Critical-Time Analysis of Cyber-Physical Systems subject to Actuator Attacks and Faults

Arthur Perodou, Christophe Combastel, Ali Zolghadri

Critical-Time Analysis of Cyber-Physical Systems subject to Actuator Attacks and Faults

Arthur Perodou, Christophe Combastel and Ali Zolghadri, *Senior Member*, *IEEE*

***Abstract*— A novel quantitative criterion, namely critical time, is investigated to characterize the degree of resilience of controlled cyber-physical systems. Resilience is defined as system's ability to contain the maximal impact of anomalies and recover to a nominal mode. Anomalies are understood as any kind of attack or fault that leads to abnormal behavior of the controlled system. The critical time is the maximal time-horizon for which a system is considered to be safe after the occurrence of an anomaly. An increase of critical time will leave more time for defense mechanisms, including human operators, to detect and mitigate anomalies. While most of the literature focuses on the impact part of resilience, this criterion is tied with the recovery part. In this work, it is shown how the computation of the critical time can be done for discrete-time LTI models. To achieve this, sufficient conditions in the form of iterative LMI-based algorithms are established. A numerical example is provided to illustrate the theoretical results.**

Keywords: resilience, cyber-physical systems, security, quadratic constraints.

I. Introduction

An open challenge in cyber-physical systems (CPS) security is to find an appropriate trade-off between the desired security level and the satisfaction of a performance level of practical interest. In the last decade, the System and Control community has developed numerous methods to address this issue [1], [2]. A relevant concept that has emerged is resilience. Resilience is the system's ability to contain the maximal impact of anomalies and recover to a nominal mode [1], [3], [4], where an anomaly is understood here as any difference between the behaviors of a system and a suitable operating model, resulting for instance from an attack or a fault.

There exist several criteria to quantify the resilience of a system [1], [2]. For instances, the anomalies effect on the cost function of an optimal control problem is considered in [4]; in [5], the attacks are additionally constrained to be stealthy; in [6], the maximum perturbation on the state trajectory is evaluated for stealthy attacks with minimum resources. While these works focus on the impact part of the concept of resilience, additional resilient metrics tied to the recovery part are proposed in [7], such as the required time to recover to normal operation, but no explicit computing methods are provided. In this work, we investigate and compute a new resilience criterion, namely critical time.

The critical time is the maximal time-horizon for which a system is considered to be safe after the occurrence of an anomaly, that is the system is not in a critical state and is still able to recover to a normal mode. The underlying motivation is that an increase of critical time allows more time for defense mechanisms, including human operators, to detect and mitigate anomalies. In particular, this criterion covers the detection and reconfiguration delays classically used in the fault-management literature [8], [9].

In this paper, the critical time will be computed for any actuator anomaly that is allowed by the physical limitations of the actuators. This includes for instance deny-of-service (DoS) or false-data injection attacks on actuators. To achieve this, we will take advantage from the framework of quadratic constraints (QC). This framework has led to numerous methods for system analysis [10], [11], [12] and synthesis [13], [14], [15]. However, to the best of our knowledge, no analog problems to critical time computation were considered using QCs. An important benefit of the QC framework is its special link with linear matrix inequality (LMI) optimization [16].

The contribution of this paper is considered to be twofold: (i) Firstly, a new criterion for evaluating the resilience of a system is proposed and (ii) Secondly, the critical-time computation problem is tackled for a discrete-time linear time-invariant (LTI) system under actuator anomalies subject to actuator limitations. By using the QC framework, it is shown that this leads to solve iterative algorithms involving LMI feasibility problems.

The paper is organized as follows. First, brief reminders on QCs are provided in Section II. In Section III, the critical-time computation problems, with pre-specified or free initial state, are explicitly formulated. In Section IV and Section V, it is then shown how the computation of the critical time can be done for discrete-time LTI models. Finally, an illustrative example is provided in Section VI, while Section VII provides some concluding remarks.

II. Preliminaries

A. Notations

Lower (upper) case letters are used for vectors (matrices). $\mathbb{N}$ denotes the set of natural numbers, $\mathbb{Z}$ the set of integers, $[\![k_1, k_2]\!]$ the integers between, and including, k_1 and k_2, $\mathbb{R}^{n\times m}$ the set of real-valued matrices of size $n \times m$ and $\mathbb{D}^n$ the set of diagonal real-valued matrices of size $n \times n$. For the sake of brevity, $z_{[\![k_1,k_2]\!]} := \begin{bmatrix} z'_{k_1} & \dots & z'_{k_2} \end{bmatrix}'$ is used. I_n and $0_{n\times m}$ are respectively the identity matrix of $\mathbb{R}^{n\times n}$ and

The authors are with Univ. Bordeaux, IMS-lab, CNRS UMR 5218, Bat. A31, 351 cours de la Libération, 33400, Talence, France. e-mail: {arthur.perodou, christophe.combastel, ali.zolghadri}@ims-bordeaux.fr

This study has been carried out with financial support from the French National Research Agency (ANR) in the framework of the Investments for the Future Programme IdEx Bordeaux—SysNum (ANR-10-IDEX-03-02). The financial support from the "Conseil Régional de la Nouvelle-Aquitaine" is also gratefully acknowledged.

the zero matrix of $\mathbb{R}^{n\times m}$. The subscripts are omitted when obvious from the context. X' stands for transpose of X while $M > (\text{resp. } \geq)\ 0$ denotes positive (semi-) definiteness. $\mathrm{trace}(M)$ is the sum of the diagonal elements of M and $\mathrm{diag}(M)$ is their concatenation in a column vector. The sign $\otimes$ represents the Kronecker product. Bold characters denote either explicit decision variables in a design problem or optimization variables in an optimization problem.

B. Background

In this work, constraint sets will be defined using QCs.

Definition 1 (Quadratic constraint):
A vector $z \in \mathbb{R}^n$ is said to satisfy a quadratic constraint ϕ, with $\phi = \phi' \in \mathbb{R}^{(n+1)\times(n+1)}$, if $\begin{bmatrix} z \\ 1 \end{bmatrix}' \phi \begin{bmatrix} z \\ 1 \end{bmatrix} \geq 0$ holds.

