Designing Resilient Linear Systems

Jean-Baptiste Bouvier, *Student Member, IEEE,* and Melkior Ornik

***Abstract*—Critical systems must be designed resilient to malfunctions and especially to a loss of control authority over actuators. This malfunction considers actuators producing uncontrolled and possibly undesirable outputs. We investigate the design of resilient linear systems capable of reaching their target even after such a malfunction. In contrast with the settings considered by robust control and fault-tolerant control, we consider undesirable but observable inputs of the same magnitude as controls since they are produced by a faulty actuator belonging to the system. The control inputs can then depend on these undesirable inputs. Building on our previous work, we focus on designing resilient systems able to withstand the loss of one or multiple actuators. Since resilience refers to the existence of a control law driving the state to the target, we naturally continue with the synthesis of such a control law. We conclude with the application of our theory to the ADMIRE fighter jet model.**

***Index Terms*—Linear systems, Reachability analysis, Control design, Reliability, Redundancy**

I. Introduction

REDUNDANCY is the key to guarantee the resilience of a system, as proven by NASA during the space race [1]. We focus on the resilience of linear systems to the loss of control authority over some of their actuators. This malfunction studied in [2, 3] refers to actuators producing undesirable and uncontrolled outputs. Thanks to sensors on each actuators and a fault-detection mechanism as in [4], the controller has real-time readings over all inputs even the uncontrolled ones and can identify defective actuators.

This paper is a continuation of our initial work in [3] and investigates how to design linear systems resilient to a loss of control authority over some of their actuators, i.e., that can still reach their initial target. We say that a target is *resiliently reachable* from an initial state if for any undesirable inputs, there exists a control law — possibly dependent on current undesirable inputs, but with no knowledge of future ones — able to drive the system to the target. While not referring to it as resilient reachability, [5] and [6] considered this setting but developed complex algorithms giving absolutely no hindsight about how to design resilient systems or how to synthesize a resilient control input, which are our two objectives. Moreover, the resilience analysis of a system, like the one performed in Section VI-A is impossible with the methods of [5, 6]. Building on [7], the work [3] established reachability conditions for linear systems, but it did not investigate resilience of systems.

Loss of control authority over actuators is not covered by fault-tolerant papers as they consider either actuators locking in place [8], losing effectiveness but remaining controllable [9], or a combination of both [10], but not uncontrolled and fully effective actuators. While the field of robust control [11, 12] encompasses our type of malfunction, it is too conservative to solve our problem. Indeed, our undesirable inputs can have the same magnitude as the controlled inputs and thus are too large to be handled by a robust control law [13]. Moreover, the robust control setting treats undesirable inputs as unknown, while we assume to have real-time readings of them. Thus, our resilient controller adapts to the undesirable inputs and performs much better than an overly conservative robust controller, as demonstrated in Section VI-B.

Our objective is to design linear systems resilient to the loss of control authority over some of their actuators with a minimal redundancy. The contributions of this paper are twofold. First, we determine the minimal degree of overactuation necessary to design a resilient system. Second, we synthesize a control law driving a resilient system's state to its target despite loss of control authority over some actuators. To establish these results, we will first focus on driftless systems, a common application in robotics [14], before extending our findings to systems with drift.

The remainder of the paper is organized as follows. Section II defines the problems of interest and introduces the preliminary results from [3]. In Section III, we develop the notion of resilient control matrices and we determine their minimal size in Section IV. Building on the driftless case, Section V focuses on the synthesis of a resilient control law for linear systems with and without drift. We illustrate our theory in Section VI with two scenarios featuring a model of a fighter jet undergoing a loss of control authority.

Notation: A positive semidefinite matrix is denoted by $M \succeq 0$ and a positive definite matrix by $M \succ 0$. The set of eigenvalues of a square matrix M is $\lambda(M)$ and $\det(M)$ is its determinant. The singular values of a rectangular matrix M are the $\sigma^M \geq 0$ such that $\det\left((\sigma^M)^2 I - M^\top M\right) = 0$, and $\sigma^M_{max} := \max \sqrt{\lambda(M^\top M)}$. The vector e_i is composed of zeros except its i^{th} element is one. The column vector $z = (z_1, \dots, z_n) \in \mathbb{R}^n$ has a norm $\|z\| := \sqrt{\sum z_i^2}$. The set of integers from 1 to n is denoted by $[n]$. The unit sphere in $\mathbb{R}^n$ is $\mathbb{S} := \left\{x \in \mathbb{R}^n : \|x\| = 1\right\}$, while $\mathbb{B}_X(c, \varepsilon) := \left\{x \in X : \|x - c\| \leq \varepsilon\right\}$ denotes the ball of center c and radius ε in the space X. The ellipsoid of center c and shape matrix $P \succ 0$ is $\mathcal{E}(c, P) := \left\{x : (x-c)^\top P (x-c) \leq 1\right\}$. The space of square integrable functions $u : [0, T] \to \mathbb{R}^m$ is $\mathcal{L}_2\big([0, T],\ \mathbb{R}^m\big)$, and contains all functions with a finite $\mathcal{L}_2$-norm: $\|u\|^2_{\mathcal{L}_2} := \int_0^T \|u(t)\|^2 dt$. The real part of a complex number is given by $Re : \mathbb{C} \to \mathbb{R}$. For $p \leq m \in \mathbb{N}$, the number of p-combinations among m elements is $\binom{m}{p}$.

J.-B. Bouvier and M. Ornik are with the Department of Aerospace Engineering and the Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA. e-mail: (bouvier3@illinois.edu & mornik@illinois.edu)

Manuscript received July 2020; revised May 2021.

