Quantitative Resilience of Generalized Integrators

Jean-Baptiste Bouvier, Kathleen Xu, and Melkior Ornik *Senior Member, IEEE*

***Abstract*— When failure is not an option, systems are designed to be resistant to various malfunctions, like a loss of control authority over actuators. This malfunction consists in some actuators producing uncontrolled and thus possibly undesirable inputs with their full actuation range. After such a malfunction, a system is deemed resilient if its target is still reachable despite these undesirable inputs. However, the malfunctioning system might be significantly slower to reach its target compared to its initial capabilities. To quantify this loss of performance we introduce the notion of quantitative resilience as the maximal ratio over all targets of the minimal reach times for the initial and malfunctioning systems. Since quantitative resilience is then defined as four nested nonlinear optimization problems, we establish an efficient computation method for control systems with multiple integrators and nonsymmetric input sets. Relying on control theory and on two specific geometric results we reduce the computation of quantitative resilience to a linear optimization problem. We illustrate our method on an octocopter.**

***Index Terms*— fault-tolerant, linear systems, optimization, quantitative resilience, reachability, time-invariant.**

I. Introduction

RESISTANCE to malfunctions is usually acquired through actuator redundancy and fault-tolerant controllers [1] using adaptive control [2] or active disturbance rejection [3]. Fault-tolerant theory typically considers either actuators locking in place [2], actuators losing effectiveness but remaining controllable [1], or a combination of both [3]. However, after damage [4] or hostile takeover, some actuators may produce undesirable inputs with their full actuation range over which the controller has readings but no control. Such a malfunction happened to the Nauka module as it docked to the International Space Station [4] and has been previously discussed in [5] under the name of *loss of control authority over actuators*.

Manuscript received July 10, 2022. This work was supported by an Early Stage Innovations grant from NASA's Space Technology Research Grants Program, grant no. 80NSSC19K0209. This material is partially based upon work supported by the United States Air Force AFRL/SBRK under contract no. FA864921P0123.

J.-B. Bouvier is with the Department of Aerospace Engineering, University of Illinois Urbana-Champaign, Urbana, IL 61801 USA (e-mail: bouvier3@illinois.edu).

K. Xu was with the University of Illinois Urbana-Champaign and is now with the Department of Aeronautics and Astronautics, Massachussetts Institute of Technology, Cambridge, MA 80523 USA (e-mail: bfst@mit.edu).

M. Ornik is with the Department of Aerospace Engineering and the Coordinated Science Laboratory, University of Illinois Urbana-Champaign, Urbana, IL 61801 USA (e-mail: mornik@illinois.edu).

In contrast to the robust control framework where the undesirable inputs may not be observable and have a small magnitude compared to the actuators' inputs [6], in the setting of loss of control authority, undesirable inputs are observable and can have a magnitude similar to the controlled inputs. As demonstrated in [7], a robust controller generally cannot handle a loss of control authority over actuators.

After a partial loss of control authority over actuators, a target is *resiliently reachable* if for any undesirable inputs of the malfunctioning actuators there exists a control driving the state to the target [5]. However, the malfunctioning system might need considerably more time to reach its target compared to the initial system. To measure the delays caused by the loss of control authority, we rely on the notion of quantitative resilience introduced in [8]. Similar concepts have been previously developed for nuclear power plants [9], but were limited to their specific applications.

We formulate quantitative resilience as the maximal ratio over all targets of the minimal reach times for the initial and malfunctioning systems. This formulation leads to a nonlinear minimax optimization problem with an infinite number of constraints. Our main contribution is to reduce the quantitative resilience of systems with multiple integrators to a linear optimization problem. To do so we combine two optimization results designed specifically for this application [10] with the theorems of [11], [12] stating the existence of time-optimal controls. However, these controls are bang-bang [13], [14] and hence cannot be exactly implemented by physical actuators. As a first step towards a more high-fidelity application, we then incorporate propellers' dynamics to our octocopter model and quantify its resilience.

The contributions of this paper are threefold. First, we propose an efficient method to compute the quantitative resilience of linear systems with multiple integrators and nonsymmetric inputs by simplifying a nonlinear problem of four nested optimizations into a single linear optimization problem. Second, we establish necessary and sufficient conditions to verify if a system is resilient to the loss of control over one of its actuators. Finally, we provide all the proofs omitted from [8].

The remainder of the paper is organized as follows. Section II introduces preliminary notions on resilience. We calculate the optimal reach times for the initial and malfunctioning systems in Section III. The pinnacle of this work is the efficient method to compute quantitative resilience in Section IV for the loss of control over a single actuator. This metric also allows to assess whether a system is resilient, as detailed in

Section V. We study the quantitative resilience of systems with multiple integrators in Section VI before applying our theory to an octocopter losing control over one of its propellers in Section VII.

A preliminary version of this work was presented in [8], where simpler dynamics were used. We now extend our theory to linear systems with multiple integrators and general input sets. Sections VI and VII are entirely novel, and we provide all the proofs omitted from [8].

Notation: For a set $\mathcal{X}$ we denote its boundary $\partial\mathcal{X}$, its interior $\text{int}(\mathcal{X}) := \mathcal{X}\backslash\partial\mathcal{X}$. The set of time functions taking value in $\mathcal{X}$ is denoted $\mathcal{F}(\mathcal{X}) := \big\{f : f(t) \in \mathcal{X} \text{ for all } t \geq 0\big\}$. The set of integers between a and b included is $[\![a, b]\!]$. The factorial of $k \in \mathbb{N}$ is denoted $k!$. Let $\mathbb{R}^+ := [0, \infty)$ and we use the subscript $_*$ to exclude zero, for instance $\mathbb{R}^+_* := (0, \infty)$. The Euclidean norm is $\|\cdot\|$ and the unit sphere is $\mathbb{S} := \{x \in \mathbb{R}^n : \|x\| = 1\}$. For $k \in \mathbb{N}$, the k^{th} derivative of function f is denoted as $f^{(k)}$.

II. Preliminaries and problem statement

The control of a physical system usually involves steering its position with inputs only affecting its acceleration [15]. With these systems in mind, we focus on generalized k^{th} order integrators in $\mathbb{R}^n$, i.e.,

$$x^{(k)}(t) = \bar{B}\bar{u}(t), \quad \bar{u}(t) \in \bar{\mathcal{U}},\ x(0) = x_0,\ x^{(l)}(0) = 0, \quad (1)$$

for all $l \in [\![1, k-1]\!]$ and $k \in \mathbb{N}$. Matrix $\bar{B} \in \mathbb{R}^{n\times(m+p)}$ is constant. The control set is the hyperrectangle $\bar{\mathcal{U}} := \prod_{i=1}^{m+p} \big[\bar{u}_i^{min}, \bar{u}_i^{max}\big] \subseteq \mathbb{R}^{m+p}$, with $\bar{u} \in \mathcal{F}(\bar{\mathcal{U}})$.

After a malfunction, the system loses control authority over p of its $m+p$ actuators. We then split $\bar{B}$ into B and C, $\bar{\mathcal{U}}$ into $\mathcal{U}$ and $\mathcal{W}$, and $\bar{u}$ into the remaining control inputs $u \in \mathcal{F}(\mathcal{U})$ and the undesirable inputs $w \in \mathcal{F}(\mathcal{W})$. Then, the initial conditions are the same as in (1) but the dynamics become

$$x^{(k)}(t) = Bu(t) + Cw(t), \quad u(t) \in \mathcal{U},\ w(t) \in \mathcal{W}, \quad (2)$$

$$\mathcal{U} := \prod_{i=1}^{m} \big[u_i^{min}, u_i^{max}\big], \quad \mathcal{W} := \prod_{i=1}^{p} \big[w_i^{min}, w_i^{max}\big].$$

We now recall the definition of *resilience* from [7].

Definition 1: System (1) is *resilient* to the loss of p of its actuators corresponding to the matrix C as above if for all undesirable inputs $w \in \mathcal{F}(\mathcal{W})$ and all target $x_{goal} \in \mathbb{R}^n$ there exists a control $u_w \in \mathcal{F}(\mathcal{U})$ and a time T such that the state of the system (2) reaches the target at time T, i.e., $x(T) = x_{goal}$.

While a resilient system is by definition capable of reaching any target after a partial loss of control authority, the malfunctioning system might be considerably slower than the initial system to reach the same target. We introduce the following two reach times for the target $x_{goal} \in \mathbb{R}^n$ and the target distance $d := x_{goal} - x_0 \in \mathbb{R}^n$.

Definition 2: The *nominal reach time of order* k $T^*_{k,N}$, is the shortest time required for the state x of (1) to reach the target x_{goal} under admissible control $\bar{u} \in \mathcal{F}(\bar{\mathcal{U}})$:

$$T^*_{k,N}(d) := \inf_{\bar{u}\,\in\,\mathcal{F}(\bar{\mathcal{U}})} \big\{T \geq 0 : x(T) - x_0 = d\big\}. \quad (3)$$

Definition 3: The *malfunctioning reach time of order* k $T^*_{k,M}$, is the shortest time required for the state x of (2) to reach the target x_{goal} under admissible control $u \in \mathcal{F}(\mathcal{U})$ when the undesirable input $w \in \mathcal{F}(\mathcal{W})$ is chosen to make that time the longest:

$$T^*_{k,M}(d) := \sup_{w\,\in\,\mathcal{F}(\mathcal{W})} \Big\{ \inf_{u\,\in\,\mathcal{F}(\mathcal{U})} \big\{T \geq 0 : x(T) - x_0 = d\big\}\Big\}. \quad (4)$$

The causality issue arising from (4) is discussed at the end of the section. By definition, if the system is controllable, then $T^*_{k,N}(d)$ is finite for all $d \in \mathbb{R}^n$, and if it is resilient, then $T^*_{k,M}(d)$ is also finite. The malfunctioning system (2) can take up to $\frac{T^*_{k,M}(d)}{T^*_{k,N}(d)}$ times longer than the initial system (1) to reach the target $d + x_0$.