Define $\phi := \begin{bmatrix} Q & s \\ s' & r \end{bmatrix}$, where $Q = Q' \in \mathbb{R}^{n\times n}$, $s \in \mathbb{R}^{n\times 1}$ and $r \in \mathbb{R}$. Notice that if $Q \leq 0$, the set of all vectors $z \in \mathbb{R}^n$ that satisfy the previous QC is convex. In particular, the resulting set is inside an ellipsoid if $Q < 0$ and in a halfspace if $Q = 0$. Finally, observe the following lemma.

Lemma 1:
Let $z \in \mathbb{R}$ be a real scalar. Then:

$$z \in [z_{min}, z_{max}] \ \Leftrightarrow\ \begin{bmatrix} z \\ 1 \end{bmatrix}' \begin{bmatrix} -1 & z_c \\ z_c & z_r^2 - z_c^2 \end{bmatrix} \begin{bmatrix} z \\ 1 \end{bmatrix} \geq 0$$

where $z_c := (z_{min} + z_{max})/2$ and $z_r := (z_{max} - z_{min})/2$.

An important result in the QC framework is the so-called S-procedure.

Lemma 2 (S-procedure for quadratic constraints [17]):
Consider the following quadratic functions: $\forall z \in \mathbb{R}^n$,

$$\sigma_q(z) = \begin{bmatrix} z \\ 1 \end{bmatrix}' \begin{bmatrix} Q_q & s_q \\ s_q' & r_q \end{bmatrix} \begin{bmatrix} z \\ 1 \end{bmatrix}, \quad q = 0, 1, \ldots, N$$

where $Q_q = Q_q' \in \mathbb{R}^{n\times n}$, $s_q \in \mathbb{R}^{n\times 1}$ and $r_q \in \mathbb{R}$.
Then $(ii) \Rightarrow (i)$.

(i) The constraint $\sigma_0(z) \geq 0$ holds for all $z \in \mathbb{R}^n$ such that $\sigma_q(z) \geq 0$, $q = 1, \ldots, N$.

(ii) There exist $\boldsymbol{\tau_q} \geq 0$, $q = 1, \ldots, N$, such that

$$\begin{bmatrix} Q_0 & s_0 \\ s_0' & r_0 \end{bmatrix} - \sum_{q=1}^{N} \boldsymbol{\tau_q} \begin{bmatrix} Q_q & s_q \\ s_q' & r_q \end{bmatrix} \geq 0$$

III. Problem Statement

A. Critical-time definition

Consider a controlled cyber-physical system subject to general anomalies modeled as:

$$\begin{cases} x_{k+1} = Ax_k + Bu_k + E_{1_k}\alpha_k + D_{1_k}d_k \\ y_k = Cx_k + E_{2_k}\alpha_k + D_{2_k}d_k \end{cases}$$

where $x_k \in \mathbb{R}^n$, $u_k \in \mathbb{R}^m$, and $y_k \in \mathbb{R}^l$ are respectively the state, the control input and the measured output signals evaluated at time k. The anomaly $\alpha_k \in \mathbb{R}^{m_\alpha}$ stands for either attacks or faults. The vector $d_k \in \mathbb{R}^w$ models additive noise or unknown disturbance, and may include model uncertainties. In a similar fashion to [8], this linear time-varying model covers actuator, sensor and component anomalies.

Moreover, assume that the signals u, α and d are constrained by $\mathcal{S}_u \subseteq \mathbb{R}^m$, $\mathcal{S}_\alpha \subseteq \mathbb{R}^{m_\alpha}$ and $\mathcal{S}_d \subseteq \mathbb{R}^w$ such that:

$$\forall k \in \mathbb{Z}, \quad u_k \in \mathcal{S}_u \qquad \alpha_k \in \mathcal{S}_\alpha \qquad d_k \in \mathcal{S}_d$$

In addition, assume that a safety set $\mathcal{S}_s$, that is a set of states x for which the system is considered to be safe, is provided. The safety set $\mathcal{S}_s$ may be derived from physical constraints or the validity domain of a linearized model. Finally, without loss of generality, assume that the anomalies appear from initial time $k = 0$.

Definition 2 (Critical-time):
The critical time k_c is the maximal time-horizon k_f such that, after the occurrence of an anomaly, the system is safe over the time-window $\mathcal{I}(k_f) := [\![0, k_f]\!]$. Using previous notations:

$$k_c = \max\{k_f \,|\forall k \in \mathcal{I}(k_f), \forall u_k \in \mathcal{S}_u, \forall \alpha_k \in \mathcal{S}_\alpha, \forall d_k \in \mathcal{S}_d, x_k \in \mathcal{S}_s\}$$

There are several expected benefits from availability of the critical-time criterion. First, one can evaluate the time that can be allowed for defense mechanisms. Moreover, by considering all states that additionally satisfy some performance criteria $\mathcal{S}_p \subseteq \mathcal{S}_s$, one may improve the resilience of the system by driving it to the state that has the maximum critical-time, while guaranteeing a performance level. Finally, it is expected to provide a relevant trade-off between anomalies with opposite impacts, as for instance in the case of DoS attacks and attacks by upper saturation.

In the sequel, two problems are formulated and solved: 1) the computation of the critical-time for a system in a given state x_0 and 2) the computation of the critical-time when the initial state x_0 is to be selected among a set of admissible states that satisfy some performance constraints $\mathcal{S}_p$.

B. Problem formulation

This paper focusing on actuator anomalies, $m_\alpha = m$ and

$$\forall k \in \mathbb{Z}, \qquad E_{1_k} = B \quad D_{1_k} = D \quad E_{2_k} = 0 \quad D_{2_k} = 0$$

are considered, where $D \in \mathbb{R}^{n\times w}$ is a known matrix. Then, by defining the contaminated input $u_a := u + \alpha$, the controlled system under actuator anomalies is described as:

$$(\Sigma): \begin{cases} x_{k+1} = Ax_k + Bu_{a_k} + Dd_k \\ y_k = Cx_k \end{cases} \tag{1}$$

In addition, due to physical limitations, such as saturation or slew rate, assume that the abnormal input u_a is constrained by a given set $\mathcal{S}_a \subseteq \mathbb{R}^m$ as follows: $\forall k \in \mathbb{N},\ u_{a_k} \in \mathcal{S}_a$.

Remark 1: Under previous assumptions, a significant class of anomalies are considered, such as actuator additive faults, DoS attacks or attacks by saturation. By considering the augmented system of (Σ) interconnected with a controller by a communication network, this may also include abnormal control inputs, resulting for instance from measurement falsification, or from direct attacks on the controller.