This work was supported by an Early Stage Innovations grant from NASA's Space Technology Research Grants Program, grant no. 80NSSC19K0209.

II. Problem Statement and Preliminaries

Consider a system governed by the differential equation

$$\dot{x} = Ax + \bar{B}\bar{u}, \qquad x(0) = x_0 \in \mathbb{R}^n, \tag{1}$$

where $A \in \mathbb{R}^{n\times n}$ and $\bar{B} \in \mathbb{R}^{n\times m}$ are constant matrices. Let $G \subset \mathbb{R}^n$ be the *target ball* to be reached by the state x. During its mission the system loses control authority over p of its m actuators. These p actuators are then producing uncontrolled and undesirable inputs w. Thanks to sensors on each actuators, we separate w from the controls u by writing $\bar{u} = (u,\ w)$ and $\bar{B} = [B\ C]$, with $B \in \mathbb{R}^{n\times(m-p)}$ and $C \in \mathbb{R}^{n\times p}$, leading to

$$\dot{x}(t) = Ax(t) + Bu(t) + Cw(t), \qquad x(0) = x_0 \in \mathbb{R}^n. \tag{2}$$

We follow the assumptions of [3, 7] by considering inputs of finite energy and thus square integrable. The set of admissible control laws is U and the set of undesirable inputs is W with

$$\begin{aligned} U &:= \big\{u \in \mathcal{L}_2\big([0,T],\ \mathbb{R}^{m-p}\big) : \|u\|_{\mathcal{L}_2} \leq 1\big\} = \mathbb{B}_{\mathcal{L}_2}(0,1),\\ W &:= \big\{w \in \mathcal{L}_2\big([0,T],\ \mathbb{R}^{p}\big) : \|w\|_{\mathcal{L}_2} \leq 1\big\} = \mathbb{B}_{\mathcal{L}_2}(0,1),\\ G &:= \big\{x \in \mathbb{R}^n : \|x - x_{goal}\| \leq \varepsilon\big\} = \mathbb{B}_{\mathbb{R}^n}(x_{goal}, \varepsilon). \end{aligned}$$

We want to characterize systems that are able to reach their target even after a loss of control over some of their actuators.

Definition 1. The target G is *resiliently reachable at time T* from x_0 by system (2) if for any undesirable inputs $w \in W$, there exists a control law $u_w \in U$ such that $x(T) \in G$.

As in [3], the control law u_w can depend on the undesirable input w. Indeed, we assume to have sensors on each actuators so that all inputs to the system are available to the controller. Unlike in robust control [11, 12], our resilient controller is thus aware of the undesirable inputs and should be able to counteract them more efficiently. Therefore, resilient reachability guarantees that whatever the undesirable inputs are, there is a control law *dependent on the undesirable inputs* driving the system to its target. We have the intuition that a system resilient to the loss of control over some of its actuators must be initially *overactuated*, i.e., its control matrix $\bar{B}$ has strictly more columns than rows. Since adding actuators in practice comes with a cost, we consider the following problem.

Problem 1. Determine the minimal degree of overactuation required to build a resilient system.

Our definition of resilience calls for the existence of a control law, so we are naturally led to our second objective.

Problem 2. For a resilient system sustaining an undesirable input w, synthesize a control law u_w that drives the system's state $x(t)$ to the target G.

The resilience of a linear system (1) is mostly determined by its control matrix $\bar{B}$. Therefore, in the next two sections we first focus on driftless systems, i.e., where (2) becomes

$$\dot{x}(t) = Bu(t) + Cw(t), \qquad x(0) = x_0 \in \mathbb{R}^n. \tag{3}$$

According to [3], the resilience of these systems is linked to the sign of the maximum of $g(h) := \|C^\top h\| - \|B^\top h\|$ over $h \in \mathbb{S}$. Since this maximum is difficult to compute, we introduce an equivalent but more convenient criteria.

Theorem 1. For $F := BB^\top - CC^\top$, the following hold:

(a) If $F \succ 0$, there exists a time t_{lim} such that G is resiliently reachable for all $t \geq t_{lim}$.

(b) If $F \not\succeq 0$, there exists a time t_{lim} such that G is not resiliently reachable for all $t > t_{lim}$.

Proof. If $F \succ 0$, then for all $h \in \mathbb{S}$, we have $0 < h^\top Fh$, i.e., $h^\top CC^\top h < h^\top BB^\top h$. This is equivalent to $\max_{h\in\mathbb{S}} g(h) < 0$, and thus according to Theorem 6 of [3], there exists a time t_{lim} after which G is resilient reachable.

Similarly, if $F \not\succeq 0$, there is $h \in \mathbb{S}$ such that $h^\top Fh < 0$, i.e., $\max_{h\in\mathbb{S}} g(h) > 0$. Following Theorem 4 of [3] there exists a time t_{lim} after which G is not resiliently reachable. ■

With this simple resilient reachability condition, we can now investigate the resilience of a system.

III. Resilient Control Matrices

When losing control authority over p actuators, we remove the corresponding columns $j_1, \dots, j_p$ from $\bar{B}$ to form the matrix C, and we name B the remaining control matrix.

Definition 2. The control matrix $\bar{B} \in \mathbb{R}^{n\times m}$ is *p-resilient* if for all pairwise distinct $j_1, \dots, j_p \in [m]$ the system following the driftless dynamics (3) can resiliently reach any target ball.

The *degree of resilience* of matrix $\bar{B}$ is the largest $p \in \mathbb{N}$ for which $\bar{B}$ is p-resilient.