Definition 4: The *quantitative resilience of order* k of system (2) is

$$r_{k,q} := \inf_{d\,\in\,\mathbb{R}^n_*} \frac{T^*_{k,N}(d)}{T^*_{k,M}(d)}. \quad (5)$$

For a resilient system, $r_{k,q} \in (0, 1]$. The closer $r_{k,q}$ is to 1, the smaller is the loss of performance caused by the malfunction.

Problem 1: How to calculate efficiently $r_{k,q}$?

Indeed, a naive computation of $r_{k,q}$ requires solving four nested optimization problems whose constraint sets are $\mathbb{R}^n_*$ and three infinite-dimensional function spaces. A brute force approach to this problem is doomed to fail.

We will explore thoroughly the simple case $k = 1$ in the following sections and generalize their results to $k \in \mathbb{N}$ in Section VI. For $k = 1$, systems (1) and (2) simplify into

$$\dot{x}(t) = \bar{B}\bar{u}(t), \qquad \bar{u}(t) \in \bar{\mathcal{U}}, \quad x(0) = x_0 \in \mathbb{R}^n, \quad (6)$$

$$\dot{x}(t) = Bu(t) + Cw(t), \quad u(t) \in \mathcal{U},\ w(t) \in \mathcal{W}. \quad (7)$$

For brevity, in the case $k = 1$ we lose the subscript 1 and write the *nominal reach time* $T^*_N = T^*_{1,N}$ as

$$T^*_N(d) := \inf_{\bar{u}\,\in\,\mathcal{F}(\bar{\mathcal{U}})} \Big\{T \geq 0 : \int_0^T \bar{B}\bar{u}(t)\,dt = d\Big\}, \quad (8)$$

with $d = x_{goal} - x_0$. Similarly, we write the *malfunctioning reach time* $T^*_M = T^*_{1,M}$ as

$$T^*_M(d) := \sup_{w\,\in\,\mathcal{F}(\mathcal{W})} \left\{ \inf_{u\,\in\,\mathcal{F}(\mathcal{U})} \Big\{T \geq 0 : \int_0^T \big[Bu(t) + Cw(t)\big]\,dt = d\Big\}\right\}. \quad (9)$$

The *quantitative resilience* r_q of a system following (7) is then

$$r_q := \inf_{d\,\in\,\mathbb{R}^n_*} \frac{T^*_N(d)}{T^*_M(d)} = r_{1,q}. \quad (10)$$

We now discuss the information setting in the malfunctioning system. The resilience framework of [5], [7] assumes that u has only access to the past and current values of w, but not to their future. Then, the optimal control u^* in (9) cannot anticipate a truly random undesirable input w. Hence, this strategy is not likely to result in the global time-optimal trajectory of Definition 3.

In fact, there would be no single obvious choice for $u^*\big(t, w(t)\big)$, rendering T^*_M ill-defined and certainly not time-optimal, whereas T^*_N is time-optimal. In this case, our concept of quantitative resilience becomes meaningless. The work [16] states that to calculate u^* without future knowledge of w^*

the only technique is to solve the intractable Isaac's equation. Thus, the paper [16] derives only suboptimal solutions and concludes that its practical contribution is minimal.

Instead, we follow [17] where the inputs u^* and w^* are both chosen to make the transfer from x_0 to x_{goal} time-optimal in the sense of Definition 3. The controller knows that w^* will be chosen to make T_M^* the longest. Thus, u^* is chosen to react optimally to this worst undesirable input. Then, w^* is chosen, and to make T_M^* the longest, it is the same as the controller had predicted. Hence, from an outside perspective it looks as if the controller knew w^* in advance, as reflected by (4).

We will prove in the following sections that with this information setting w^* is constant. Then, the controller can more easily and more reasonably predict what is the worst w^* and build the adequate u^*. With these two input signals, T_M^* is time-optimal in the sense of Definition 3 and can be meaningfully compared with T_N^* to define the quantitative resilience of control systems.

III. Optimal reach times

We start with the dynamical system (6) to calculate the nominal reach time T_N^* of (8). We easily show in Lemma 1 of Appendix I, that if system (6) is controllable, the optimal control $\bar{u}^*$ of (8) exists and is constant:

$$T_N^*(d) = \min_{\bar{u}\,\in\,\bar{\mathcal{U}}}\big\{T \geq 0 : \bar{B}\bar{u}\,T = d\big\}. \tag{11}$$

Since the input set $\bar{\mathcal{U}}$ is bounded, the controllability of system (6) is equivalent to $\operatorname{rank}(\bar{B}) = n$ and $0 \in \operatorname{int}(\bar{\mathcal{U}})$ [18]. The multiplication of variables $\bar{u}$ and T makes (11) a bilinear optimization problem. For easier computation, we solve instead the linear optimization $T_N^*(d) = 1/\max_{\bar{u}\,\in\,\bar{\mathcal{U}}}\big\{\lambda : \bar{B}\bar{u} = \lambda d\big\}$.

We now study the malfunctioning system (7) to compute the malfunctioning reach time T_M^* of (9). As above, we easily prove in Lemma 2 of Appendix I that if system (7) is resilient, the optimal control $u^*(w)$ of (9) exists and is constant for any undesirable input $w \in \mathcal{F}(\mathcal{W})$:

$$T_M^*(d) = \sup_{w\,\in\,\mathcal{F}(\mathcal{W})}\left\{\min_{u^*(w)\,\in\,\mathcal{U}}\left\{T : Bu^*(w)T + \int_0^T Cw(t)\,dt = d\right\}\right\}. \tag{12}$$

Tackling the supremum in (12) requires a different approach.

Proposition 1: If system (7) is resilient, then for all $d \in \mathbb{R}_*^n$ the supremum $T_M^*(d)$ of (9) is a maximum achieved by a constant undesirable input $w^* \in \mathcal{W}$.

Proof: For $w \in \mathcal{F}(\mathcal{W})$, let $w^c := \int_0^{T_M(w,d)} \frac{w(t)}{T_M(w,d)}\,dt$ with T_M defined in (24). Then, for $i \in [\![1,p]\!]$ we have $w_i^{min} \leq w_i(t) \leq w_i^{max}$. Integrating yields $w_i^{min} \leq w_i^c \leq w_i^{max}$, so $w^c \in \mathcal{W}$. Then, $\int_0^{T_M(w,d)} Cw(t)dt = Cw^cT_M(w,d) = d - Bu^*(w)T_M(w,d)$.

Conversely, note that for all $w^c \in \mathcal{W}$ and $T > 0$, we can define $w(t) := \frac{1}{T}w^c$ for $t \in [0,T]$ such that $\int_0^T Cw(t)\,dt = Cw^c$ and $w \in \mathcal{F}(\mathcal{W})$. Thus, the constraint space of the supremum of (9) can be restricted to constant inputs in $\mathcal{W}$.

We define the function $\varphi(w) := Bu^*(w) + Cw$ for $w \in \mathcal{W}$. When applying the constant inputs w and $u^*(w)$, dynamics (7) become $\dot{x} = \varphi(w)$. Because $\big(Bu^*(w) + Cw\big)T_M(w,d) = d$, we have $\varphi(w) = \frac{1}{T_M(w,d)}d$ and φ is continuous in w according to Lemma 3 in Appendix I. Set $\mathcal{W}$ is compact and $x_0 \in \mathbb{R}^n$ is fixed. Then, Theorem 1 of [12] states that $\mathcal{A}_{\mathcal{W}} := \big\{(x_1,T) : \int_0^T \varphi(w)dt = x_1 - x_0,\ \text{for } w \in \mathcal{W}\big\}$ is compact. Note that $T_M^*(d) = \sup\big\{T : (x_{goal},T) \in \mathcal{A}_{\mathcal{W}}\big\}$ is the supremum of a continuous function over the compact set $\mathcal{A}_{\mathcal{W}}$, so $T_M^*(d)$ is a maximum achieved on $\mathcal{W}$. ■

Then, the malfunctioning reach time becomes

$$T_M^*(d) = \max_{w\,\in\,\mathcal{W}}\left\{\min_{u\,\in\,\mathcal{U}}\big\{T \geq 0 : \big(Bu + Cw\big)T = d\big\}\right\}. \tag{13}$$

We will show that the maximum of (13) is achieved by an extreme undesirable input, i.e., at the set of vertices of $\mathcal{W}$, denoted by $\mathcal{V}$. However, we cannot directly apply the bang-bang principle, as it has been mostly derived for systems with a linear dependency on the input [11], [13], [14], while φ introduced in Proposition 1 is not linear in w. The works [12], [19], [20] consider a nonlinear φ, but they require conditions that are not satisfied in our case. Thus, we need a new optimization result, namely Theorem 2.1 from [10], which applies to polytopes.

Definition 5: A *polytope* in $\mathbb{R}^n$ is a compact intersection of finitely many half-spaces.

We define $\mathcal{X} := \big\{Cw : w \in \mathcal{W}\big\}$ and $\mathcal{Y} := \big\{Bu : u \in \mathcal{U}\big\}$. Since $\mathcal{U}$ and $\mathcal{W}$ are polytopes, so are $\mathcal{X}$ and $\mathcal{Y}$ [21].

Proposition 2: If system (7) is resilient, then $\dim \mathcal{Y} = n$ and $-\mathcal{X} \subseteq \operatorname{int}(\mathcal{Y})$.

Proof: Following Proposition 1 we know that for all $x \in \mathcal{X}$ and all $d_0 \in \mathbb{R}^n$ there exist $y \in \mathcal{Y}$ and $T \geq 0$ such that $(x+y)T = d_0$. Since d_0 can be freely chosen in $\mathbb{R}^n$, we must have $\dim \mathcal{Y} = n$.