Moreover, assume that the sets $\mathcal{S}_p$, $\mathcal{S}_s$, $\mathcal{S}_a$ and $\mathcal{S}_d$ are defined using multiple quadratic constraints such as:

$$\mathcal{S}_p := \cap_{h=1}^{n_p}\{x_0 \in \mathbb{R}^n, \sigma_{p_h}(x_0) \geq 0\} \quad (2)$$
$$\mathcal{S}_s := \cap_{i=1}^{n_s}\{x \in \mathbb{R}^n, \sigma_{s_i}(x) \geq 0\} \quad (3)$$
$$\mathcal{S}_a := \cap_{j=1}^{n_a}\{u_a \in \mathbb{R}^m, \sigma_{a_j}(u_a) \geq 0\} \quad (4)$$
$$\mathcal{S}_d := \cap_{g=1}^{n_d}\{d \in \mathbb{R}^w, \sigma_{d_g}(d) \geq 0\} \quad (5)$$

where

$$\sigma_{p_h}(x_0) := \begin{bmatrix} Cx_0 \\ 1 \end{bmatrix}' \begin{bmatrix} Q_{p_h} & s_{p_h} \\ s'_{p_h} & r_{p_h} \end{bmatrix} \begin{bmatrix} Cx_0 \\ 1 \end{bmatrix}$$
$$\sigma_{s_i}(x) := \begin{bmatrix} x \\ 1 \end{bmatrix}' \begin{bmatrix} Q_{s_i} & s_{s_i} \\ s'_{s_i} & r_{s_i} \end{bmatrix} \begin{bmatrix} x \\ 1 \end{bmatrix}$$
$$\sigma_{a_j}(u_a) := \begin{bmatrix} u_a \\ 1 \end{bmatrix}' \begin{bmatrix} Q_{a_j} & s_{a_j} \\ s'_{a_j} & r_{a_j} \end{bmatrix} \begin{bmatrix} u_a \\ 1 \end{bmatrix}$$
$$\sigma_{d_g}(d) := \begin{bmatrix} d \\ 1 \end{bmatrix}' \begin{bmatrix} Q_{d_g} & s_{d_g} \\ s'_{d_g} & r_{d_g} \end{bmatrix} \begin{bmatrix} d \\ 1 \end{bmatrix}$$

The problem of computing the critical-time of a system for a given initial state x_0 is now explicitly formulated.

Problem 1 (Critical-time computation for a given x_0):
GIVEN

- a system (Σ) modeled by (1) with initial state $x_0 \in \mathbb{R}^n$,
- a safety set $\mathcal{S}_s$ defined by (3),
- an abnormal input set $\mathcal{S}_a$ defined by (4),
- a disturbance set $\mathcal{S}_d$ defined by (5),

FIND the maximal time-index $\boldsymbol{k_f}$ such that system (1) is safe over the time-window $\mathcal{I}_{\boldsymbol{k_f}} = [\![0, \boldsymbol{k_f}]\!]$ for all abnormal inputs of $\mathcal{S}_a$ and disturbances of $\mathcal{S}_d$:

$$\max_{\boldsymbol{k_f} \in \mathbb{N}} \boldsymbol{k_f}$$

subject to $\forall k \in [\![0, \boldsymbol{k_f}]\!]$, $\forall u_{a_k} \in \mathbb{R}^m$, $\forall d_k \in \mathbb{R}^w$,

$$\forall i = 1, \ldots, n_s, \qquad \sigma_{s_i}(x_k) \geq 0 \quad (6)$$
$$\forall j = 1, \ldots, n_a, \qquad \sigma_{a_j}(u_{a_k}) \geq 0 \quad (7)$$
$$\forall g = 1, \ldots, n_d, \qquad \sigma_{d_g}(d_k) \geq 0 \quad (8)$$

hold.

A second interesting problem is the computation of the critical-time of a system for which the initial state x_0 is not specified but assumed to belong to the performance domain $\mathcal{S}_p$. The resulting state may then be used as a target state for resilient control.

Problem 2 (System critical-time computation):
GIVEN $\mathcal{S}_s$, $\mathcal{S}_a$ and $\mathcal{S}_d$ as in Problem 1 and

- a system (Σ) modeled by (1),
- a performance set $\mathcal{S}_p$ defined by (2)

FIND $\boldsymbol{x_0} \in \mathcal{S}_p$ that maximizes the time index $\boldsymbol{k_f}$ such that the system (1) is safe over the time-window $\mathcal{I}_{\boldsymbol{k_f}} = [\![0, \boldsymbol{k_f}]\!]$ for all abnormal inputs of $\mathcal{S}_a$ and disturbances of $\mathcal{S}_d$:

$$\max_{\boldsymbol{x_0} \in \mathbb{R}^n,\ \boldsymbol{k_f} \in \mathbb{N}} \boldsymbol{k_f}$$

subject to $\forall k \in [\![0, \boldsymbol{k_f}]\!]$, $\forall u_{a_k} \in \mathbb{R}^m$, $\forall d_k \in \mathbb{R}^w$, $(6) - (8)$,

$$\forall h = 1, \ldots, n_p, \qquad \sigma_{p_h}(\boldsymbol{x_0}) \geq 0 \quad (9)$$

hold.

IV. CRITICAL-TIME COMPUTATION WITH SPECIFIED x_0

In this section, Problem 1 is tackled. To achieve this, the sub-problem of checking if the state x_{k_f} is into the safety set $\mathcal{S}_s$, over all abnormal inputs of $\mathcal{S}_a$ and disturbances of $\mathcal{S}_d$, for a fixed time-index k_f is first considered. Then, an algorithm is proposed to find the maximum k_f, providing an under-estimate of the critical time k_c: $k_f \leq k_c$.

A. Fixed time-index k_f

Assume that $x_0 \in \mathbb{R}^n$ is given and $k_f \in \mathbb{N}$ is fixed. Define P_k and G_k as: $P_0 = 0$, $G_0 = 0$ and for all $k \geq 1$,

$$P_k = \begin{bmatrix} A^{k-1}B & \ldots & AB & B \end{bmatrix}$$
$$G_k = \begin{bmatrix} A^{k-1}D & \ldots & AD & D \end{bmatrix}$$

Using the recursive equation of (1), x_{k_f} is computed as:

$$x_{k_f} = A^{k_f}x_0 + P_{k_f}u_{a_{[\![0,k_f-1]\!]}} + G_{k_f}d_{[\![0,k_f-1]\!]} \quad (10)$$

This property enables to solve an alternative version of Problem 1, with fixed k_f, as shown in next lemma.