Proposition 1. The control matrix $\bar{B}$ is p-resilient if and only if $\max_{h\in\mathbb{S}} g(h) < 0$ for all pairwise distinct $j_1, \dots, j_p \in [m]$ if and only if $F \succ 0$ for all pairwise distinct $j_1, \dots, j_p \in [m]$.

Proof. If $\max_{h\in\mathbb{S}} g(h) < 0$ for all pairwise distinct $j_1, \dots, j_p \in [m]$, then from Theorem 6 of [3], any target ball is resiliently reachable, so $\bar{B}$ is p-resilient.

On the other hand, assume that $\bar{B}$ is p-resilient. For all pairwise distinct $j_1, \dots, j_p \in [m]$, the continuous function g reaches a maximum g_{max} over the compact set $\mathbb{S}$. If $g_{max} \geq 0$, then from Theorems 4 and 5 of [3] some target balls are not resiliently reachable. Therefore, $g_{max} < 0$.

From Theorem 1, the equivalence with $F \succ 0$ holds. ■

Proposition 1 enables us to assess the p-resilience of a system with m actuators by verifying the positive definiteness of $\binom{m}{p}$ matrices. We now establish several results concerning resilient matrices in order to address Problem 1.

Proposition 2. If $\bar{B}$ is p-resilient with $p \geq 1$, then $\bar{B}\bar{B}^\top \succ 0$.

Proof. Assume that $\bar{B}\bar{B}^\top$ is not positive definite. Then, there exists $x \neq 0$ such that $x\bar{B}\bar{B}^\top x \leq 0$. Let C be the last column of $\bar{B}$, so that $\bar{B}\bar{B}^\top = \begin{bmatrix}B & C\end{bmatrix}\begin{bmatrix}B^\top\\ C^\top\end{bmatrix} = BB^\top + CC^\top$. Then, $F = BB^\top - CC^\top = \bar{B}\bar{B}^\top - 2CC^\top$. Thus, $x^\top Fx = x^\top\bar{B}\bar{B}^\top x - 2x^\top CC^\top x \leq 0 - 2\|C^\top x\|^2 \leq 0$, so $F \not\succeq 0$. By Proposition 1, $\bar{B}$ is not 1-resilient and thus not p-resilient either since $p \geq 1$. ■

Proposition 3. If $\bar{B}$ is p-resilient with $p \geq 1$, then the system is overactuated.

Proof. Assume $\bar{B} \in \mathbb{R}^{n\times m}$ is not overactuated, i.e., $m \leq n$. After losing control of one actuator, the remaining control matrix B has n rows and at most $n-1$ columns. From [15], $rank(BB^\top) \leq rank(B) \leq n-1$. Since $BB^\top \in \mathbb{R}^{n\times n}$, it is not invertible. Then, $BB^\top \not\succ 0$, so $F = BB^\top - CC^\top \not\succ 0$ either. According to Proposition 1, $\bar{B}$ is not p-resilient. ■

Intuitively a system without actuator redundancy cannot be resilient, because a malfunctioning actuator cannot be counteracted. On the other hand, numerous copies of each actuator guarantees resilience. In between these extremes lies a minimum degree of overactuation required for resilience.

Proposition 4. The degree of resilience of $\bar{B}$ is not affected by left multiplication by an invertible matrix.

Proof. For P invertible, note that $PFP^\top \succ 0$ if and only if $F \succ 0$. Proposition 1 concludes the proof. ■

We can now simplify the resilience investigation with the Singular Value Decomposition (SVD). The compact SVD [16] of $\bar{B}$ is UDV, with U orthogonal of size $n \times n$, D a diagonal matrix gathering the n singular values of $\bar{B}$, and V of size $n \times m$ with orthonormal rows, i.e., $VV^\top = I_n$.

Proposition 5. The following statements hold for $p \geq 1$:

(a) If $\bar{B}$ is p-resilient, then V is also p-resilient.
(b) If V is p-resilient and $\bar{B}\bar{B}^\top \succ 0$, then $\bar{B}$ is p-resilient.

Proof. (a) According to Proposition 2, $\bar{B}\bar{B}^\top \succ 0$, so the singular values of $\bar{B}$ are non-zero [16]. Then, D is invertible and since U is also invertible, Proposition 4 states that $\bar{B} = UDV$ and V have the same degree of resilience.

(b) Since $\bar{B}\bar{B}^\top \succ 0$, the matrix D is invertible. Then, by Proposition 4, $\bar{B}$ has the same degree of resilience as V. ■

We can then work on V to determine the resilience of $\bar{B}$. After a malfunction we split V like $\bar{B}$ into $V = \begin{bmatrix} C_V & B_V \end{bmatrix}$.

Proposition 6. The matrix $V \in \mathbb{R}^{n\times m}$ is p-resilient if and only if $\sigma_{max}^{C_V^\top} < \frac{1}{\sqrt{2}}$ for all $\binom{m}{p}$ possible C_V matrices.

Proof. We investigate whether $F_V := B_V B_V^\top - C_V C_V^\top \succ 0$. Note that $VV^\top = B_V B_V^\top + C_V C_V^\top$. Since $VV^\top = I_n$, $F_V = VV^\top - 2C_V C_V^\top = I_n - 2C_V C_V^\top$. Let λ be an eigenvalue of F_V:

$$\begin{aligned} 0 &= \det\left(\lambda I_n - F_V\right) = \det\left(\lambda I_n - I_n + 2C_V C_V^\top\right) \\ &= \det\left((\lambda-1)I_n + 2C_V C_V^\top\right) \\ &= \big(-2\big)^n \det\left(\Big(\frac{1-\lambda}{2}\Big) I_n - C_V C_V^\top\right). \end{aligned}$$

Define $s := \frac{1-\lambda}{2}$, so that s is an eigenvalue of $C_V C_V^\top$. Let $x \neq 0$ be an eigenvector such that $C_V C_V^\top x = sx$. A left multiplication by $x^\top$ lead to $\|C_V^\top x\|^2 = s\|x\|^2$, so $s \geq 0$.