Take $d_0 = x \in \mathcal{X}$, $x \neq 0$. Then, there exists $y_1 \in \mathcal{Y}$ and $T_1 > 0$ such that $(x + y_1)T_1 = x$. Hence, $\lambda_1 x \in \mathcal{Y}$ with $\lambda_1 := -1 + 1/T_1$. Now take $d_0 = -x$. Then, there exists $y_2 \in \mathcal{Y}$ and $T_2 > 0$ such that $(x + y_2)T_2 = -x$. Hence, $\lambda_2 x \in \mathcal{Y}$ with $\lambda_2 := -1 - 1/T_2$. Since $\lambda_2 \leq -1 \leq \lambda_1$ and $\mathcal{Y}$ is convex, we have $-x \in \mathcal{Y}$.

If $x = 0$, this process fails because we would get $T = 0$ when taking $d = 0$. Instead, take $d_0 \in \mathbb{S}$. Then there exist $T > 0$ and $y \in \mathcal{Y}$ such that $yT = d_0$. Repeating the same for $-d_0$ and using the convexity of $\mathcal{Y}$ as in the previous paragraph, we obtain $0 \in \mathcal{Y}$. Thus $-\mathcal{X} \subseteq \mathcal{Y}$.

Assume that there exists $-x_1 \in -\mathcal{X} \cap \partial\mathcal{Y}$. For $d = -x_1$, $T_M(x_1,-x_1) = \min_{y\,\in\,\mathcal{Y}}\big\{T \geq 0 : (x_1 + y)T = -x_1\big\}$, with T_M introduced in (24). Since $T \geq 0$, the optimal y (called y^*) must make $x_1 + y$ positively collinear with $-x_1$. Thus, y^* is positively collinear with $-x_1$ and the largest it can be is $y^* = -x_1$ because $-x_1 \in \partial\mathcal{Y}$. Then, the constraint in $T_M(x_1,-x_1)$ is $0T = -x_1$. The lack of solution contradicts the resilience of the system. Thus, $-\mathcal{X} \cap \partial\mathcal{Y} = \varnothing$, i.e., $-\mathcal{X} \subseteq \operatorname{int}(\mathcal{Y})$. ■

We now prove that the maximum of (13) is achieved on $\mathcal{V}$.

Proposition 3: If system (7) is resilient, then for all $d \in \mathbb{R}_*^n$, the maximum of (13) is achieved with a constant input $w^* \in \mathcal{V}$.

Proof: Replacing $\frac{1}{T}$ by λ in (13) leads to $T_M^*(d) = 1/\min_{x\,\in\,\mathcal{X}}\big\{\max_{y\,\in\,\mathcal{Y}}\big\{\lambda > 0 : x + y = \lambda d\big\}\big\}$. Since $\lambda \geq 0$, we write

$\lambda = |\lambda| = \|\lambda d\|/\|d\| = \|x+y\|/\|d\|$. Then,

$$T_M^*(d) = \frac{\|d\|}{\min\limits_{x\in\mathcal{X}}\{\max\limits_{y\in\mathcal{Y}}\{\|x+y\| : x+y \in \mathbb{R}^+ d\}\}}. \quad (14)$$

Following Proposition 2, we can apply Theorem 2.1 of [10] and conclude that the argument of the minimum in (14) is at a vertex x^* of $\mathcal{X}$. Since the transformation between $\mathcal{W}$ and $\mathcal{X}$ is linear, $x^* = Cv$ with $v \in \mathcal{V}$ a vertex of $\mathcal{W}$ [21]. Therefore, the maximum of (13) is achieved on $\mathcal{V}$. ∎

We have then reduced the outer constraint set of (9) from an infinite-dimensional function set $\mathcal{F}(\mathcal{W})$ to a finite set $\mathcal{V}$ of cardinality 2^p with p the number of malfunctioning actuators. Then,

$$T_M^*(d) = \max_{w\in\mathcal{V}}\left\{\min_{u\in\mathcal{U}}\{T \geq 0 : (Bu+Cw)T = d\}\right\}. \quad (15)$$

Because u is chosen to counteract w and make $Bu+Cw$ collinear with $d \in \mathbb{R}^n$, while w is chosen freely in $\mathcal{W}$, the minimum of (15) cannot be restricted to the vertices of $\mathcal{U}$. We will now prove that both reach times are linear in the target distance.

Proposition 4: For any $d \in \mathbb{R}^n$ and $\lambda \geq 0$ we have $T_N^*(\lambda d) = \lambda\, T_N^*(d)$ and $T_M^*(\lambda d) = \lambda\, T_M^*(d)$.

Proof: The case $\lambda = 0$ is trivial since $T_N^*(0) = T_M^*(0) = 0$, so consider $\lambda > 0$. The nominal reach time for d is $T_N^*(d)$, so there exists $\bar{u}_d \in \bar{\mathcal{U}}$ such that $\bar{B}\bar{u}_d T_N^*(d) = d$. Then, $\bar{B}\,\bar{u}_d\,\lambda T_N^*(d) = \lambda d$. The optimality of $T_N^*(\lambda d)$ to reach λd leads to $T_N^*(\lambda d) \leq \lambda T_N^*(d)$.

Similarly, there exists $\bar{u}_{\lambda d} \in \bar{\mathcal{U}}$ such that $\bar{B}\bar{u}_{\lambda d} T_N^*(\lambda d) = \lambda d$, so $\bar{B}\,\bar{u}_{\lambda d}\,\frac{T_N^*(\lambda d)}{\lambda} = d$. The optimality of $T_N^*(d)$ to reach d yields $T_N^*(d) \leq \frac{T_N^*(\lambda d)}{\lambda}$. Thus, $\lambda T_N^*(d) \leq T_N^*(\lambda d)$.

A similar proof does not work for T_M^* because of the minimax structure of (15).

For $d \in \mathbb{R}_*^n$ and $w \in \mathcal{W}$, we define $x = Cw$ and $y^*(x,d) := \arg\min\limits_{y\in\mathcal{Y}}\{T \geq 0 : (y+x)T = d\}$. Note that $Bu^*(w)+Cw = y^*(x,d)+x$, with u^* defined in Lemma 2. Then, with T_M introduced in (24), we have $(Bu^*(w)+Cw)T_M(w,d) = d$, i.e., $y^*(x,d) = \frac{1}{T_M(w,d)}d - x$. For $\lambda > 0$, we define $\alpha(\lambda) := \frac{\lambda}{T_M(w,\lambda d)} - \frac{1}{T_M(w,d)}$, such that $y^*(x,\lambda d) - y^*(x,d) = \alpha(\lambda)d$.

The polytope $\mathcal{Y}$ in $\mathbb{R}^n$ has a finite number of faces, so we can choose $d \in \mathbb{R}_*^n$ not collinear with any face of $\mathcal{Y}$. Since $\mathcal{Y}$ is convex, the ray $\{y^*(x,d)+\alpha d : \alpha \in \mathbb{R}\}$ intersects with $\partial\mathcal{Y}$ at most twice. Since $y^*(x,d) \in \partial\mathcal{Y}$, one intersection happens at $\alpha = 0$. If there exists another intersection, it occurs for some $\alpha_0 \neq 0$. Since $y^*(x,\lambda d) \in \partial\mathcal{Y}$, we have $y^*(x,d) + \alpha(\lambda)d \in \partial\mathcal{Y}$. Then, $\alpha(\lambda) \in \{0, \alpha_0\}$ for all $\lambda > 0$.

According to Lemma 3, T_M is continuous in d, so α is continuous in λ but its codomain is finite. Therefore, α is constant and we know that $\alpha(1) = 0$. So α is null for all $\lambda > 0$, leading to $T_M(w,\lambda d) = \lambda T_M(w,d)$ for all $\lambda > 0$ and d not collinear with any face of $\partial\mathcal{Y}$. Since the dimension of each face of $\partial\mathcal{Y}$ is at most $n-1$ in $\mathbb{R}^n$ and T_M is continuous in d, the homogeneity of T_M holds on the whole of $\mathbb{R}^n$. Note that $T_M^*(d) = \max\limits_{w\in\mathcal{W}} T_M(w,d)$. Thus, $\lambda T_M^*(d) = T_M^*(\lambda d)$. ∎

Combining the results obtained for the nominal and the malfunctioning dynamics, we can now evaluate the quantitative resilience of the system.

IV. Quantitative resilience

Focusing on the loss of control over a single actuator we will simplify tremendously the computation of r_q by noting that the effects of the undesirable inputs are the strongest along the direction described by the malfunctioning actuator.

Theorem 1: If system (7) is resilient and C is a single column matrix, the ratio of reach times is maximizing along C, i.e., $\max\limits_{d\in\mathbb{R}_*^n} \frac{T_M^*(d)}{T_N^*(d)} = \max\left\{\frac{T_M^*(C)}{T_N^*(C)}, \frac{T_M^*(-C)}{T_N^*(-C)}\right\}$.

Proof: Using Proposition 4 we reduce the constraint set of (10) from $\mathbb{R}_*^n$ to $\mathbb{S}$. We use the same process that yielded (14) but we start from (11) where we split $\bar{B}$ into B and C:

$$\begin{aligned}\frac{1}{T_N^*(d)} &= \max_{\bar{u}\in\bar{\mathcal{U}}}\{\lambda : \bar{B}\bar{u} = \lambda d\}\\ &= \max_{u\in\mathcal{U},\, w\in\mathcal{W}}\{\lambda : Bu+Cw = \lambda d\}\\ &= \max_{x\in\mathcal{X},\, y\in\mathcal{Y}}\{\|y+x\| : y+x \in \mathbb{R}^+ d\}. \end{aligned} \quad (16)$$

We can now gather (14) with $d \in \mathbb{S}$ and (16) into

$$\frac{T_M^*(d)}{T_N^*(d)} = \frac{\max\limits_{x\in\mathcal{X},\, y\in\mathcal{Y}}\{\|x+y\| : x+y \in \mathbb{R}^+ d\}}{\min\limits_{x\in\mathcal{X}}\{\max\limits_{y\in\mathcal{Y}}\{\|x+y\| : x+y \in \mathbb{R}^+ d\}\}}.$$

Because C is a single column, $\dim\mathcal{X} = 1$. Then, following Proposition 2 we conclude with the Maximax Minimax Quotient Theorem of [10]. ∎

Theorem 1 is the strongest result of this work as it solves the nonlinear fractional optimization of r_q over $d \in \mathbb{S}$. Its proof is brief because all the heavy lifting is done in [10].

