyDeviation)*	0.299 %
P3	*Pr[<=500;1000](<>GRC_monitor.violated UpperBoundGRC)*	99.7 %
P4	*Pr[<=500;1000](<>GRC_monitor.violated LowerBoundGRC)*	99.7 %

the system violates the upper and lower limits for the rate of change in generating power. Therefore, to remedy this, we added two limiters, bounded by $\pm r$, to restrict the generation ramp rate and ensure compliance with the specified limits. These limiters play a crucial role in mitigating the observed violations and enhancing the overall stability and performance of the closed-loop system.

E. LFC SYSTEM WITH RESILIENT CONTROLLER AND LIMITER

Figures 13 and 14 provide a visual comparison of the generation rate of the system before and after the inclusion of these limiters, as observed in MATLAB. It is evident from these figures that after adding the limiter, the generation ramp rate of the system is restricted within $\pm r$, where $r = 0.0005$ p.u/sec. The frequency deviations of the system equipped with the resilient controller and adding limiter under delay attacks are depicted in Figure 12.

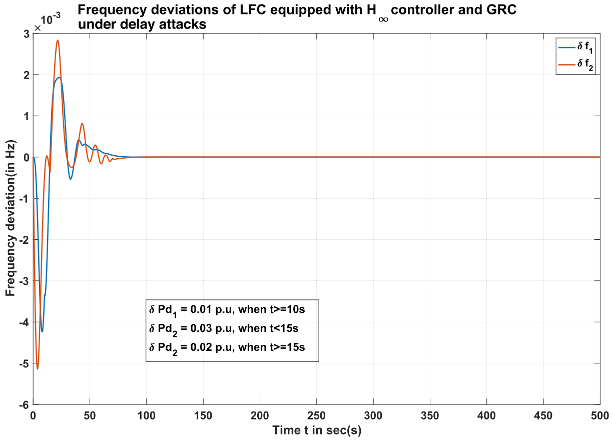

FIGURE 12. Frequency deviations of LFC system with H_∞ controller and GRC under delay attacks.

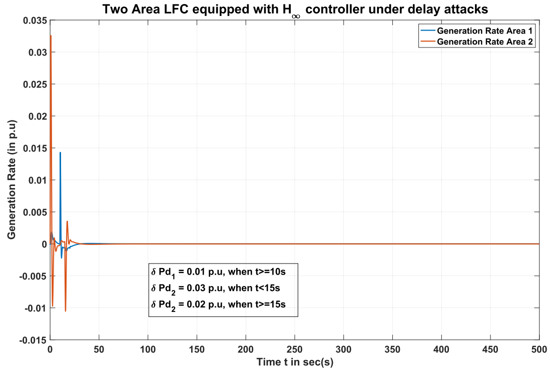

FIGURE 13. Generation rate before adding limiter.

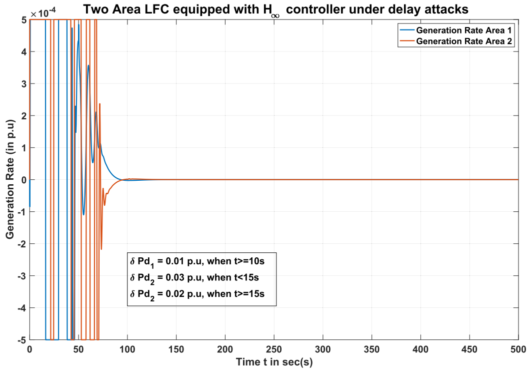

FIGURE 14. Generation rate after adding limiter.

The results, therefore, demonstrate the merit of the proposed framework in ensuring the stability and safety of a cyber-physical system under *time-delay* attacks.

V. CONCLUSION

While conventional control theory adequately addresses stability concerns and formal methods focus on safety analysis, a comprehensive and cohesive approach that seamlessly integrates stability and safety analysis for CPSs is currently lacking. In this work, we develop a robust and unified framework to ensure both the stability and safety of CPS, combining formal methods and control theory. Furthermore, we present a novel application of the developed framework by illustrating the attack mitigation of time-delay attacks on an LTI CPS.