Lemma 3:
Let (Σ) be a system defined by (1) with a given state x_0. Consider the associate sets $\mathcal{S}_s$, $\mathcal{S}_a$ and $\mathcal{S}_d$ given by (3)-(5). Assume that the time-index $k_f \in \mathbb{N}$ is fixed.
Then $(i) \Rightarrow (ii)$.

(i) $\forall i = 1, \ldots, n_s$, $\forall j = 1, \ldots, n_a$, $\forall g = 1, \ldots, n_d$, $\exists \mathbf{T_{i,j}} \in \mathbb{D}^{k_f} \geq 0$, $\exists \boldsymbol{\Theta_{i,g}} \in \mathbb{D}^{k_f} \geq 0$,

$$N'_{k_f}\begin{bmatrix} Q_{s_i} & s_{s_i} + Q_{s_i}A^{k_f}x_0 \\ (s_{s_i} + Q_{s_i}A^{k_f}x_0)' & r_{s_i} + 2s'_{s_i}A^{k_f}x_0 \end{bmatrix} N_{k_f}$$
$$- \sum_{j=1}^{n_a}\begin{bmatrix} \mathbf{T_{i,j}} \otimes Q_{a_j} & 0 & \mathrm{diag}\,(\mathbf{T_{i,j}}) \otimes s_{a_j} \\ 0 & 0 & 0 \\ \mathrm{diag}\,(\mathbf{T_{i,j}})' \otimes s'_{a_j} & 0 & \mathrm{trace}(\mathbf{T_{i,j}}r_{a_j}) \end{bmatrix}$$
$$- \sum_{g=1}^{n_d}\begin{bmatrix} 0 & 0 & 0 \\ 0 & \boldsymbol{\Theta_{i,g}} \otimes Q_{d_g} & \mathrm{diag}\,(\boldsymbol{\Theta_{i,g}}) \otimes s_{d_g} \\ 0 & \mathrm{diag}\,(\boldsymbol{\Theta_{i,g}})' \otimes s'_{d_g} & \mathrm{trace}(\boldsymbol{\Theta_{i,g}}r_{d_g}) \end{bmatrix}$$
$$+ \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & (A^{k_f}x_0)'Q_{s_i}A^{k_f}x_0 \end{bmatrix} \geq 0 \quad (11)$$

where $N_k := \begin{bmatrix} P_k & G_k & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

(ii) The system (Σ) with initial state x_0 is safe at time k_f for all past abnormal inputs of $\mathcal{S}_a$ and disturbances of $\mathcal{S}_d$: $\forall k \in [\![0, k_f - 1]\!]$, $\forall u_{a_k} \in \mathbb{R}^m$, $\forall d_k \in \mathbb{R}^w$, $(7) - (8)$,

$$\forall i = 1, \ldots, n_s, \qquad \sigma_{s_i}(x_{k_f}) \geq 0$$

hold.

Proof: See App. A. ∎

Remark 2: Condition (i) is a feasibility optimization problem with LMI constraints. It is then solvable in polynomial-time. This computational advantage comes at the price of the conservatism of condition (i), that implies but is not equivalent to condition (ii). This results from the application of the S-procedure (see [13], [17], and the references therein, for a detailed discussion).

B. Critical-time computation

In order to compute the critical-time k_c, Algorithm 1 is proposed. Based on the sufficient condition provided by Lemma 3, the time index k_f is incremented until there is no more solution to the LMI feasibility problem. An under-estimate of the critical-time k_c is so obtained and ensures that the system is safe at least until the obtained result k_f^*.

Theorem 1:
Let (Σ) be a system defined by (1) with a given state x_0. Consider the associate sets $\mathcal{S}_s$, $\mathcal{S}_a$ and $\mathcal{S}_d$ given by (3)-(5). Denote k_f^* as the solution returned by Algorithm 1.
Then the system (Σ) with initial state x_0 is safe over the time-window $\mathcal{I}(k_f^*) = [\![0, k_f^*]\!]$ and for all abnormal inputs of $\mathcal{S}_a$ and disturbances of $\mathcal{S}_d$.

Proof: By Lemma 3, (Σ) is safe for each $k \in \mathcal{I}(k_f^*)$. ■

Algorithm 1: Critical-time computation with fixed x_0

```
k_f ← 0
f ← true
while f do
    k_f ← k_f + 1
    f ← isFeasible(
    ∃ {T_{i,j} ∈ D^{k_f} ≥ 0, i = 1,...,n_s, j = 1,...,n_a},
    ∃ {Θ_{i,g} ∈ D^{k_f} ≥ 0, i = 1,...,n_s, g = 1,...,n_d},
    such that (11) hold. )
    /* true if a solution is found /*
k_f ← k_f − 1
return k_f
```

V. System Critical-Time Computation

In this section, Problem 2 is tackled. Analogous to Section IV, the sub-problem of finding an initial state $\boldsymbol{x_0} \in \mathcal{S}_p$ such that $x_k \in \mathcal{S}_s$, $k \in [\![0, k_f]\!]$, over all abnormal inputs of $\mathcal{S}_a$ and disturbances of $\mathcal{S}_d$, for a fixed time-index k_f is first considered. Then, an algorithm is proposed to find the maximum k_f, providing an under-estimate of the system critical-time k_c, as well as a related state x_0.

A. Fixed time-index k_f

First, the problem of finding an initial state $\boldsymbol{x_0}$ for a fixed time-index k_f is addressed.