Since the sets $\mathcal{U}$ and $\mathcal{W}$ are not symmetric, in general $\frac{T_M^*(C)}{T_N^*(C)} \neq \frac{T_M^*(-C)}{T_N^*(-C)}$. Thus, to calculate the quantitative resilience r_q we need to evaluate $T_N^*(\pm C)$ and $T_M^*(\pm C)$, i.e., solve four optimization problems. The computation load can be halved with the following result.

Theorem 2: If system (7) is resilient and C is a single nonzero column, then $r_q = \min\{r_C^+, r_C^-\}$, with

$$r_C^+ := \frac{w^{min} + \lambda^+}{w^{max} + \lambda^+}, \quad r_C^- := \frac{w^{max} - \lambda^-}{w^{min} - \lambda^-}, \quad (17)$$

and $\lambda^\pm := \max\limits_{v\in\mathcal{U}}\{\lambda : Bv = \pm\lambda C\}$.

Proof: Let $\bar{u} \in \bar{\mathcal{U}}$, $u \in \mathcal{U}$ and $w \in \mathcal{W}$ be the arguments of the optimization problems (11) and (15) for $d = C \neq 0$. We write $\bar{u} = (u_B,\ u_C) \in \mathcal{U}\times\mathcal{W}$. Then,

$$\begin{aligned}\bar{B}\bar{u}\,T_N^*(C) = Bu_B\,T_N^*(C) + Cu_C\,T_N^*(C) = C,\\ Bu\,T_M^*(C) + Cw\,T_M^*(C) = C.\end{aligned} \quad (18)$$

We consider the loss of a single actuator, thus $\mathcal{W} = [w^{min}, w^{max}] \subseteq \mathbb{R}$ which makes $CwT_M^*(C)$ and $Cu_CT_N^*(C)$ collinear with C. From Proposition 3, we know that $w \in \partial\mathcal{W}$. Since w maximizes $T_M^*(C)$ in (18), we obviously have $w = w^{min}$. On the contrary, u_C is chosen to minimize $T_N^*(C)$ in (18), so $u_C = w^{max}$.

According to (18), Bu_B and Bu are collinear with C, and they are chosen to minimize respectively $T_N^*(C)$ and $T_M^*(C)$. Thus, u and u_B are the vectors in $\mathcal{U}$ that maximize the norm of Bu and Bu_B and make them positively collinear with C, i.e., $u = u_B = \arg\min\limits_{v\in\mathcal{U}}\{\tau : Bv\tau = C\}$. Using $\lambda = \frac{1}{\tau}$ we

render this problem linear:

$$\lambda^+ = \max_{v \in \mathcal{U}} \{\lambda : Bv = \lambda C\}$$
$$u = u_B = \arg\max_{v \in \mathcal{U}} \{\lambda : Bv = \lambda C\}.$$

By combining all the results, (18) simplifies into:

$$C(\lambda^+ + w^{max})T_N^*(C) = C,$$
$$C(\lambda^+ + w^{min})T_M^*(C) = C.$$

Since C is a nonzero column, $\frac{T_N^*(C)}{T_M^*(C)} = \frac{\lambda^+ + w^{min}}{\lambda^+ + w^{max}} = r_C^+$. Following the same reasoning for $d = -C$, we obtain

$$C(-\lambda^- + w^{min})T_N^*(C) = -C$$
$$C(-\lambda^- + w^{max})T_M^*(C) = -C,$$

with $\lambda^- = \max_{v \in \mathcal{U}} \{\lambda : Bv = -\lambda C\}$. Then, $\frac{T_N^*(-C)}{T_M^*(-C)} = \frac{w^{max} - \lambda^-}{w^{min} - \lambda^-} = r_C^-$. Following Theorem 1,

$$r_q = \min\left\{\frac{T_N^*(C)}{T_M^*(C)}, \frac{T_N^*(-C)}{T_M^*(-C)}\right\} = \min\{r_C^+, r_C^-\}.$$

■

We introduced quantitative resilience as the solution of four nonlinear nested optimization problems and with Theorem 2 we reduced r_q to the solution of two linear optimization problem. We can thus quickly calculate the maximal delay caused by the loss of control of a given actuator.

V. Resilience conditions

So far, all our results need the system to be resilient. However, we know that verifying the resilience of a system with inputs of finite energy is not an easy task [7], and thus we can assume it is not trivial either with our component bounded inputs.

Proposition 5: A system following (6) is resilient to the loss of control over a column C if and only if it is controllable and both $T_M^*(C)$ and $T_M^*(-C)$ are finite.

Proof: If system (6) is resilient, then it is controllable a fortiori and Proposition 1 yields $T_M^*(C)$ and $T_M^*(-C)$ are finite.

On the other hand, assume that system (6) is controllable and $\max\{T_M^*(C), T_M^*(-C)\}$ is finite. Let $w \in \mathcal{W}$ and $d \in \mathbb{R}_*^n$. By controllability of system (6), there exists $\bar{u} \in \bar{\mathcal{U}}$ and $\lambda > 0$ such that $\bar{B}\bar{u} = \lambda d$. We split $\bar{B}$ into B and C, and $\bar{u}$ into u_d and w_d. Then, $u_d \in \mathcal{U}$ and $\bar{B}\bar{u} = Bu_d + Cw_d = \lambda d$. In the case $C = 0$, this equation yields $Bu_d = \lambda d = Bu_d + Cw$, so the system is resilient.

For $C \neq 0$, we will first show that for any $w \in \mathcal{W}$ we can find $u \in \mathcal{U}$ such that $Bu + Cw = 0$. Because $T_M^*(C)$ and $T_M^*(-C)$ are finite, $T_M(w, \pm C)$ is positive and finite for all $w \in \mathcal{W} = [w^{min}, w^{max}]$, with $T_M(\cdot,\cdot)$ defined in (24). Take $w \in \mathcal{W}$. Then, there exist $u_+^w \in \mathcal{U}$ and $u_-^w \in \mathcal{U}$ such that $(Bu_+^w + Cw)T_M(w, C) = C$ and $(Bu_-^w + Cw)T_M(w, -C) = -C$. Define $\alpha := \frac{T_M(w,C)}{T_M(w,C) + T_M(w,-C)} \in (0,1)$ and $u := \alpha u_+^w + (1-\alpha)u_-^w$. Then, $u \in \mathcal{U}$ because $\mathcal{U}$ is convex. Notice that

$$\begin{aligned} Bu + Cw &= \alpha(Bu_+^w + Cw) + (1-\alpha)(Bu_-^w + Cw) \\ &= \frac{T_M(w,C)}{T_M(w,C) + T_M(w,-C)} \frac{C}{T_M(w,C)} \\ &\quad + \frac{T_M(w,-C)}{T_M(w,C) + T_M(w,-C)} \frac{-C}{T_M(w,-C)} = 0. \end{aligned}$$

We want to make a convex combination of u and u_d to build the desired control. If $w \in \partial\mathcal{W}$ the resulting control will not be stronger than the adversary. So, we need to show that even if w is a little bit outside of $\mathcal{W}$ we can still counteract it. Let $\varepsilon := \min\left(\frac{1}{2T_M(w^{min},C)}, \frac{1}{2T_M(w^{max},-C)}\right) > 0$. Now take $w' \in (w^{max}, w^{max} + \varepsilon]$. There exists $u_- \in \mathcal{U}$ and $u_+ \in \mathcal{U}$ such that $(Bu_+ + Cw^{max})T_M(w^{max}, C) = C$ and $(Bu_- + Cw^{max})T_M(w^{max}, -C) = -C$. Then, we can define $T^+ > 0$ such that

$$\begin{aligned} Bu_+ + Cw' &= Bu_+ + Cw^{max} + C(w' - w^{max}) \\ &= C\left(\frac{1}{T_M(w^{max}, C)} + w' - w^{max}\right) = \frac{C}{T^+}. \end{aligned}$$

Since $w' - w^{max} \leq 1/2T_M(w^{max}, -C)$, we can similarly define $T^- > 0$ such that

$$Bu_- + Cw' = -C\left(\frac{1}{T_M(w^{max}, -C)} - (w' - w^{max})\right) = \frac{-C}{T^-}.$$

We take $\alpha = \frac{T^+}{T^+ + T^-} \in (0,1)$ which yields $u' = \alpha u_+ + (1-\alpha)u_- \in \mathcal{U}$ by convexity. Then, $Bu' + Cw' = 0$. With a similar approach we can build another u' to counteract any $w' \in [w^{min} - \varepsilon, w^{min})$.

Since $\mathcal{W}$ is convex, $w \in \mathcal{W}$ and $w_d \in \mathcal{W}$, we can take $w' \in [w^{min} - \varepsilon, w^{max} + \varepsilon]$ such that there exists $\gamma \in (0,1)$ for which $w = \gamma w_d + (1-\gamma)w'$. We build $u' \in \mathcal{U}$ as above to make $Bu' + Cw' = 0$. By convexity of $\mathcal{U}$, $u := \gamma u_d + (1-\gamma)u' \in \mathcal{U}$. Then,

$$Bu + Cw = \gamma(Bu_d + Cw_d) + (1-\gamma)(Bu' + Cw') = \gamma\lambda d.$$

Since $\gamma > 0$, we have $\gamma\lambda > 0$ making the system resilient to the loss of column C. ■

The intuition behind Proposition 5 is that a resilient system has two properties: the ability to reach any state prior to a malfunction, i.e., controllability, and the ability to do so after the malfunction despite the worst undesirable inputs, i.e., $T_M^*(\pm C)$ is finite. We can now derive resilience from a computation, making it easier to verify.