Initially, a resilient H_∞ based controller is synthesized to ensure stability and performance under delay attacks. Subsequently, we developed a structural translation procedure to translate the state space model of the closed-loop system into timed automata. To investigate the safety aspects of the system, the timed automata models of the Plant, Controller, and Attacker are constructed, and the safety properties are verified using formal verification in UPPAAL. To showcase the practical applicability of our framework, we present a compelling case study involving a two-area LFC system with EVs. This case study serves as a demonstration of how our proposed framework effectively ensures stability and guarantees safety in the face of delay attacks.

Our future research will be aimed at extending our framework to investigate the impact of combining delay attacks with other types of cyber attacks, such as False Data Injection Attacks (FDIA) [42], [43], which necessitate the need for comprehensive attacker modelling and application of various advanced control strategies that can better enhance the performance.

REFERENCES

[1] R. Baheti and H. Gill, "Cyber-physical systems," *Impact Control Technol.*, vol. 12, no. 1, pp. 161–166, 2011.

[2] P. Agathoklis and L. Bruton, "Practical-BIBO stability of n-dimensional discrete systems," *IEE Proc. G Electron. Circuits Syst.*, vol. 130, no. 6, pp. 236–242, 1983.

[3] L. Lamport, "Proving the correctness of multiprocess programs," *IEEE Trans. Softw. Eng.*, vol. SE-3, no. 2, pp. 125–143, Mar. 1977.

[4] K. S. Xiahou, Y. Liu, and Q. H. Wu, "Robust load frequency control of power systems against random time-delay attacks," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 909–911, Jan. 2021.

[5] M. Victorio, A. Sargolzaei, and M. R. Khalghani, "A secure control design for networked control systems with linear dynamics under a time-delay switch attack," *Electronics*, vol. 10, no. 3, p. 322, Jan. 2021.

[6] G. Bahig and A. El-Kadi, "Formal verification of automotive design in compliance with ISO 26262 design verification guidelines," *IEEE Access*, vol. 5, pp. 4505–4516, 2017.

[7] N. Rajabli, F. Flammini, R. Nardone, and V. Vittorini, "Software verification and validation of safe autonomous cars: A systematic literature review," *IEEE Access*, vol. 9, pp. 4797–4819, 2021.

[8] C. Belta, B. Yordanov, and E. A. Gol, *Formal Methods for Discrete-Time Dynamical Systems*, vol. 15. Cham, Switzerland: Springer, 2017.

[9] O. A. Jasim and S. M. Veres, "Verification framework for control theory of aircraft," *Aeronaut. J.*, vol. 127, no. 1307, pp. 41–56, Jan. 2023.

[10] X. C. Ding, C. Belta, and C. G. Cassandras, "Receding horizon surveillance with temporal logic specifications," in *Proc. 49th IEEE Conf. Decis. Control (CDC)*, Dec. 2010, pp. 256–261.

[11] C. Belta and S. Sadraddini, "Formal methods for control synthesis: An optimization perspective," *Annu. Rev. Control, Robot., Auto. Syst.*, vol. 2, no. 1, pp. 115–140, May 2019.

[12] J. Qadir and O. Hasan, "Applying formal methods to networking: Theory, techniques, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 256–291, 1st Quart., 2015.

[13] J. C. Willems, "From time series to linear system—Part I. Finite dimensional linear time invariant systems," *Automatica*, vol. 22, no. 5, pp. 561–580, Sep. 1986.

[14] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[15] Z. Pang and G. Liu, "Design and implementation of secure networked predictive control systems under deception attacks," *IEEE Trans. Control Syst. Technol.*, vol. 20, no. 5, pp. 1334–1342, Sep. 2012.