Then, $\sqrt{s}$ is a singular value of $C_V^\top$. We note that $\lambda > 0$ if and only if $\sqrt{s} < \frac{1}{\sqrt{2}}$. Since $\sigma_{max}^{C_V^\top}$ is the maximal singular value of $C_V^\top$, $F_V \succ 0$ if and only if $\sigma_{max}^{C_V^\top} < \frac{1}{\sqrt{2}}$. ■

With Propositions 5 and 6, Problem 1 is now within our reach for 1-resilient matrices.

IV. Minimal size of resilient matrices

We will now establish a necessary condition determining the minimal size of a 1-resilient control matrix.

Theorem 2. If $\bar{B} \in \mathbb{R}^{n\times m}$ is 1-resilient, then $m \geq 2n+1$.

Proof. Proposition 5 (a) states that V is 1-resilient. Let C_j be the columns of V and r_i its rows, with $\|r_i\| = 1$. Then,

$$\sum_{j=1}^{m} \|C_j\|^2 = \sum_{j=1}^{m}\sum_{i=1}^{n} V_{ij}^2 = \sum_{i=1}^{n}\sum_{j=1}^{m} V_{ij}^2 = \sum_{i=1}^{n} \|r_i\|^2 = n.$$

Thus, $\max_j \|C_j\|^2 \geq \frac{n}{m}$. From [15], $\max_j \|C_j\|^2 = \left(\sigma_{max}^{C^\top}\right)^2$. Then, Proposition 6 yields $\frac{n}{m} < \frac{1}{2}$, i.e., $m \geq 2n+1$. ■

Theorem 2 shows that at least $2n+1$ actuators are required to have a 1-resilient control system in n dimensions. We will now prove that $n \times (2n+1)$ is in fact the minimal size of 1-resilient matrices by producing such a matrix for all $n \in \mathbb{N}$. Let $\bar{B}_k := [I_n \dots I_n \; D]$ composed of k identity matrices and a column vector $D := \frac{1}{\sqrt{n}}[1 \dots 1]^\top$.

Proposition 7. The matrix $\bar{B}_{2p}$ is p-resilient.

Proof. We calculate the maximum of $g(h) = \|C^\top h\| - \|B^\top h\|$ over $h \in \mathbb{S}$ for all possible losses of p actuators.

First, assume the system loses control of p columns belonging all to the identity matrices. Without loss of generality we assume losing one column per matrix. The index of the column lost in the i^{th} identity matrix is $j_i \in [n]$. These columns form the matrix $C = \begin{bmatrix} e_{j_1} \dots e_{j_p} \end{bmatrix}$, while B is the remaining control matrix. Then, $h = \big(h_1, \dots, h_n\big) \in \mathbb{S}$, i.e., $\|h\|^2 = 1$, yields

$$\begin{aligned} C^\top h &= \big(h_{j_1}, \dots, h_{j_p}\big) \quad \text{so} \quad \|C^\top h\|^2 = \sum_{i=1}^{p} h_{j_i}^2, \\ \|B^\top h\|^2 &= 2p\sum_{i=1}^{n} h_i^2 - \sum_{i=1}^{p} h_{j_i}^2 + \left(\sum_{i=1}^{n} \frac{h_i}{\sqrt{n}}\right)^2 \\ &= 2p - \sum_{i=1}^{p} h_{j_i}^2 + \frac{1}{n}\left(\sum_{i=1}^{n} h_i\right)^2, \\ g(h) < 0 &\iff \sum_{i=1}^{p} h_{j_i}^2 < 2p - \sum_{i=1}^{p} h_{j_i}^2 + \frac{1}{n}\left(\sum_{i=1}^{n} h_i\right)^2 \\ &\iff \sum_{i=1}^{p} h_{j_i}^2 < p + \frac{1}{2n}\left(\sum_{i=1}^{n} h_i\right)^2. \end{aligned} \tag{4}$$

If $j_1 = \dots = j_p$, and $h = e_{j_1}$, then (4) simplifies into $p < p + \frac{1}{2n}$, which is true. In all other cases, because $\|h\| = 1$, at least one $h_{j_i} < 1$, so the left hand side of (4) is strictly smaller than p. Then, the inequality also holds true, $g(h) < 0$ for all $h \in \mathbb{S}$. For lack of space, details can be found in [17].

The other possibility is that $\bar{B}_{2p}$ loses $p-1$ columns among the identity matrices and the last column D. Then,

$$g(h) = \sqrt{\sum_{i=1}^{p-1} h_{j_i}^2 + \frac{1}{n}\left(\sum_{i=1}^{n} h_i\right)^2} - \sqrt{2p - \sum_{i=1}^{p-1} h_{j_i}^2}\,.$$

Since $\|h\| = 1$, $h_{j_i}^2 \leq 1$ for all $i \in [p\text{-}1]$. Then, $(\sum h_i)^2 \leq (\sum h_i^2)(\sum 1^2) = \|h\|^2 \; n = n$, by the Cauchy-Schwarz

inequality [18]. Thus, $g(h) \leq \sqrt{p-1+\frac{1}{n}n} - \sqrt{2p-(p-1)} \leq \sqrt{p} - \sqrt{p+1} < 0$, i.e., $\max_{h \in \mathbb{S}} g(h) < 0$, so $\bar{B}_{2p}$ is p-resilient from Proposition 1. ■

Then, $\bar{B}_2 = \begin{bmatrix} I_n \, I_n \, D \end{bmatrix}$ is 1-resilient and has only $2n+1$ columns. Following Theorem 2, the minimal size of a 1-resilient matrix is then exactly $n \times (2n+1)$.