Corollary 1: System (6) is resilient to the loss of control over a nonzero column C if and only if it is controllable, and r_C^+ and r_C^- from Theorem 2 are in $(0, 1]$.

Proof: If $C = 0$, the controllability is equivalent to resilience and $r_C^+ = r_C^- = 1$. If $C \neq 0$ and system (6) is resilient, then by Proposition 5, both $T_M^*(\pm C)$ are finite and system (6) is controllable, so both $T_N^*(\pm C)$ are finite too. Trivially $T_N^* \leq T_M^*$, so we have both $r_C^+ = \frac{T_N^*(C)}{T_M^*(C)} \in (0,1]$ and $r_C^- = \frac{T_N^*(-C)}{T_M^*(-C)} \in (0,1]$ according to Theorem 2.

On the other hand, assume that the system is controllable and that $\frac{w^{min} + \lambda^+}{w^{max} + \lambda^+}$ and $\frac{w^{max} - \lambda^-}{w^{min} - \lambda^-} \in (0,1]$. If $w^{min} + \lambda^+ < 0$, then $w^{max} + \lambda^+ \leq w^{min} + \lambda^+$ because $r_C^+ \in (0,1]$. This

leads to the impossible conclusion that $w^{max} \leq w^{min}$. If $w^{min} + \lambda^+ = 0$, then $r_C^+ = 0$. Therefore, $w^{min} + \lambda^+ > 0$. Let $u \in \mathcal{U}$ such that $Bu = \lambda^+ C$. For $w \in \mathcal{W}$, we define $T_w := \frac{1}{w+\lambda^+}$, so that $(Bu + Cw)T_w = C$. Note that T_w is positive and finite because $w + \lambda^+ \geq w^{min} + \lambda^+ > 0$. Since $T_M^*(C) \leq \max_{w \in \mathcal{W}} T_w = \frac{1}{w^{min}+\lambda^+}$, $T_M^*(C)$ is finite.

The same reasoning holds for r_C^-. We can show that $w^{max} - \lambda^- < 0$ and that $T_w := \frac{1}{\lambda^- - w} > 0$ for all $w \in \mathcal{W}$. With $u \in \mathcal{U}$ such that $Bu = -\lambda^- C$ we have $(Bu + Cw)T_w = -C$. Then, $T_M^*(-C) \leq \max_{w \in \mathcal{W}} T_w = \frac{1}{\lambda^- - w^{max}}$, so $T_M^*(-C)$ is finite. Then, Proposition 5 states that the system is resilient. ∎

We now have all the tools to assess the quantitative resilience of system (6). We summarize the main steps of this process in Algorithm 1.

Algorithm 1: Resilience algorithm for system (6)

Data: A column C of $\bar{B}$, r_C^+ and r_C^- from (17)
if $\operatorname{rank}(\bar{B}) = n$ *and* $0 \in \operatorname{int}(\bar{\mathcal{U}})$ **then**
  if $r_C^+ \in (0, 1]$ *and* $r_C^- \in (0, 1]$ **then**
    $r_q = \min\{r_C^+, r_C^-\}$ `# resilient to loss of` C
  else
    $r_q = 0$ `# not resilient to loss of` C
  end
else
  $r_q = 0$ `# not resilient to any loss`
end

VI. Systems with multiple integrators

We can now extend the results obtained for driftless systems to generalized higher-order integrators.

Proposition 6: If system (6) is controllable, then the infimum of (3) is achieved with the same constant control input $\bar{u}^* \in \bar{\mathcal{U}}$ as T_N^* in (8), and $T_{k,N}^*(d) = \sqrt[k]{k!\ T_N^*(d)}$ for all $d \in \mathbb{R}^n$.

Proof: If $d = 0$, then $T_{k,N}^*(d) = 0 = T_N^*(d)$, so the result holds. Let $d \neq 0$. By assumption, system $\dot{y}(t) = \bar{B}\bar{u}(t)$ with $y(0) = 0$ is controllable. Following Lemma 1 there exists a constant optimal control $\bar{u} \in \bar{\mathcal{U}}$ such that $y\big(T_N^*(d)\big) - y(0) = d = \bar{B}\bar{u}T_N^*(d)$, with $T_N^*(d) > 0$. Then, applying the control input $\bar{u}$ to (1) on the time interval $[0,\ t_1]$ leads to

$$x(t_1) - x_0 = \int_0^{t_1}\int_0^{t_2}\dots\int_0^{t_k} x^{(k)}(t_{k+1})\,dt_{k+1}\dots dt_2$$
$$= \int_0^{t_1}\int_0^{t_2}\dots\int_0^{t_k} \bar{B}\bar{u}\,dt_{k+1}\dots dt_2 = \bar{B}\bar{u}\frac{t_1^k}{k!} = \frac{d}{T_N^*(d)}\frac{t_1^k}{k!},$$

since $x^{(l)}(0) = 0$ for $l \in [\![1, k-1]\!]$ and $\bar{B}\bar{u} = \frac{d}{T_N^*(d)} \in \mathbb{R}^n$ is constant. By taking $t_1 = \sqrt[k]{k!\ T_N^*(d)}$, we obtain $x(t_1) - x_0 = d$. Thus, the state x_{goal} is reachable in finite time t_1, so the system (1) is controllable and $T_{k,N}^*(d) \leq t_1$.

Assume for contradiction purposes that there exists $\tilde{u} \in \bar{\mathcal{U}}$ such that the state of (1) can reach x_{goal} in a time $\tau < t_1$. Since $\tilde{u}$ can be time-varying, we build $\hat{u} := \frac{k!}{\tau^k}\int_0^\tau \dots \int_0^{t_k} \tilde{u}(t_{k+1})\,dt_{k+1}\dots dt_2$. Since $\tilde{u} \in \bar{\mathcal{U}}$, $\tilde{u}_i(t) \in [\bar{u}_i^{min}, \bar{u}_i^{max}]$ for all $i \in [\![1, m+p]\!]$ and $t \in [0, \tau]$. Because $\bar{u}_i^{min}$ and $\bar{u}_i^{max}$ are constant, one can easily obtain through k successive integrations that $\hat{u}_i \in [\bar{u}_i^{min}, \bar{u}_i^{max}]$ for all $i \in [\![1, m+p]\!]$. Thus, $\hat{u}$ is an admissible constant control input. Then, we apply $\tilde{u}$ to (1) on the time interval $[0, \tau]$ and we obtain

$$x(\tau) - x_0 = d = \int_0^\tau \dots \int_0^{t_k} \bar{B}\tilde{u}(t_{k+1})\,dt_{k+1}\dots dt_2 = \bar{B}\hat{u}\frac{\tau^k}{k!},$$

so $\bar{B}\hat{u} = \frac{k!d}{\tau^k}$. Applying the control input $\hat{u}$ to the system $\dot{y}(t) = \bar{B}\bar{u}(t)$ on the interval $[0, T]$ with $T := \frac{\tau^k}{k!}$ leads to

$$y(T) = \int_0^T \dot{y}(t)\,dt = \int_0^T \bar{B}\hat{u}\,dt = \bar{B}\hat{u}T = \frac{k!d}{\tau^k}\frac{\tau^k}{k!} = d.$$

Thus, y can reach d in a time $T = \frac{\tau^k}{k!} < \frac{t_1^k}{k!} = T_N^*(d)$, which contradicts the optimality of $T_N^*(d)$. In other words, t_1 is the minimal time for the state of (1) to reach x_{goal}. Therefore, the infimum of (3) is achieved with the same constant input $\bar{u} \in \bar{\mathcal{U}}$ as $T_N^*(d)$ in (8), and $T_{k,N}^*(d) = \sqrt[k]{k!\ T_N^*(d)}$. ∎

A result similar to Proposition 6 holds for the malfunctioning reach time of order k.

Proposition 7: If system (7) is resilient, then system (2) is resilient for all $k \in \mathbb{N}$. The supremum and infimum of (4) are achieved with the same constant inputs $u^* \in \mathcal{U}$ and $w^* \in \mathcal{W}$ as T_M^* in (9), and $T_{k,M}^*(d) = \sqrt[k]{k!\ T_M^*(d)}$ for $d \in \mathbb{R}^n$.

Proof: We use the same calculations as in Proposition 6 but with $Bu^*(w) + Cw$ instead of $\bar{B}\bar{u}$ and $T_M(w, d)$ instead of $T_N^*(d)$. Then, u^* from Lemma 2 produces the best control input $u^*(w)$ for any $w \in \mathcal{W}$ for system (2).

We go again through the proof of Proposition 6, but this time we use $Bu^*(w^*) + Cw^*$ and $T_M^*(d)$. We conclude that $T_{k,M}^*(d) = \sqrt[k]{k!\ T_M^*(d)}$ and that w^* from Proposition 1 is also the worst undesirable input for system (2). ∎

We can now evaluate the quantitative resilience of order k.

Theorem 3: If system (6) is resilient, then for all $k \in \mathbb{N}$ system (1) is resilient and $r_{k,q} = \sqrt[k]{r_q}$.

Proof: Based on Propositions 6 and 7, $\frac{T_{k,M}^*(d)}{T_{k,N}^*(d)} = \frac{\sqrt[k]{k!\ T_M^*(d)}}{\sqrt[k]{k!\ T_N^*(d)}} = \sqrt[k]{\frac{T_M^*(d)}{T_N^*(d)}}$, so $r_{k,q} = \sqrt[k]{r_q}$. ∎

For a resilient system $r_q \in (0, 1]$, then $r_{k,q} \geq r_q$. Thus, adding integrators to a resilient system increases its quantitative resilience. By studying $\dot{x}(t) = \bar{B}\bar{u}(t)$ we can then calculate the quantitative resilience of any system of the form $x^{(k)}(t) = \bar{B}\bar{u}(t)$ for $k \in \mathbb{N}$. We will now apply our theory to a numerical example.