Lemma 4:
Let (Σ) be a system defined by (1). Consider the associate sets $\mathcal{S}_p$, $\mathcal{S}_s$, $\mathcal{S}_a$ and $\mathcal{S}_d$ given by $(2)-(5)$. Assume that

$$\begin{aligned} \forall h = 1,\dots,n_p, \quad Q_{p_h} \leq 0 \text{ and } \quad r_{Q_{p_h}} := \operatorname{rank}(Q_{p_h}) \geq 1 \\ \forall i = 1,\dots,n_s, \quad Q_{s_i} \leq 0 \text{ and } \quad r_{Q_{s_i}} := \operatorname{rank}(Q_{s_i}) \geq 1 \end{aligned}$$

Factorize each Q_{p_h} and Q_{s_i} such as

$$Q_{p_h} := V_{p_h}' \Sigma_{p_h} V_{p_h} \qquad Q_{s_i} := V_{s_i}' \Sigma_{s_i} V_{s_i}$$

where $\Sigma_{p_h} < 0 \in \mathbb{D}^{r_{Q_{p_h}}}$, $V_{p_h} \in \mathbb{R}^{r_{Q_{p_h}} \times l}$, $\Sigma_{s_i} < 0 \in \mathbb{D}^{r_{Q_{s_i}}}$ and $V_{s_i} \in \mathbb{R}^{r_{Q_{s_i}} \times n}$. In addition, assume that $k_f \in \mathbb{N}$ is fixed. Then $(i) \Rightarrow (ii)$.

(i) $\exists \boldsymbol{x_0} \in \mathbb{R}^n$ subject to
$\forall h = 1,\dots,n_p$,

$$\begin{bmatrix} r_{p_h} + 2s'_{p_h}(C\boldsymbol{x_0}) & (V_{p_h} C\boldsymbol{x_0})' \\ V_{p_h} C\boldsymbol{x_0} & -\Sigma_{p_h}^{-1} \end{bmatrix} \geq 0 \tag{12}$$

$\forall i = 1,\dots,n_s$, $\forall j = 1,\dots,n_a$, $\forall g = 1,\dots,n_d$, $\forall k \in [\![0, k_f]\!]$, $\exists \mathbf{T}_{\boldsymbol{i,j,k}} \in \mathbb{D}^k \geq 0$, $\exists \boldsymbol{\Theta}_{\boldsymbol{i,g,k}} \in \mathbb{D}^k \geq 0$,

$$\begin{aligned} &\widehat{N}'_{k,s_i} \begin{bmatrix} Q_{s_i} & s_{s_i} + Q_{s_i} A^k \boldsymbol{x_0} & 0 \\ (s_{s_i} + Q_{s_i} A^k \boldsymbol{x_0})' & r_{s_i} + 2s'_{s_i} A^k \boldsymbol{x_0} & 0 \\ 0 & 0 & 0 \end{bmatrix} \widehat{N}_{k,s_i} \\ &- \sum_{j=1}^{n_a} \begin{bmatrix} \mathbf{T}_{\boldsymbol{i,j,k}} \otimes Q_{a_j} & 0 & \operatorname{diag}(\mathbf{T}_{\boldsymbol{i,j,k}}) \otimes s_{a_j} & 0 \\ 0 & 0 & 0 & 0 \\ \operatorname{diag}(\mathbf{T}_{\boldsymbol{i,j,k}})' \otimes s'_{a_j} & 0 & \operatorname{trace}(\mathbf{T}_{\boldsymbol{i,j,k}} r_{a_j}) & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \\ &- \sum_{g=1}^{n_d} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & \boldsymbol{\Theta}_{\boldsymbol{i,g,k}} \otimes Q_{d_g} & \operatorname{diag}(\boldsymbol{\Theta}_{\boldsymbol{i,g,k}}) \otimes s_{d_g} & 0 \\ 0 & \operatorname{diag}(\boldsymbol{\Theta}_{\boldsymbol{i,g,k}})' \otimes s'_{d_g} & \operatorname{trace}(\boldsymbol{\Theta}_{\boldsymbol{i,g,k}} r_{d_g}) & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \\ &+ \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \left(V_{s_i} A^k \boldsymbol{x_0}\right)' \\ 0 & 0 & V_{s_i} A^k \boldsymbol{x_0} & -\Sigma_{s_i}^{-1} \end{bmatrix} \geq 0 \end{aligned} \tag{13}$$

where $\widehat{N}_{k,s_i} := \begin{bmatrix} N_k & 0 \\ 0 & 0_{r_{Q_{s_i}} \times r_{Q_{s_i}}} \end{bmatrix}$.

(ii) There exists an admissible initial state $\boldsymbol{x_0} \in \mathcal{S}_p$ such that system (1) is safe over the time-window $[\![0, k_f]\!]$ for all abnormal inputs of $\mathcal{S}_a$ and disturbances of $\mathcal{S}_d$: $\forall k \in [\![0, k_f]\!]$, $\forall u_{a_k} \in \mathbb{R}^m$, $\forall d_k \in \mathbb{R}^w$, $(6)-(9)$ hold.

Proof: By the Schur Lemma [17], (12) is equivalent to (9), i.e. $\boldsymbol{x_0} \in \mathcal{S}_p$. In addition, by Lemma 3 coupled with the application of the Schur Lemma, (13) implies that the system is safe at each time step k. As this is true for all $k \in [\![0, k_f]\!]$, the system is safe over the whole interval. ■

Similarly to Lemma 3, condition (ii) is a feasibility problem with LMI constraints, relying on the S-procedure.

Remark 3: The factorization of symmetric matrices Q_{p_h} and Q_{s_i} may be obtained using an eigenvalue decomposition. For instance: $\exists U_{p_h} \in \mathbb{R}^{l \times l}$, $\exists \Sigma_{p_h} \in \mathbb{R}^{r_{Q_{p_h}} \times r_{Q_{p_h}}}$,

$$Q_{p_h} = U'_{p_h} \begin{bmatrix} \Sigma_{p_h} & 0 \\ 0 & 0 \end{bmatrix} U_{p_h} = U'_{p_h} \begin{bmatrix} I & 0 \end{bmatrix}' \Sigma_{p_h} \begin{bmatrix} I & 0 \end{bmatrix} U_{p_h}$$

The matrix V_{p_h} can then be defined as $V_{p_h} := \begin{bmatrix} I & 0 \end{bmatrix} U_{p_h}$.

B. System critical-time computation

To compute the critical-time and an associate x_0, Algorithm 2 is proposed. Based on Lemma 4, k_f is incremented until there is no more solution to the LMI feasibility problem. The resulting under-estimate k_f^* of the critical-time k_c, ensures that the system with initial state x_0^* is safe until k_f^*.

Theorem 2:
Let (Σ) be defined by (1) and consider the sets $\mathcal{S}_p$, $\mathcal{S}_s$, $\mathcal{S}_a$ and $\mathcal{S}_d$ as in Lemma 4. Denote k_f^* and x_0^* the solutions returned by Algorithm 2. Then the system (Σ) with admissible initial state $x_0^* \in \mathcal{S}_p$ is safe over the time-window $\mathcal{I}(k_f^*) = [\![0, k_f^*]\!]$ and for all abnormal inputs of $\mathcal{S}_a$ and disturbances of $\mathcal{S}_d$.