To extend our minimal size investigation to $p \geq 2$ we only need an equivalent of Theorem 2, because Proposition 7 generates p-resilient matrices of size $n \times (2pn+1)$. However, the calculations fail for $p \geq 2$ as we found 2-resilient matrices of size $n \times 4n$ for $n = 6$ and $n = 8$. Therefore, the minimal size of a p-resilient matrix is not $n \times (2pn+1)$ and that is why Theorem 2 cannot be extended to $p \geq 2$. More details are given in [17]. It is now time to tackle Problem 2.

V. Control synthesis

The definition of resilient reachability asks for the existence of a control law. A natural follow-up question is thus one of designing such a control law. When B is not invertible, this question is not trivial as the control u needs to counteract $w \in W$ while remaining in U.

Theorem 3. If $F \succ 0$, then there exists $\alpha > 0$ such that

$$u(t) := B^\top \big(BB^\top\big)^{-1} \Big(-Cw(t) + \alpha\big(x_{goal} - x(t)\big)\Big) \quad (5)$$

drives the state of (3) to x_{goal} and $u \in U$ for any $w \in W$.

Proof. Since $F = BB^\top - CC^\top \succ 0$, obviously $BB^\top \succ 0$, so $BB^\top$ is invertible, and (5) is well-defined. If we plug (5) into the state equation (3) we obtain

$$\begin{aligned} \dot{x} &= BB^\top \big(BB^\top\big)^{-1} \Big(-Cw + \alpha\big(x_{goal} - x\big)\Big) + Cw \\ &= \alpha\big(x_{goal} - x\big). \end{aligned}$$

The solution is $x(t) = x_{goal} + e^{-\alpha t} d$, with $d = x(0) - x_{goal}$. Since $\alpha > 0$, x converges globally exponentially to x_{goal}, the control law is successful. We need to prove that $\|u\|_{\mathcal{L}_2} \leq 1$ for all $w \in W$. Note that $x_{goal} - x(t) = -e^{-\alpha t} d$, and let $v(t) := Cw(t) + \alpha e^{-\alpha t} d$, so that $u(t) = -B^\top \big(BB^\top\big)^{-1} v(t)$. Then,

$$\|u\|^2_{\mathcal{L}_2} = \int_0^T u(t)^\top u(t)\, dt = \int_0^T v(t)^\top \big(BB^\top\big)^{-1} v(t)\, dt.$$

To simplify, let $P := \big(BB^\top\big)^{-1} \succ 0$, and expand $v(t)$ as

$$\begin{aligned} v(t)^\top P v(t) = &\underbrace{w(t)^\top C^\top P C w(t)}_{=\, T_1} + \underbrace{w(t)^\top C^\top P \alpha e^{-\alpha t} d}_{=\, T_2} \\ &+ \underbrace{\alpha e^{-\alpha t} d^\top P C w(t)}_{=\, T_3} + \underbrace{\alpha^2 d^\top e^{-\alpha t} P e^{-\alpha t} d}_{=\, T_4} \end{aligned} \quad (6)$$

From the Woodbury formula [15], $\big(I + C^\top F^{-1} C\big)$ is invertible, because F is invertible,

$$P = \big(F + CC^\top\big)^{-1} = F^{-1} - F^{-1} C \big(I + C^\top F^{-1} C\big)^{-1} C^\top F^{-1}.$$

Let $D := C^\top F^{-1} C$. Then, $C^\top P C = D - D\big(I+D\big)^{-1} D$. Expanding $\big(I+D\big)^{-1}\big(I+D\big) = I$ yields $\big(I+D\big)^{-1} D = I - \big(I+D\big)^{-1}$, so that $C^\top P C = D - D + D\big(I+D\big)^{-1}$. Similarly, from $\big(I+D\big)\big(I+D\big)^{-1} = I$, we finally obtain $C^\top \big(BB^\top\big)^{-1} C = I - \big(I+D\big)^{-1}$. Let λ be an eigenvalue of $C^\top \big(BB^\top\big)^{-1} C$. Then,

$$\begin{aligned} 0 &= \det\big(\lambda I - C^\top \big(BB^\top\big)^{-1} C\big) = \det\big(\lambda I - I + \big(I+D\big)^{-1}\big) \\ &= \det\big((\lambda-1)(I+D)(I+D)^{-1} + I(I+D)^{-1}\big) \\ &= \det\big((\lambda-1)(I+D) + I\big) \det(I+D)^{-1}. \end{aligned}$$

From the Woodbury formula we know that $(I+D)$ is invertible, so $\det(I+D))^{-1} \neq 0$. If $\lambda = 1$, then $\det(I) = 0$, which is absurd. Thus $\lambda \neq 1$, so we can divide by $(\lambda - 1)$:

$$0 = \det\Big(I + D + \frac{1}{\lambda - 1} I\Big) = \det\Big(\frac{\lambda}{\lambda - 1} I + D\Big).$$