VII. Resilience of an octocopter

Resilience of unmanned aerial vehicles (UAV) to propeller failure is crucial to their operations over populated areas [22]. Because quadcopters have 4 inputs for 6 degrees of freedom, they are underactuated and thus cannot be resilient to the loss of control authority over one of their propellers [22]. Instead, we consider the octocopter from [23] represented on Fig. 1. Its design decouples the rotational and the translational dynamics, allowing to keep a payload horizontal, which is crucial for pizza delivery for instance.

In Sections VII-A and VII-B, we will first quantify the resilience of this UAV model to the loss of control over one of its propellers. Since propellers cannot operate in a bang-bang fashion, we will then add propellers' dynamics to the UAV model in Section VII-C. Because of this modification the UAV dynamics are not driftless. Hence, most of our theory does not apply but still provides good intuition on the quantitative resilience of this octocopter model.

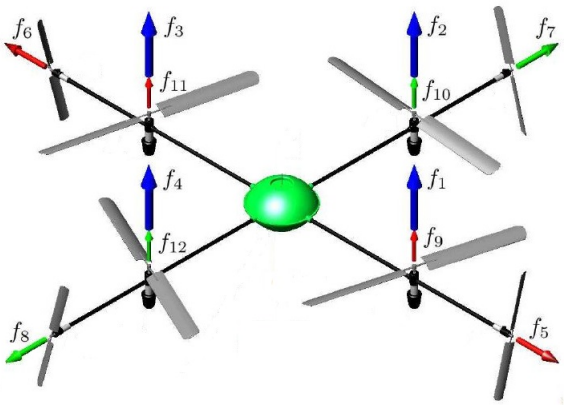

Fig. 1. Octocopter layout, image modified from [23].

A. Rotational dynamics

The roll, pitch and yaw angles of the octocopter are gathered in $Y := (\phi, \theta, \psi)$. The propeller $i \in [\![1, 8]\!]$ spinning at an angular velocity ω_i produces a force $f_i = k\omega_i^2$, with the thrust coefficient $k = 10^{-5}\, N \cdot s^{-2}$. The airflow created by the lateral rotors produces the extra vertical forces $f_9, \dots, f_{12}$ on Fig. 1. From [23], $f_{9+i} = bf_{5+i}$ for $i \in [\![0, 3]\!]$ with the coupling constant $b = 0.64$. The rotational equations are linearized around $\dot{Y} = 0$ and become $\ddot{Y} = \bar{B}_r \Omega$, with $\Omega \in \mathbb{R}^8$ gathering the squared angular velocities of the propellers $\omega_1^2, \dots, \omega_8^2$ and

$$\bar{B}_r = \begin{bmatrix} \frac{lk}{I_x} & 0 & 0 \\ 0 & \frac{lk}{I_y} & 0 \\ 0 & 0 & \frac{d}{I_z} \end{bmatrix} \begin{bmatrix} -1 & 0 & 1 & 0 & 0 & 0 & b & -b \\ 0 & 1 & 0 & -1 & b & -b & 0 & 0 \\ -1 & 1 & -1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix},$$

with an arm length $l = 40\, cm$, drag coefficient $d = 3 \times 10^{-7}\, m \cdot s^2$, inertias $I_x = I_y = \frac{1}{2} I_z = 44 \times 10^{-3}\, kg \cdot m^2$, mass $m = 1.64\, kg$ and maximal angular velocity $\omega_{max} = 838\, rad \cdot s^{-1}$ [15]. Since the input sets are nonsymmetric: $\bar{u}_i := \omega_i^2 \in [0, \omega_{max}^2]$, and the dynamics are given by a double integrator, the theory of [8] cannot deal with this UAV model. Using Theorem 2 we calculate the quantitative resilience of the system $\dot{v}_Y(t) = \bar{B}_r \bar{u}(t)$ with $v_Y := \dot{Y}$ for the loss of control over each single propeller: $r_{min} = \begin{bmatrix} 0.1 & 0.1 & 0.1 & 0.1 & 0.1 & 0.1 & 0.1 & 0.1 \end{bmatrix}$. Based on Corollary 1, the UAV is thus resilient to the loss of control over any single propeller in terms of angular velocity and $r_q = \min\{r_C^{\pm}\}$. Following Theorem 3 we deduce that $\ddot{Y}(t) = \bar{B}_r \bar{u}(t)$ is also resilient and $r_{2,q} = \sqrt{r_q} = \sqrt{0.1} = 0.32$. Then, $\frac{1}{r_{2,q}} = 3$ and $\frac{1}{r_q} = 10$ mean that after the loss of control over any single propeller the UAV might take as much as three times longer to reach a given orientation, while it might be ten times slower to reach a given angular velocity.

B. Translational dynamics

Since the rotational dynamics are resilient, we know that the controller can maintain the UAV horizontal even after the loss of control over a propeller. From now on, we will then assume $\theta = \phi = 0°$. To prevent obfuscating the following analysis, we assume that this orientation is maintained no matter the inputs u and w. Additionally, the yaw angle does not affect the translational dynamics, so we also take $\psi = 0°$. Then, the translational dynamics of the octocopter are equivalent to that of a point-mass model and they are fully decoupled from the rotational dynamics, as desired by design [23]. The position of the UAV is $X := (x, y, z)$ and satisfies

$$m\ddot{X} = \begin{bmatrix} k(\omega_5^2 - \omega_6^2) \\ k(\omega_7^2 - \omega_8^2) \\ k\sum_{i=1}^4 \omega_i^2 + bk\sum_{i=5}^8 \omega_i^2 - mg \end{bmatrix}.$$

The horizontal propellers $(\omega_1, \dots, \omega_4)$ are designed to sustain the weight of the drone while the lateral ones $(\omega_5, \dots, \omega_8)$ are smaller and should mostly be used for lateral displacements. Thus, we define the inputs $\bar{u}_i := k\omega_i^2 - \frac{mg}{4} \in [-\frac{mg}{4}, k\omega_{max}^2 - \frac{mg}{4}]$ for $i \in [\![1, 4]\!]$ and $\bar{u}_i := k\omega_i^2 \in [0, k\omega_{max}^2]$ for $i \in [\![5, 8]\!]$. Then, the translational dynamics become

$$\ddot{X}(t) = \bar{B}_t \bar{u}(t), \quad \dot{X}(0) = X(0) = 0 \in \mathbb{R}^3, \tag{19}$$

with $\bar{B}_t = \frac{1}{m} \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 1 & 1 & 1 & 1 & b & b & b & b \end{bmatrix}$.

After the loss of control authority over a propeller, we split $\bar{B}_t$ and $\bar{u}$ into B, C and u, w as before. The initial state is the same and the malfunctioning dynamics are

$$\ddot{X}(t) = Bu(t) + Cw(t). \tag{20}$$

For system $\dot{v} = \bar{B}_t \bar{u}$, with $v := \dot{X}$, Theorem 2 yields

$$r_C^+ = \begin{bmatrix} 0.766 & 0.766 & 0.766 & 0.766 & 0 & 0 & 0 & 0 \end{bmatrix},$$
$$r_C^- = \begin{bmatrix} 0.564 & 0.564 & 0.564 & 0.564 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Then, according to Corollary 1 the system of dynamics $\dot{v} = \bar{B}_t \bar{u}$ is only resilient to the loss of any one of the first four propellers. Following Theorem 2, $r_q = \min\{r_C^+, r_C^-\} = \begin{bmatrix} 0.564 & 0.564 & 0.564 & 0.564 & 0 & 0 & 0 & 0 \end{bmatrix}$. Since Theorem 3 only applies to resilient systems, we use it on the first four propellers $r_{2,q} = \sqrt{r_q} = \begin{bmatrix} 0.75 & 0.75 & 0.75 & 0.75 \end{bmatrix}$. Then, $\frac{1}{r_q} = 1.77$ and $\frac{1}{r_{2,q}} = 1.33$ mean that the after the loss of a horizontal propeller, the UAV might need 1.77 times longer to reach a given velocity but only 1.33 times longer to reach a desired position.

Let us now evaluate how the loss of a propeller impacts the vertical velocity. We take $d = (0, 0, -1)$ and compute

$$\frac{T_M^*(d)}{T_N^*(d)} = \begin{bmatrix} 1.77 & 1.77 & 1.77 & 1.77 & 2.26 & 2.26 & 2.26 & 2.26 \end{bmatrix}. \tag{21}$$

The first four values are the same as $1/r_q$ because the direction the worst impacted by the loss of a horizontal propeller is along d. We now simulate various loss of controls and aim to fly vertically the UAV along $d = (0, 0, -1)$.