Proof: This follows by application of Lemma 4. ■

Algorithm 2: System critical-time computation

$k_f \leftarrow 0$
$x_{0_{k_f}} \leftarrow [\,]$ /* empty set /*
$f \leftarrow false$
while $not(f)$ **do**
  $k_f \leftarrow k_f + 1$
  $x_0 \leftarrow x_{0_{k_f}}$
  $x_{0_{k_f}} \leftarrow$ Find $\boldsymbol{x_0} \in \mathbb{R}^n$ subject to: $\forall k \in [\![0, k_f]\!]$,
  $\exists \left\{\mathbf{T_{i,j,k}} \in \mathbb{D}^k \geq 0, i = 1, \ldots, n_s, j = 1, \ldots, n_a\right\}$,
  $\exists \left\{\mathbf{\Theta_{i,g,k}} \in \mathbb{D}^k \geq 0, i = 1, \ldots, n_s, g = 1, \ldots, n_d\right\}$,
   such that (12), (13) hold
  $f \leftarrow isempty(x_{0_{k_f}})$ /* true if no solution /*
$k_f \leftarrow k_f - 1$
return k_f, x_0

C. Lemma 4 with halfspace sets

In Lemma 4, the sets were assumed to be ellipsoidal, potentially partially rank-degenerated, that is described by quadratic constraints such as in Definition 1 with $Q \leq 0$. One may notice that halfspace sets, i.e. when $Q = 0$, may be straightly considered by simply removing appropriate lines and columns in (12) or (13). For instance, if $Q_{p_h} = 0$, (12) is replaced by the following LMI

$$r_{p_h} + 2s'_{p_h}(C\boldsymbol{x_0}) \geq 0$$

VI. Illustration

In this section, a numerical example is provided to illustrate the main results established in the previous sections. Consider a system given by (1) with:

$$A = \begin{bmatrix} 0.9710 & 0.0563 \\ 0 & 0.9428 \end{bmatrix} \quad B = \begin{bmatrix} 0.0181 \\ 0.0173 \end{bmatrix} \quad C = \begin{bmatrix} 0.5 \\ 0 \end{bmatrix}'$$

For the sake of clarity, no disturbance d is considered. Moreover, it is assumed that the performance constraint leads to $y_0 \in [y_{min}, y_{max}]$, where $y_{min} = 0.363$ and $y_{max} = 3.27$, for all $k \in \mathbb{Z}$ the system is safe if $x_k(1) \in [x_{1_{min}}, x_{1_{max}}]$ and $x_k(2) \in [x_{2_{min}}, x_{2_{max}}]$, where $x_{1_{min}} = x_{2_{min}} = 0.10$, $x_{1_{max}} = 6.90$ and $x_{2_{max}} = 1.72$, while the actuator limitations allow only inputs $u_a \in [u_{min}, u_{max}]$, where $u_{min} = 0$ and $u_{max} = 6$. The performance set $\mathcal{S}_p$ and the actuator-limitations set $\mathcal{S}_a$ are then defined using (2), (4) and Lemma 1, while the safety set $\mathcal{S}_s$ is defined by (3) and

$$\left[\begin{array}{c|c} Q_{s_1} & s_{s_1} \\ \hline s'_{s_1} & r_{s_1} \end{array}\right] = \left[\begin{array}{cc|c} -1.00 & 0 & 3.50 \\ 0 & 0 & 0 \\ \hline 3.50 & 0 & -0.690 \end{array}\right]$$

$$\left[\begin{array}{c|c} Q_{s_2} & s_{s_2} \\ \hline s'_{s_2} & r_{s_2} \end{array}\right] = \left[\begin{array}{cc|c} 0 & 0 & 0 \\ 0 & -1.00 & 0.912 \\ \hline 0 & 0.912 & -0.172 \end{array}\right]$$

For illustration purposes, the system is simulated starting from the initial points $x_{0_1} = \begin{bmatrix} 1.4536 & 0.3629 \end{bmatrix}'$ and $x_{0_2} = \begin{bmatrix} 5.8143 & 1.4517 \end{bmatrix}'$ under either a DoS attack, i.e. $u_a = 0$, or an attack by upper saturation, i.e. $u_a = u_{max}$, that occurs from $k_a = 10$. The evolution of $x(2)$ is plotted in Fig. 1.

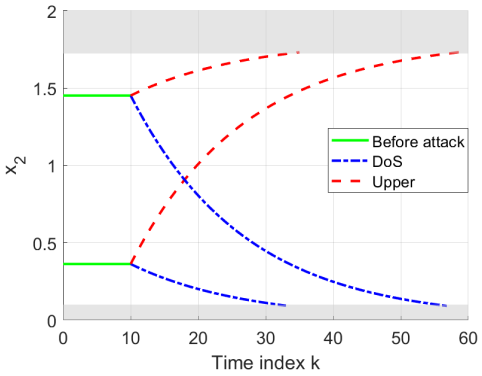

Fig. 1. Illustration of DoS and Upper saturation attacks on x_2 starting from two different initial points. Grey parts represent unsafe regions.

Applying Theorem 2, Algorithm 2 is solved using the Robust Control Toolbox of MATLAB. The maximal time-index is found $k_f^* = 38$ with $x_0^* = \begin{bmatrix} 1.9035 & 0.9946 \end{bmatrix}'$. To provide a comparative insight of this result, a DoS attack and an attack by upper saturation are applied to the system for different initial points and the related critical-time index k_c is computed for each attack. For the sake of illustration, these initial points are arbitrarily chosen such that $x_0^{\{\lambda\}} = \lambda \cdot x_0^\star$, where $\lambda \in \mathbb{R}$. The simulation results plotted in Fig. 2 highlight the tradeoff arising when both attacks are considered. The index k_f^* suggests to be an adequate tradeoff to ensure the maximal time for defense mechanisms.