Since $F^{-1} \succ 0$, $C^\top F^{-1} C \succeq 0$, i.e. the eigenvalues of D are nonnegative, so $\frac{-\lambda}{\lambda - 1} \geq 0$. Since $BB^\top \succ 0$, $\big(BB^\top\big)^{-1} \succeq 0$ and then $C^\top \big(BB^\top\big)^{-1} C \succeq 0$, thus $\lambda \geq 0$. Then $\lambda - 1 < 0$, i.e. $\lambda < 1$. Let $\lambda_M < 1$ the maximal eigenvalue of $C^\top \big(BB^\top\big)^{-1} C$

$$\begin{aligned} \int_0^T T_1 dt = \int_0^T w(t)^\top C^\top \big(BB^\top\big)^{-1} C w(t)\, dt \leq \int_0^T w(t)^\top \lambda_M w(t)\, dt \\ \leq \lambda_M \|w\|^2_{\mathcal{L}_2} \leq \lambda_M. \end{aligned} \quad (7)$$

We can now tackle the integral of the second term of (6):

$$\int_0^T T_2 dt = \int_0^T \alpha w(t)^\top C^\top P e^{-\alpha t} d\, dt = \alpha \int_0^T w(t)^\top e^{-\alpha t} dt\; C^\top P d.$$

We use the Cauchy-Schwarz inequality

$$\begin{aligned} \left|\left| \int_0^T w(t)^\top e^{-\alpha t} dt \right|\right|_{\mathbb{R}^m} &= \sqrt{\sum_{i=1}^m \left(\int_0^T w_i(t) e^{-\alpha t} dt \right)^2} \\ &\leq \sqrt{\sum_{i=1}^m \left(\int_0^T w_i^2(t) dt \right) \left(\int_0^T e^{-2\alpha t} dt \right)} \\ &= \sqrt{\left[\frac{e^{-2\alpha t}}{-2\alpha} \right]_0^T \int_0^T \sum_{i=1}^m w_i^2(t) dt} = \sqrt{\frac{1 - e^{-2\alpha T}}{2\alpha}}\ \|w\|_{\mathcal{L}_2}. \end{aligned}$$

Thus, $$\int_0^T T_2\ dt \leq \sqrt{\frac{\alpha}{2}} \|C^\top P d\|\ \|w\|_{\mathcal{L}_2}. \quad (8)$$

And similarly, $$\int_0^T T_3\ dt \leq \sqrt{\frac{\alpha}{2}} \|d^\top P C\|\ \|w\|_{\mathcal{L}_2}. \quad (9)$$

We also simplify the integral of the fourth term of (6):

$$\begin{aligned} \int_0^T T_4 &= \int_0^T \alpha^2 d^\top e^{-\alpha t} P e^{-\alpha t} d\ dt = \alpha^2 d^\top P d \int_0^T e^{-2\alpha t}\ dt \\ &= \alpha^2 d^\top P d \left[\frac{e^{-2\alpha t}}{-2\alpha} \right]_0^T = \frac{\alpha}{2} d^\top P d \big(1 - e^{-2\alpha T}\big) \leq \frac{\alpha}{2}\ d^\top P d. \end{aligned} \quad (10)$$

Then, we combine (7), (8), (9) and (10):

$$\|u\|^2_{\mathcal{L}_2}\ \leq\ \frac{\alpha}{2}\ d^\top P d + 2\sqrt{\frac{\alpha}{2}} \|C^\top P d\| + \lambda_M. \quad (11)$$

Since $\lambda_M < 1$, and d, P and C are constant, we can choose α small enough so that the right hand side of (11) is smaller than 1, which finally leads to $\|u\|^2_{\mathcal{L}_2} \leq 1$, i.e. $u \in U$. ■

The maximum α satisfying Theorem 3 and thus ensuring the fastest convergence to x_{goal} is given by

$$\alpha^* := 2\,\frac{\left(\sqrt{b^2+(1-\lambda_M)a}-b\right)^2}{a^2}, \tag{12}$$

with $a = d^\top P d$ and $b = \|C^\top P d\|$. We now return to system (2). For all $\eta > \max(Re(\lambda(A)))$, we can find $\beta > 0$ such that $\|e^{At}\| \leq \beta e^{\eta t}$ for all $t \geq 0$ [15], and we define the set

$$\mathcal{A}_\eta := \Big\{\alpha > \eta : \lambda_M + \frac{\alpha\sqrt{2}\beta\|x_0\|}{\sqrt{\alpha-\eta}}\|C^\top P\| + \frac{\alpha^2\beta^2\|x_0\|^2\|P\|}{2(\alpha-\eta)} \leq 1\Big\}.$$

Theorem 4. If $F \succ 0$ and if there exists $\eta > \max(Re(\lambda(A)))$ such that $\mathcal{A}_\eta$ is not empty, then for all $\alpha \in \mathcal{A}_\eta$, control law $u(t) := B^\top\big(BB^\top\big)^{-1}\big(-Cw(t) - \alpha x(t)\big)$ drives the state of (2) to $x_{goal} = 0$, and $u \in U$ for any $w \in W$.

Proof. The only change compared to Theorem 3 is that $e^{-\alpha t}d$ is replaced by $e^{\tilde{A}t}x_0$ with $\tilde{A} := A - \alpha I$. We use $\|e^{\tilde{A}t}\| \leq \beta e^{\eta t}e^{-\alpha t}$ before proceeding as in the proof of Theorem 3. The complete proof is available in [17]. ■

Set $\mathcal{A}_\eta$ depends on $\|x_0\|$, so the further away x_0 is, the less instability can be counteracted by the control law.

Corollary. If A is Hurwitz and $\bar{B}$ is p-resilient, then the system $\dot{x} = Ax + \bar{B}u$ is also p-resilient for $x_{goal} = 0$.