As illustrated on Fig. 2, to reach the velocity $v = (0, 0, -1)$,

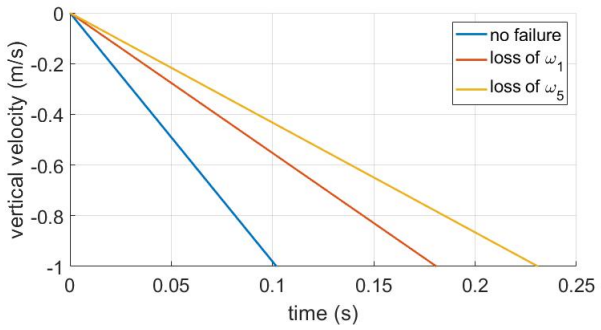

Fig. 2. Time evolution of $\dot{\boldsymbol{z}}$. For 'no failure', $\dot{\boldsymbol{v}} = \bar{\boldsymbol{B}}_{\boldsymbol{t}}\bar{\boldsymbol{u}}^{\boldsymbol{min}}$. For 'loss of $\boldsymbol{\omega_1}$', $\dot{\boldsymbol{v}} = \boldsymbol{Bu} + \boldsymbol{Cw}$ with $\boldsymbol{C}$ the $\boldsymbol{1}^{\boldsymbol{st}}$ column of $\bar{\boldsymbol{B}}_{\boldsymbol{t}}$, $\boldsymbol{w} = \boldsymbol{k\omega}_{\boldsymbol{max}}^{\boldsymbol{2}} - \boldsymbol{mg}/\boldsymbol{4}$ and $\boldsymbol{u} = \boldsymbol{u}^{\boldsymbol{min}}$. For 'loss of $\boldsymbol{\omega_5}$', $\dot{\boldsymbol{v}} = \boldsymbol{Bu}+\boldsymbol{Cw}$ with $\boldsymbol{C}$ the $\boldsymbol{5}^{\boldsymbol{th}}$ column of $\bar{\boldsymbol{B}}_{\boldsymbol{t}}$, $\boldsymbol{w} = \boldsymbol{k\omega}_{\boldsymbol{max}}^{\boldsymbol{2}}$ and $\boldsymbol{u} = \boldsymbol{u}^{\boldsymbol{min}}$ except $\bar{\boldsymbol{u}}_{\boldsymbol{6}} = \boldsymbol{k\omega}_{\boldsymbol{max}}^{\boldsymbol{2}}$ to keep the UAV on the $\boldsymbol{z}$-axis.

the nominal system needs $0.102\,s$, while the malfunctioning ones need $0.181\,s$ and $0.231\,s$ after the loss of ω_1 and ω_5 respectively. Then, the reach times increased by factors 1.77 and 2.26, exactly the values calculated in (21) as the choice of inputs in the simulation is optimal.

We now study $T_N^*(d)$ and $T_M^*(d)$ for the velocity targets $d(\beta) = (0, \cos\beta, \sin\beta)$ for all $\beta \in [0, 2\pi]$. After the loss of ω_1, $\frac{1}{r_q} = 1.77$, so $T_M^*(d) \leq 1.77\ T_N^*(d)$ for any $d \in \mathbb{R}^n$, as illustrated on Fig. 3.

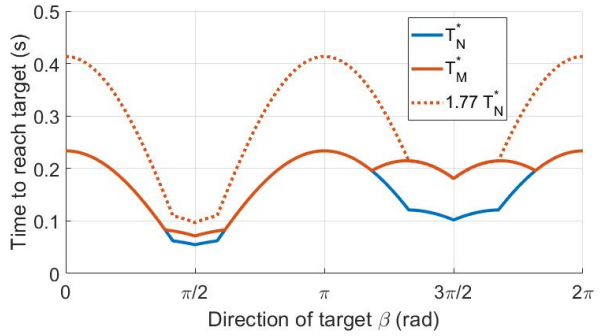

Fig. 3. Evolution of $\boldsymbol{T_N^*(d)}$ and $\boldsymbol{T_M^*(d)}$ for a velocity target $\boldsymbol{d(\beta) = (0, \cos\beta, \sin\beta)}$.

Note that $d(\frac{3\pi}{2}) = (0, 0, -1)$ and as calculated in (21) we have $T_M^*(d(\frac{3\pi}{2})) = 1.77\ T_N^*(d(\frac{3\pi}{2}))$ as shown on Fig. 3. The lack of input symmetry results in $T_M^*(\beta) \neq T_M^*(\beta + \pi)$ as shown on Fig. 3. Such a situation could not be handled by the preliminary work [8].

C. High-fidelity dynamics of the propellers

So far in this work, all inputs were bang-bang because our definition of quantitative resilience asks for time-optimal transfers. The inputs of the translational dynamics (19) encode the propellers' angular velocities, which cannot physically change in a bang-bang fashion. Thus, in order to provide a more realistic model and display the capabilities of our work, we follow [24] and add first-order propellers' dynamics:

$$\ddot{X}(t) = \bar{B}_t\bar{u}(t), \quad \dot{\bar{u}}(t) = \frac{1}{\tau}\big(\bar{u}^c(t) - \bar{u}(t)\big), \tag{22}$$

with $\bar{u}^c \in \mathbb{R}^8$ a new, possibly bang-bang, command signal. System (22) is not driftless, hence preventing a direct application of our theory. Instead, we proceed heuristically, building on the intuition provided by our theory to tackle this high-fidelity model.

The time constant $\tau = 0.1\ s$ is chosen to match the propeller response in Fig. 3 of [25]. After the loss of control over the first propeller, we split $\bar{B}_t$ and $\bar{u}$ as before such that

$$\ddot{X}(t) = Bu(t)+Cw(t), \quad \begin{cases} \dot{u}(t) = \frac{1}{\tau}\big(u^c(t) - u(t)\big), \\ \dot{w}(t) = \frac{1}{\tau}\big(w^c(t) - w(t)\big), \end{cases} \tag{23}$$

with the bang-bang command signals u^c and w^c. We will now study how the actuators' dynamics impact the resilience of the UAV in the vertical direction $d = (0, 0, 1)$.

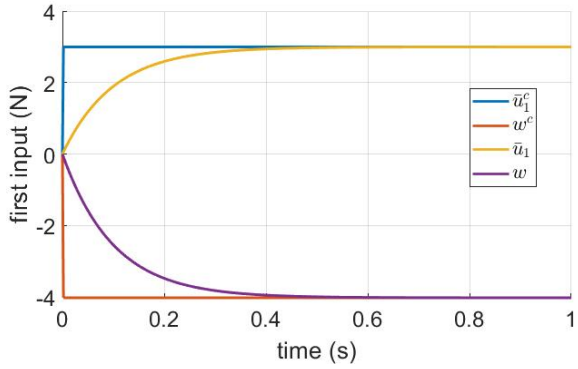

Fig. 4. Exponential convergence of $\bar{\boldsymbol{u}}_{\boldsymbol{1}}$ and $\boldsymbol{w}$ to their bang-bang commands $\bar{\boldsymbol{u}}_{\boldsymbol{1}}^{\boldsymbol{c}} = \bar{\boldsymbol{u}}_{\boldsymbol{1}}^{\boldsymbol{max}} = \boldsymbol{k\omega}_{\boldsymbol{max}}^{\boldsymbol{2}} - \frac{\boldsymbol{mg}}{\boldsymbol{4}}$ and $\boldsymbol{w^c} = \bar{\boldsymbol{u}}_{\boldsymbol{1}}^{\boldsymbol{min}} = -\frac{\boldsymbol{mg}}{\boldsymbol{4}}$.

Since the inputs $\bar{u}$ in (22) and (u, w) in (23) have a non-zero rise time as shown on Fig. 4, the vertical velocities $\dot{z}_N$ of (22) and $\dot{z}_M$ of (23) react smoothly and slower than their bang-bang counterparts, as illustrated on Fig. 5. For $t \geq 0.4\,s$, $\bar{u}$ and (u, w) have converged to their commands $\bar{u}^c$ and (u^c, w^c), and thus the two slopes of $\dot{z}_N(t)$ in (19) and (22) are equal, as shown on Fig. 5, and so are that of $\dot{z}_M(t)$ in (20) and (23).

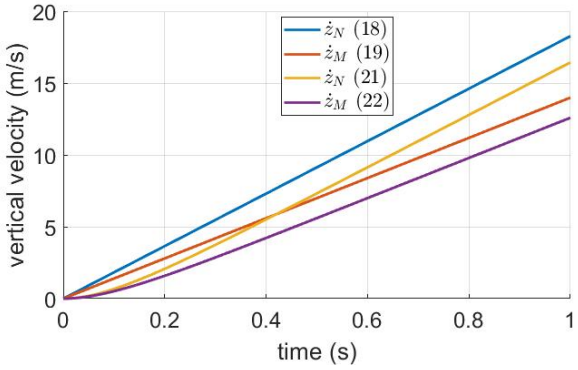

Fig. 5. Vertical velocities $\dot{\boldsymbol{z}}_{\boldsymbol{N}}\boldsymbol{(t)}$ and $\dot{\boldsymbol{z}}_{\boldsymbol{M}}\boldsymbol{(t)}$ of the nominal and malfunctioning systems demonstrating the impact of the propellers' dynamics in (22) and (23).

The slower reaction time caused by the dynamics of the propellers is also reflected on the vertical positions z_N and z_M on Fig. 6.

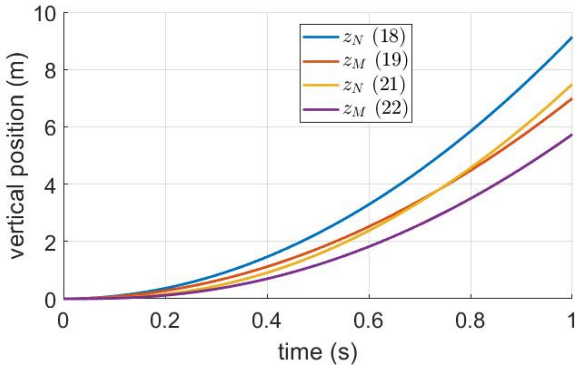

Fig. 6. Vertical positions $\boldsymbol{z_N(t)}$ and $\boldsymbol{z_M(t)}$ of the nominal and malfunctioning systems demonstrating the impact of the propellers' dynamics in (22) and (23).

Because of the specific geometry of the system, the optimal inputs for direction $d = (0, 0, 1)$ were trivial to determine. Then, we calculate the ratio of reach times for systems (22) and (23), $\frac{T^*_M(d)}{T^*_N(d)} = 1.12$ and for systems (19) and (20), $\frac{T^{c*}_M(d)}{T^{c*}_N(d)} = 1.14$. Hence, modeling the dynamics of the propellers increases slightly the resilience of the vertical dynamics.