[16] J. Li, X. Liu, and X. Su, "Sliding mode observer-based load frequency control of multi-area power systems under delayed inputs attack," in *Proc. Chin. Control Decis. Conf. (CCDC)*, Jun. 2018, pp. 3716–3720.

[17] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, Jan. 2018.

[18] P. Ji, J. Ye, Y. Mu, W. Lin, Y. Tian, C. Hens, M. Perc, Y. Tang, J. Sun, and J. Kurths, "Signal propagation in complex networks," *Phys. Rep.*, vol. 1017, pp. 1–96, May 2023.

[19] L. Dugard and E. I. Verriest, *Stability and Control of Time-Delay Systems*, vol. 228. Cham, Switzerland: Springer, 1998.

[20] A. Sargolzaei, K. Yen, and M. Abdelghani, "Delayed inputs attack on load frequency control in smart grid," in *Proc. ISGT*, Feb. 2014, pp. 1–5.

[21] T. R. B. Kushal, Z. Gao, J. Wang, and M. S. Illindala, "Causal chain of time delay attack on synchronous generator control," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2020, pp. 1–5.

[22] I. Kamwa, R. Grondin, and Y. Hebert, "Wide-area measurement based stabilizing control of large power systems—A decentralized/hierarchical approach," *IEEE Trans. Power Syst.*, vol. 16, no. 1, pp. 136–153, Feb. 2001.

[23] A. Sargolzaei, K. K. Yen, and M. Abdelghani, "Control of nonlinear heartbeat models under time-delay-switched feedback using emotional learning control," *Int. J. Recent Trends Eng. Technol.*, vol. 10, no. 2, p. 85, 2014.

[24] A. Sargolzaei, K. K. Yen, and M. N. Abdelghani, "Preventing time-delay switch attack on load frequency control in distributed power systems," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 1176–1185, Mar. 2016.

[25] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 1–33, May 2011.

[26] P. Ganesh, X. Lou, Y. Chen, R. Tan, D. K. Y. Yau, D. Chen, and M. Winslett, "Learning-based simultaneous detection and characterization of time delay attack in cyber-physical systems," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3581–3593, Jul. 2021.

[27] X. Lou, C. Tran, R. Tan, D. K. Y. Yau, Z. T. Kalbarczyk, A. K. Banerjee, and P. Ganesh, "Assessing and mitigating impact of time delay attack: Case studies for power grid controls," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 1, pp. 141–155, Jan. 2020.

[28] N. Pitropakis, E. Panaousis, T. Giannetsos, E. Anastasiadis, and G. Loukas, "A taxonomy and survey of attacks against machine learning," *Comput. Sci. Rev.*, vol. 34, Nov. 2019, Art. no. 100199.

[29] K. Anto, P. S. Roop, and A. K. Swain, "Formal modelling of attack scenarios and mitigation strategies in IEEE 1588," in *Proc. 19th ACM-IEEE Int. Conf. Formal Methods Models Syst. Design (MEMOCODE)*, Nov. 2021, pp. 134–141.

[30] B. Moussa, M. Debbabi, and C. Assi, "A detection and mitigation model for PTP delay attack in an IEC 61850 substation," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 3954–3965, Sep. 2018.

[31] P. Gahinet and P. Apkarian, "A linear matrix inequality approach to H_∞ control," *Int. J. Robust Nonlinear Control*, vol. 4, no. 4, pp. 421–448, 1994.

[32] X. Li and C. E. D. Souza, "Criteria for robust stability and stabilization of uncertain linear systems with state delay," *Automatica*, vol. 33, no. 9, pp. 1657–1662, Sep. 1997.

[33] S. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan, *Linear Matrix Inequalities in System and Control Theory*. Philadelphia, PA, USA: SIAM, 1994.