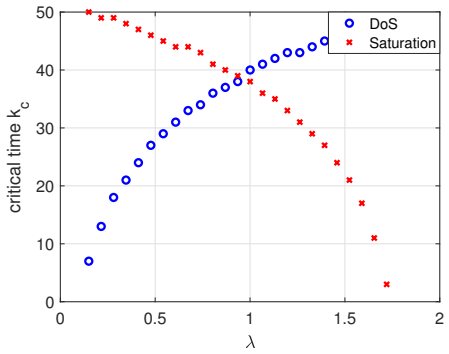

Fig. 2. Illustration critical time index k_c for different initial state x_0 and trade-off between DoS attack and attack by saturation

VII. Conclusion

In this paper, a novel criterion, namely critical time, was investigated to characterize the degree of resilience of controlled CPS subject to actuator anomalies, including attacks or faults. This criterion has been defined as the maximum time-horizon for which a system is ensured to be safe after the occurrence of an anomaly. Using the framework of quadratic constraints, sufficient conditions have been established to compute the critical time of discrete-time LTI systems through iterative LMI-based algorithms. This

work paves the way for further investigations. This includes extension to more general attack models, for instance replay or covert attacks, and system dynamics as nonlinear or multi-agent systems, the use of other convex sets such as zonotopes [18] and the integration of communication and networking models. This is a topic of our current research.

APPENDIX

A. Proof of Lemma 3

Proof:

First, denote $\mathcal{I} := [\![0, k_f - 1]\!]$ and $z_{\mathcal{I}} := \begin{bmatrix} u'_{a_{\mathcal{I}}} & d'_{\mathcal{I}} \end{bmatrix}'$. Using (10), rewrite $\sigma_{s_i}(x_{k_f})$ and define $\rho_{s_i}(z_{\mathcal{I}})$ as follows

$$\sigma_{s_i}(x_{k_f}) = \underbrace{\begin{bmatrix} z_{\mathcal{I}} \\ 1 \end{bmatrix}' \begin{bmatrix} \widetilde{Q}_{s_i} & \widetilde{s}_{s_i} \\ \widetilde{s}'_{s_i} & \widetilde{r}_{s_i} \end{bmatrix} \begin{bmatrix} z_{\mathcal{I}} \\ 1 \end{bmatrix}}_{:=\rho_{s_i}(z_{\mathcal{I}})}$$

$$\begin{aligned} \text{where} \quad \widetilde{Q}_{s_i} &:= \begin{bmatrix} P_{k_f} & G_{k_f} \end{bmatrix}' Q_{s_i} \begin{bmatrix} P_{k_f} & G_{k_f} \end{bmatrix} \\ \widetilde{s}_{s_i} &:= \begin{bmatrix} P_{k_f} & G_{k_f} \end{bmatrix}' \left(Q_{s_i} A^{k_f} x_0 + s_{s_i} \right) \\ \widetilde{r}_{s_i} &:= \left(x_0 A^{k_f} \right)' Q_{s_i} A^{k_f} x_0 + 2 s'_{s_i} A^{k_f} x_0 + r_{s_i} \end{aligned}$$

Moreover, define $\rho_{a_j,k}(z_{\mathcal{I}})$ and $\rho_{d_g,k}(z_{\mathcal{I}})$ as $\forall k \in \mathcal{I}$,

$$\rho_{a_j,k}(z_{\mathcal{I}}) := \begin{bmatrix} z_{\mathcal{I}} \\ 1 \end{bmatrix}' \begin{bmatrix} Q_{a_j,k} & s_{a_j,k} \\ s'_{a_j,k} & r_{a_j,k} \end{bmatrix} \begin{bmatrix} z_{\mathcal{I}} \\ 1 \end{bmatrix}$$

$$\rho_{d_g,k}(z_{\mathcal{I}}) := \begin{bmatrix} z_{\mathcal{I}} \\ 1 \end{bmatrix}' \begin{bmatrix} Q_{d_g,k} & s_{d_g,k} \\ s'_{d_g,k} & r_{d_g,k} \end{bmatrix} \begin{bmatrix} z_{\mathcal{I}} \\ 1 \end{bmatrix}$$

where

$$Q_{a_j,k} := \begin{bmatrix} E_k \otimes Q_{a_j} & 0 \\ 0 & 0_{w \cdot k_f} \end{bmatrix} \quad Q_{d_g,k} := \begin{bmatrix} 0_{m \cdot k_f} & 0 \\ 0 & E_k \otimes Q_{d_g} \end{bmatrix}$$

$$\begin{aligned} s_{a_j,k} &:= \begin{bmatrix} \operatorname{diag}(E_k)' \otimes s_{a_j} & 0_{m \times (w \cdot k_f)} \end{bmatrix} & r_{a_j,k} &:= r_{a_j} \\ s_{d_g,k} &:= \begin{bmatrix} 0_{w \times (m \cdot k_f)} & \operatorname{diag}(E_k)' \otimes s_{d_g} \end{bmatrix} & r_{d_g,k} &:= r_{d_g} \end{aligned}$$

$$E_k := \begin{bmatrix} 0_k & & \\ & 1 & \\ & & 0_{k_f - 1 - k} \end{bmatrix}$$

This implies $\rho_{a_j,k}(z_{\mathcal{I}}) = \sigma_{a_j}(u_{a_k})$, $\rho_{d_g,k}(z_{\mathcal{I}}) = \sigma_{d_g}(d_k)$. Thus, condition (ii) is equivalent to find if, $\forall i = 1, \ldots, n_s$, $\rho_{s_i}(z_{\mathcal{I}}) \geq 0$ holds for all $z_{\mathcal{I}} \in \mathbb{R}^{(m+w) \cdot k_f}$ such that, $\forall k \in \mathcal{I}$, $\forall j = 1, \ldots, n_a$, $\forall g = 1, \ldots, n_d$, $\rho_{a_j,k}(z_{\mathcal{I}}) \geq 0$ and $\rho_{d_g,k}(z_{\mathcal{I}}) \geq 0$. Applying the S-procedure, this is implied by: $\exists \{ \boldsymbol{\tau_{i,j,k}} \geq 0 \}$, $\exists \{ \boldsymbol{\theta_{i,g,k}} \geq 0 \}$, such that $\forall z_{\mathcal{I}} \in \mathbb{R}^{(m+w) \cdot k_f}$,