However, the time-optimal commands $\bar{u}^c$ for (22) and (u^c, w^c) for (23) can be time-varying for other directions $d \in \mathbb{R}^3$ [11], and determining these optimal commands requires complex algorithms [17], [26] because the dynamics are not driftless anymore. Additionally, the Maximax-Minimax Quotient Theorem of [10] does not hold, which invalidates Theorem 1 and prevents the exact calculation of r_q without calculating $\frac{T^*_M(d)}{T^*_N(d)}$ for all $d \in \mathbb{R}^3$. A stronger theory will be needed to tackle linear non-driftless systems.

VIII. Conclusion and Future Work

This paper introduced the notion of quantitative resilience for linear systems with multiple integrators and nonsymmetric input sets. Relying on bang-bang control theory and on two specific optimization results, we transformed a nonlinear problem consisting of four nested optimizations into a single linear optimization. This simplification leads to a computationally efficient method for verifying the resilience and calculating the quantitative resilience of driftless systems with multiple integrators.

There are three promising avenues of future work. First, we want to extend Theorems 1 and 2 to the simultaneous loss of multiple actuators. Secondly, we aim at developing the theory of quantitative resilience for non-driftless linear systems. Finally, we want to extend our notion of resilience from the system's state to its output. This would allow, for instance, to assess the resilience of a drone with respect to its position, pitch, and roll angles, while disregarding its yaw angle as in [22].

Appendix I
Supporting Lemmata

Lemma 1: If system (6) is controllable, then for all $d = x_{goal} - x_0 \in \mathbb{R}^n$, the infimum $T^*_N(d)$ of (8) is a minimum achieved by a constant control input $\bar{u}^* \in \bar{\mathcal{U}}$.

Proof: According to Theorem 4.3 of [11] there exists a time optimal control $\bar{u}^* \in \mathcal{F}(\bar{\mathcal{U}})$. Following Pontryagin maximum principle [11], $\bar{u}^*$ is bang-bang but does not switch since the dynamics are driftless. Thus, the infimum T^*_N in (8) is a minimum achieved by a constant control input. ■

Lemma 2: If system (7) is resilient, then for all $d \in \mathbb{R}^n_*$ and all $w \in \mathcal{F}(\mathcal{W})$, the infimum $T_M(w, d)$ of (9) is a minimum achieved by a constant control input $u^*(w) \in \mathcal{U}$ and

$$T_M(w,d) := \min_{u \in \mathcal{U}} \left\{ T \geq 0 : \int_0^T \big[Bu(t) + Cw(t)\big]\, dt = d \right\}. \quad (24)$$

Proof: The infimum of (9) is $T_M(w, d) = \inf_{u \in \mathcal{F}(\mathcal{U})} \big\{T \geq 0 : \int_0^T Bu(t)\, dt = z\big\}$, with $z := d - \int_0^T Cw(t)\, dt \in \mathbb{R}^n$ a constant vector for w fixed. Since system (7) is resilient, any $z \in \mathbb{R}^n$ is reachable. Following Lemma 1 and Theorem 4.3 of [11], a constant time-optimal control exists and the infimum of (9) is a minimum. ■

Lemma 3: For a resilient system following (7), function $T_M(w, d) := \min_{u \in \mathcal{U}} \big\{T \geq 0 : (Bu + Cw)T = d\big\}$ is continuous in $w \in \mathcal{W}$ and $d \in \mathbb{R}^n_*$.

Proof: With $\mathcal{X} := \big\{Cw : w \in \mathcal{W}\big\}$, $\mathcal{Y} := \big\{Bu : u \in \mathcal{U}\big\}$ and $\lambda = 1/T$ we obtain $T_M(x, d) = 1/\max_{y \in \mathcal{Y}} \big\{\lambda \geq 0 : x + y = \lambda d\big\}$. Since $\|d\| > 0$ and $\lambda \geq 0$, we have $\lambda = \|\lambda d\|/\|d\| = \|x+y\|/\|d\|$. Let $d_1 := d/\|d\|$, then $T_M(x, d) = \|d\|/\max_{y \in \mathcal{Y}} \big\{\|x + y\| : x + y \in \mathbb{R}^+ d_1\big\}$ and Lemma 5.2 of [10] states that T_M is continuous in w and d. ■

References

[1] B. Xiao, Q. Hu, and P. Shi, "Attitude stabilization of spacecrafts under actuator saturation and partial loss of control effectiveness," *IEEE Transactions on Control Systems Technology*, vol. 21, no. 6, pp. 2251 – 2263, 2013.

[2] G. Tao, S. Chen, and S. M. Joshi, "An adaptive actuator failure compensation controller using output feedback," *IEEE Transactions on Automatic Control*, vol. 47, no. 3, pp. 506 – 511, 2002.

[3] Y. Yu, H. Wang, and N. Li, "Fault-tolerant control for over-actuated hypersonic reentry vehicle subject to multiple disturbances and actuator faults," *Aerospace Science and Technology*, vol. 87, pp. 230 – 243, 2019.

[4] M. Bartels, "Russia says 'software failure' caused thruster misfire at space station," *space.com*, 2021, https://www.space.com/space-station-nauka-arrival-thruster-fire-update.

[5] J.-B. Bouvier and M. Ornik, "Resilient reachability for linear systems," in *21st IFAC World Congress*, 2020, pp. 4409 – 4414.

[6] L. Y. Wang and J.-F. Zhang, "Fundamental limitations and differences of robust and adaptive control," in *2001 American Control Conference*, 2001, pp. 4802 – 4807.

[7] J.-B. Bouvier and M. Ornik, "Designing resilient linear systems," *IEEE Transactions on Automatic Control*, vol. 67, no. 9, pp. 4832 – 4837, 2022.

[8] J.-B. Bouvier, K. Xu, and M. Ornik, "Quantitative resilience of linear driftless systems," in *SIAM Conference on Control and Its Applications*, 2021, pp. 32 – 39.

[9] J. T. Kim, J. Park, J. Kim, and P. H. Seong, "Development of a quantitative resilience model for nuclear power plants," *Annals of Nuclear Energy*, vol. 122, pp. 175 – 184, 2018.

[10] J.-B. Bouvier and M. Ornik, "The maximax minimax quotient theorem," *Journal of Optimization Theory and Applications*, vol. 192, pp. 1084 – 1101, 2022.

[11] D. Liberzon, *Calculus of Variations and Optimal Control Theory: a Concise Introduction*. Princeton University Press, 2011.

[12] L. W. Neustadt, "The existence of optimal controls in the absence of convexity conditions," *Journal of Mathematical Analysis and Applications*, vol. 7, pp. 110 – 117, 1963.

[13] J. LaSalle, "Time optimal control systems," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 45, no. 4, pp. 573 – 577, 1959.
[14] H. J. Sussmann, "A bang-bang theorem with bounds on the number of switchings," *SIAM Journal on Control and Optimization*, vol. 17, no. 5, pp. 629 – 651, 1979.
[15] V. Adir and A. Stoica, "Integral LQR control of a star-shaped octorotor," *Incas Bulletin*, vol. 4, no. 2, pp. 3 – 18, 2012.
[16] W. Borgest and P. Varaiya, "Target function approach to linear pursuit problems," *IEEE Transactions on Automatic Control*, vol. 16, no. 5, pp. 449 – 459, 1971.
[17] Y. Sakawa, "Solution of linear pursuit-evasion games," *SIAM Journal on Control*, vol. 8, no. 1, pp. 100 – 112, 1970.
[18] R. F. Brammer, "Controllability in linear autonomous systems with positive controllers," *SIAM Journal on Control*, vol. 10, no. 2, pp. 339 – 353, 1972.
[19] G. Aronsson, "Global controllability and bang-bang steering of certain nonlinear systems," *SIAM Journal on Control*, vol. 11, no. 4, pp. 607 – 619, 1973.
[20] K. Glashoff and E. Sachs, "On theoretical and numerical aspects of the bang-bang-principle," *Numerische Mathematik*, vol. 29, no. 1, pp. 93 – 113, 1977.
[21] G. M. Ziegler, *Lectures on Polytopes*. Springer Science & Business Media, 2012, vol. 152.
[22] A. Freddi, A. Lanzon, and S. Longhi, "A feedback linearization approach to fault tolerance in quadrotor vehicles," in *18th IFAC World Congress*, 2011, pp. 5413 – 5418.
[23] H. Romero, S. Salazar, A. Sanchez, and R. Lozano, "A new UAV configuration having eight rotors: Dynamical model and real-time control," in *46th IEEE Conference on Decision and Control*, 2007, pp. 6418 – 6423.
[24] S. T. G. Ola Härkegård, "Resolving actuator redundancy - optimal control vs. control allocation," *Automatica*, vol. 41, pp. 137 – 144, 2005.
[25] L. Wu, Y. Ke, and B. Chen, "Systematic modeling of rotor dynamics for small unmanned aerial vehicles," in *International Micro Air Vehicle Competition and Conference*, 2016, pp. 284 – 290.
[26] J. Eaton, "An iterative solution to time-optimal control," *Journal of Mathematical Analysis and Applications*, vol. 5, no. 2, pp. 329 – 344, 1962.

Jean-Baptiste Bouvier received his dual master's degree in Aerospace Engineering from the University of Illinois Urbana-Champaign (UIUC) in 2018 and from ISAE-Supaéro in France in 2019. He received his PhD in Aerospace Engineering at UIUC in 2023. His research focuses on building a mathematical control theory to verify and quantify the resilience of autonomous systems to partial loss of control authority over their actuators.

Kathleen Xu received her B.S. degree in Aerospace Engineering from the University of Illinois Urbana-Champaign in 2021. She started her PhD in Aeronautics and Astronautics at the Massachussetts Institute of Technology in 2021. Her research interests lie at the intersection of controls and learning.

Melkior Ornik (Senior Member, IEEE) is an assistant professor in the Department of Aerospace Engineering and the Coordinated Science Laboratory at the University of Illinois at Urbana-Champaign. He received his Ph.D. degree from the University of Toronto in 2017. His research focuses on developing theory and algorithms for learning and planning of autonomous systems operating in uncertain, complex and changing environments, as well as in scenarios where only limited knowledge of the system is available.