Proof. Since $\bar{B}$ is p-resilient, we can lose p actuators and create $F \succ 0$. Since A is Hurwitz, we can pick $\alpha \in \mathcal{A}_\eta$ such that $\alpha \geq 0 > \eta > \max(Re(\lambda(A)))$. Thus, the control law (5) drives the state to 0, the system is p-resilient. ■

VI. Numerical Example

A. Resilience of a fighter jet

We illustrate our theory on the ADMIRE fighter jet model [19], a classical application for control frameworks [20], [21]. We focus on the sub-system of the model associated to the actuators. The dynamics of the angular velocities in roll, pitch and yaw (rad/s) established in [20] are $\dot{x} = Ax + \bar{B}u$, with:

$$x = \begin{bmatrix} p \\ q \\ r \end{bmatrix} \qquad A = \begin{bmatrix} -0.9967 & 0 & 0.6176 \\ 0 & -0.5057 & 0 \\ -0.0939 & 0 & -0.2127 \end{bmatrix}$$

$$\bar{B} = \begin{bmatrix} 0 & -4.2423 & 4.2423 & 1.4871 \\ 1.6532 & -1.2735 & -1.2735 & 0.0024 \\ 0 & -0.2805 & 0.2805 & -0.8823 \end{bmatrix}.$$

Since the eigenvalues of A have negative real parts, the system is stable. The inputs are the deflections of the control surfaces in radians: $u_c \in [-25, 55]\frac{\pi}{180}$ for the canard wings, u_{re} and $u_{le} \in [-30, 30]\frac{\pi}{180}$ for the right and left elevons, and $u_r \in [-30, 30]\frac{\pi}{180}$ for the rudder.

Consider the scenario in which, after sustaining damage (e.g., during air combat), one of the control surfaces of the fighter jet starts producing undesirable inputs. The pilot wants to minimize the aircraft roll, pitch and yaw rates, so the target is a ball of radius 0.1 centered around the origin, $x_{goal} = 0$.

Based on the values of $\bar{B}$ we have the intuition that the system is only resilient to the loss of the canard. Indeed, the first column can be counteracted by the combined actions of both elevons, because $1.2735 + 1.2735 > 1.6532$. Only the elevons can counteract each other's roll but it would induce a high pitching moment that cannot be counteracted. The yawing moment produced by the rudder cannot be counteracted by the other actuators: $0.8823 > 0.2805 + 0.2805$.

As predicted, $BB^\top - CC^\top \succ 0$ only for the loss of control authority over the canard. Then, we use Theorem 4 and its notations: $\lambda_M = 0.8426 < 1$, $\alpha^* = 0.0343 > 0$, $\max(Re(\lambda(A))) = -0.259 < \alpha^*$, so the control law (5) should work. We simulate our system on MATLAB and add a white noise z of amplitude 0.1 as process disturbance. We generate w as a stochastic signal with $w(t) \in [-25, 55]\frac{\pi}{180}$ for $t \in [0, 25]$. If $\|w\|_{\mathcal{L}_2} > 1$, we divide w by its $\mathcal{L}_2$-norm, so that w respects both the $\mathcal{L}_2$ bound and the same constraint as u_c. For u to respect the input constraints, we add a saturation to (5). As predicted, the state converges exponentially from $x_0 = (1,\ 1,\ 1)\ rad/s$ to the origin, as shown by the blue curve in Figure 1. With a LQR controller unaware of the undesirable input, the state does not converge, as shown in red. The time evolution of all the inputs can be found in [17].

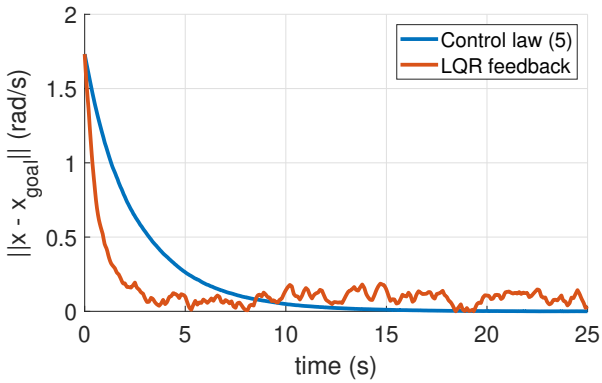

Fig. 1. Distance of the state x from the origin with $\dot{x} = Ax + Bu + Cw + z$ and z is a white noise of amplitude 0.1.

For the loss of control over an elevon $F \not\succ 0$, but $BB^\top$ is invertible. Then, control law (5) is still well-defined, but for some $w \in W$ the control is not admissible: $u_w \notin U$. For the loss of control over the rudder, $BB^\top$ is not invertible, so the control law (5) is not well-defined. We cannot guarantee that the jet can reach the desired target.

B. Comparison with robust control

A controller is robust if it *ignores the disturbance*, i.e., there exists a control u such that for all undesirable input w, we have $x(T) \in G$. On the other hand, resilient reachability considers a controller *aware of the undesirable input*, i.e., for all w, there exists a control u_w such that $x(T) \in G$.

In our setting, we reasonably assume that the undesirable input can be measured since it is produced by an actuator of the system. The resilient controller has access to more information than a robust controller, and thus should perform better.

We choose the robust control approach developed in [12], where the closed-loop reach set $\mathcal{X}[T]$ is approximated with internal and external ellipsoids. For a radius $\mu \geq 0$, $\mathcal{X}[T] := \big\{x_{goal} \in \mathbb{R}^n : \exists\, u \in U \ s.t.\ \forall\, w \in W,\ x(T) \in \mathbb{B}(x_{goal}, \mu)\big\}$.