$$\begin{aligned} \rho_{s_i}(z_{\mathcal{I}}) - \sum_{j=1}^{n_a} \sum_{k=0}^{k_f - 1} \boldsymbol{\tau_{i,j,k}} \rho_{a_j,k}(z_{\mathcal{I}}) \\ - \sum_{g=1}^{n_d} \sum_{k=0}^{k_f - 1} \boldsymbol{\theta_{i,g,k}} \rho_{d_g,k}(z_{\mathcal{I}}) \geq 0 \end{aligned}$$

that is equivalent to

$$\begin{aligned} \begin{bmatrix} \widetilde{Q}_{s_i} & \widetilde{s}_{s_i} \\ \widetilde{s}'_{s_i} & \widetilde{r}_{s_i} \end{bmatrix} - \sum_{j=1}^{n_a} \sum_{k=0}^{k_f - 1} \boldsymbol{\tau_{i,j,k}} \begin{bmatrix} Q_{a_j,k} & s_{a_j,k} \\ s'_{a_j,k} & r_{a_j,k} \end{bmatrix} \\ - \sum_{g=1}^{n_d} \sum_{k=0}^{k_f - 1} \boldsymbol{\theta_{i,g,k}} \begin{bmatrix} Q_{d_g,k} & s_{d_g,k} \\ s'_{d_g,k} & r_{d_g,k} \end{bmatrix} \geq 0 \end{aligned}$$

Finally, define $\mathbf{T}_{\boldsymbol{i,j}} := \begin{bmatrix} \boldsymbol{\tau_{i,j,0}} & & \\ & \ddots & \\ & & \boldsymbol{\tau_{i,j,k_f-1}} \end{bmatrix}$ and note

$$\begin{aligned} \sum_{k=0}^{k_f - 1} \boldsymbol{\tau_{i,j,k}} \begin{bmatrix} Q_{a_j,k} & s_{a_j,k} \\ s'_{a_j,k} & r_{a_j,k} \end{bmatrix} \\ = \begin{bmatrix} \mathbf{T}_{\boldsymbol{i,j}} \otimes Q_{a_j} & 0 & \operatorname{diag}(\mathbf{T}_{\boldsymbol{i,j}}) \otimes s_{a_j} \\ 0 & 0 & 0 \\ \operatorname{diag}(\mathbf{T}_{\boldsymbol{i,j}})' \otimes s'_{a_j} & 0 & \operatorname{trace}(\mathbf{T}_{\boldsymbol{i,j}} r_{a_j}) \end{bmatrix} \end{aligned}$$

Similar reasoning for $\Theta_{i,g}$ leads to condition (i). ■

REFERENCES

[1] S. M. Dibaji, M. Pirani, D. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "A Systems and Control Perspective of CPS Security," *Annual Reviews in Control*, vol. 47, 2019.

[2] M. S. Chong, H. Sandberg, and A. Teixeira, "A Tutorial Introduction to Security and Privacy for Cyber-Physical Systems," in *2019 18th European Control Conference (ECC)*, 2019, pp. 968–978.

[3] C. G. Rieger, D. I. Gertman, and M. A. McQueen, "Resilient Control Systems: Next Generation Design Research," in *2009 2nd Conference on Human System Interactions*, 2009, pp. 632–636.

[4] Q. Zhu and T. Basar, "Game-Theoretic Methods for Robustness, Security, and Resilience of Cyberphysical Control Systems," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 46–65, 2015.

[5] A. Teixeira, H. Sandberg, and K. H. Johansson, "Strategic stealthy attacks: The output-to-output l2-gain," in *2015 54th IEEE Conference on Decision and Control (CDC)*, 2015, pp. 2582–2587.

[6] A. Teixeira, K. C. Sou, H. Sandberg, and K. H. Johansson, "Secure Control Systems: A Quantitative Risk Management Approach," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 24–45, 2015.

[7] D. Wei and K. Ji, "Resilient Industrial Control System (RICS): Concepts, Formulation, Metrics, and Insights," in *2010 3rd International Symposium on Resilient Control Systems*, 2010, pp. 15–22.

[8] I. Hwang, S. Kim, Y. Kim, and C. E. Seah, "A Survey of Fault Detection, Isolation, and Reconfiguration Methods," *IEEE Transactions on Control Systems Technology*, vol. 18, no. 3, pp. 636–653, 2010.

[9] Y. Zhang and J. Jiang, "Bibliographical Review on Reconfigurable Fault-Tolerant Control Systems," *Annual Reviews in Control*, vol. 32, no. 2, pp. 229–252, 2008.

[10] A. Megretski and A. Rantzer, "System Analysis via Integral Quadratic Constraints," *IEEE Transactions on Automatic Control*, vol. 42, no. 6, pp. 819–830, 1997.

[11] G. Scorletti, X. Bombois, M. Barenthin, and V. Fromion, "Improved Efficient Analysis for Systems with Uncertain Parameters," in *2007 46th IEEE Conference on Decision and Control*, 2007, pp. 5038–5043.

[12] C. W. Scherer and J. Veenman, "Stability Analysis by Dynamic Dissipation Inequalities: on merging Frequency-Domain Techniques with Time-Domain Conditions," *Systems & Control Letters*, vol. 121, pp. 7–15, 2018.

[13] T. Iwasaki and S. Hara, "Generalized KYP Lemma: Unified Frequency Domain Inequalities with Design Applications," *IEEE Transactions on Automatic Control*, vol. 50, no. 1, pp. 41–59, 2005.

[14] A. Perodou, A. Korniienko, M. Zarudniev, and G. Scorletti, "Frequency Design of Interconnected Dissipative Systems: a Unified LMI Approach," in *2018 IEEE Conference on Decision and Control (CDC)*, 2018, pp. 6250–6255.

[15] A. Perodou, A. Korniienko, G. Scorletti, M. Zarudniev, J. B. David, and I. O'Connor, "Frequency Design of Lossless Passive Electronic Filters: A State-Space Formulation of the Direct Synthesis Approach," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 68, no. 1, pp. 161–174, 2021.

[16] S. P. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan, *Linear Matrix Inequalities in System and Control Theory*. SIAM, 1994, vol. 15.

[17] U. T. Jönsson, "A lecture on the S-procedure," *Lecture Note at the Royal Institute of technology, Sweden*, vol. 23, pp. 34–36, 2001.

[18] C. Combastel and A. Zolghadri, "A Distributed Kalman Filter with symbolic Zonotopes and Unique Symbols Provider for Robust State Estimation in CPS," *International Journal of Control*, vol. 93, no. 11, pp. 2596–2612, dec 2019.