[34] J. Bengtsson, K. Larsen, F. Larsson, P. Pettersson, and W. Yi, "UPPAAL—A tool suite for automatic verification of real-time systems," in *Proc. Int. Hybrid Syst. Workshop*. Cham, Switzerland: Springer, 1995, pp. 232–243.

[35] G. Rodriguez-Navas, J. Proenza, and H. Hansson, "An UPPAAL model for formal verification of master/slave clock synchronization over the controller area network," in *Proc. IEEE Int. Workshop Factory Commun. Syst.*, Jun. 2006, pp. 1–10.

[36] G. Behrmann, A. David, and K. G. Larsen, "A tutorial on UPPAAL," in *Formal Methods for the Design of Real-Time Systems*. Italy: Springer, 2004, pp. 200–236.

[37] J. C. Butcher, *Numerical Methods for Ordinary Differential Equations*. Hoboken, NJ, USA: Wiley, 2016.

[38] L. Jiang, W. Yao, Q. H. Wu, J. Y. Wen, and S. J. Cheng, "Delay-dependent stability for load frequency control with constant and time-varying delays," *IEEE Trans. Power Syst.*, vol. 27, no. 2, pp. 932–941, May 2012.

[39] T. N. Pham, H. Trinh, and L. V. Hien, "Load frequency control of power systems with electric vehicles and diverse transmission links using distributed functional observers," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 238–252, Jan. 2016.

[40] A. Swain and A. Mohanty, "Adaptive load frequency control of an interconnected hydro thermal system considering generation rate constraints," *J.-Inst. Eng. India El Elect. Eng. Division*, vol. 76, pp. 109–114, Jan. 1995.

[41] M. L. Kothari, P. S. Satsangi, and J. Nanda, "Sampled-data automatic generation control of interconnected reheat thermal systems considering generation rate constraints," *IEEE Trans. Power App. Syst.*, vol. PAS-100, no. 5, pp. 2334–2342, May 1981.

[42] X. Huang and J. Dong, "Reliable leader-to-follower formation control of multiagent systems under communication quantization and attacks," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 50, no. 1, pp. 89–99, Jan. 2020.

[43] X. Huang and J. Dong, "An adaptive secure control scheme for T–S fuzzy systems against simultaneous stealthy sensor and actuator attacks," *IEEE Trans. Fuzzy Syst.*, vol. 29, no. 7, pp. 1978–1991, Jul. 2021.

KELVIN ANTO (Member, IEEE) received the M.Eng.St. degree (Hons.) in electrical and electronic engineering from The University of Auckland, Auckland, New Zealand, in 2018, where he is currently pursuing the Ph.D. degree in electrical and electronic engineering. His research interests include the resilience of cyber-physical systems against cyber-attacks particularly using formal methods and control theory.

AKSHYA KUMAR SWAIN (Senior Member, IEEE) received the B.Sc. (Eng.) degree in electrical engineering, the M.E. degree in electronic systems and communication, and the Ph.D. degree in control engineering from The University of Sheffield, Sheffield, U.K., in 1985, 1988, and 1996, respectively. He has authored over 200 papers in international journals and conferences. His research interests include nonlinear system identification and control, machine learning, and big data.

He is an Associate Editor of IEEE Sensors Journal and an Editorial Board Member of *International Journal of Automation and Control* and *International Journal of Sensors, Wireless Communications and Control*.

PARTHA ROOP (Member, IEEE) received the B.E. degree in computer science and engineering from the College of Engineering, Anna University, Chennai, India, in 1989, the M.Tech. degree in computer science and engineering from the Indian Institute of Technology Kharagpur, Kharagpur, India, in 1993, and the Ph.D. degree in computer science (software engineering) from The University of New South Wales, Sydney, NSW, Australia, in 2001. He is currently a Professor with the Department of Electrical, Computer, and Software Engineering, The University of Auckland, Auckland, New Zealand. His research interests include the design and validation of cyber-physical systems using formal methods, including in digital health and artificial intelligence (AI) applications in cyber-physical systems.