We compare the precision of our approach with [12] based on the size of the smallest target ball guaranteed to be reached. The application case is the ADMIRE model studied in Section VI-A for the loss of control over the canards. For the bounds of the robust inputs u, we choose the maximal ellipsoid within the actuators range. More details are available in [17].

We compute the tight ellipsoidal internal approximation of the closed-loop reach set: $\mathcal{E}\big(x_{-}(T), X_{-}(T)\big) \subseteq \mathcal{X}[T]$. Then, we deduce the radius μ of the smallest robustly reachable target ball: $\mu = 5.9$. Thus, the robust control law can only guarantee to reach a target state within a radius of 5.9. The initial state $x_0 = (1,\ 1,\ 1)$ was already inside that ball. Thus, the robust control cannot even guarantee that the state will get closer to the target than its initial state.

On the other hand, we know that the jet is resilient to the loss of control over the canards. Therefore, a target ball of any size is resiliently reachable. By having access to the undesirable input, a controller ensuring resilient reachability is then more effective than a robust controller.

VII. Conclusions and Future Work

This paper introduced the notion of resilient systems that can withstand the loss of control over any single or multiple actuators and still guarantee to drive the state to its target. We determined the minimal number of actuators required to design a 1-resilient system. We then focused on the synthesis of a resilient control law for linear systems. Eventually, we illustrated our results on a model of a fighter jet.

There are three promising avenues of future work. We would like to consider the effects of measurements and process disturbances. We also want to change the type of bounds on the admissible inputs. Finally, we desire to establish a metric quantifying the resilience of a given system. For instance, by comparing the time required to reach a target with and without loss of control over actuators.

Acknowledgment

The authors thank Dr. Kenneth Bordignon and Dr. Wayne Durham for the ADMIRE model. We also thank the reviewers whose comments enabled great improvements of this paper.

References

[1] R. C. Suich and R. L. Patterson, "How much redundancy: Some cost considerations, including examples for spacecraft systems," NASA Technical Memorandum 103197, Tech. Rep., 1990.

[2] M. Bucić, M. Ornik, and U. Topcu, "Graph-based controller synthesis for safety-constrained, resilient systems," in *56th Annual Allerton Conference on Communication, Control, and Computing*, 2018, pp. 297 – 304.

[3] J.-B. Bouvier and M. Ornik, "Resilient reachability for linear systems," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 4409 – 4414, 2020, 21st IFAC World Congress.

[4] W. T. B. J. B. Davidson, F. J. Lallman, "Real-time adaptive control allocation applied to a high performance aircraft," in *5th SIAM Conference on Control and Its Applications*. SIAM, 2001.

[5] A. Marzollo and A. Pascoletti, "On the reachability of a given set under disturbances," *Control and Cybernetics*, vol. 2, no. 3, pp. 99 – 106, 1973.

[6] I. Mitchell and C. Tomlin, "Overapproximating reachable sets by hamilton-jacobi projections," *Journal of Scientific Computing*, vol. 19, pp. 323 – 346, December 2003.

[7] M. C. Delfour and S. K. Mitter, "Reachability of perturbed systems and min sup problems," *SIAM Journal on Control and Optimization*, vol. 7, no. 4, pp. 521 – 533, November 1969.

[8] 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.

[9] S. S. Tohidi, Y. Yildiz, and I. Kolmanovsky, "Fault tolerant control for over-actuated systems: An adaptive correction approach," in *2016 American Control Conference*. IEEE, 2016, pp. 2530 – 2535.

[10] 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.

[11] D. Bertsekas, "Infinite-time reachability of state-space regions by using feedback control," *IEEE Transactions on Automatic Control*, vol. 17, no. 5, pp. 604 – 612, October 1972.

[12] A. Kurzhanski and P. Varaiya, "Reachability analysis for uncertain systems-the ellipsoidal technique," *Dynamics of Continuous Discrete and Impulsive Systems Series B*, vol. 9, pp. 347 – 368, 2002.

[13] J.-F. Zhang *et al.*, "Fundamental limitations and differences of robust and adaptive control," in *Proceedings of the 2001 American Control Conference*, vol. 6. IEEE, 2001, pp. 4802 – 4807.

[14] B. Siciliano and O. Khatlib, *Springer Handbook of Robotics*. Springer, 2016.

[15] G. H. Golub and C. F. V. Loan, *Matrix Computations*, 4th ed. John Hopkins University Press, 2013.

[16] M. Gu and S. C. Eisenstat, "Downdating the singular value decomposition," *SIAM Journal on Matrix Analysis and Applications*, vol. 16, no. 3, pp. 793 – 810, July 1995.

[17] J.-B. Bouvier and M. Ornik, "Designing resilient linear driftless systems," *ArXiv*, 2020. [Online]. Available: https://arxiv.org/pdf/2006.13820.pdf

[18] J. B. Conway, *A Course in Functional Analysis*. New York City: Springer, 1990.

[19] U. N. Lars Forssell, "ADMIRE the aero-data model in a research environment version 4.0, model description," FOI - Swedish Defence Research Agency, Tech. Rep., December 2005.

[20] S. T. G. Ola Härkegård, "Resolving actuator redundancy - optimal control vs. control allocation," *Automatica*, vol. 41, pp. 137 – 144, 2005.

[21] A. Khelassi, P. Weber, and D. Theilliol, "Reconfigurable control design for over-actuated systems based on reliability indicators," in *Conference on Control and Fault-Tolerant Systems*, 2010, pp. 365 – 370.