2011 American Control Conference
on O'Farrell Street, San Francisco, CA, USA
June 29 - July 01, 2011

# Fault-Tolerant Controller Design with Applications in Power Systems and Synthetic Biology

Somayeh Sojoudi, Javad Lavaei and Richard M. Murray

*Abstract*— **This paper deals with fault-tolerant controller design for linear time-invariant (LTI) systems with multiple actuators. Given some critical subsets of the actuators, it is assumed that every combination of actuators can fail as long as the set of the remaining actuators includes one of these subsets. Motivated by electric power systems and biological systems, the goal is to design a controller so that the closed-loop system satisfies two properties: (i) stability under all permissible sets of faults and (ii) better performance after clearing every subset of the existing faults in the system. It is shown that a state-feedback controller satisfying these properties exists if and only if a linear matrix inequality (LMI) problem is feasible. This LMI condition is then transformed into an optimal-control condition, which has a useful interpretation. The results are also generalized to output-feedback and decentralized control cases. The efficacy of this work is demonstrated by designing fault-tolerant speed governors for a power system. The results developed here can be extended to more general types of faults, where each fault can possibly affect all state-space matrices of the system.**

## I. Introduction

Modern control systems can malfunction due to possible faults and failures in actuators, sensors or other components. To deal with this issue, the fault-tolerant controller design has been an active research area for several years, which aims to design a controller guaranteeing a satisfactory performance for a given system under both normal and fault conditions [1], [2]. Early studies in this area were motivated by two airplane accidents in 1970s that could have been avoided using a fault-tolerant controller with a self-repairing capability to ensure safe landing in the event of severe faults [3]. Fault-tolerant control design is particularly important for safety-critical systems, such as aircraft, spacecraft, chemical plants and power networks, where a series of minor faults in the system can lead to a catastrophic failure [4], [5].

Fault-tolerant control systems can be classified as *passive* or *active* [6]. In the passive case, the controller is designed to be sufficiently robust to pre-specified faults so that no modification in the control process is needed after experiencing a fault. In the active case, some preliminary actions are first taken to detect and diagnose the fault [1], [7], and the controller is then reconfigured based on an offline or online strategy. For a more complete survey on passive and active controller designs, see [4], [8], [9].

Motivated by power networks and biological systems (see Subsection II-A for more details), the present paper considers the case that every faulty part can be detected and subsequently isolated, but the controller parameters are not updated to compensate for a fault. Several methods have been proposed in the literature to study this problem. The most classical technique is to regard a fault as an uncertainty and design a robust controller. The uncertainty region can be considered to be continuous (e.g. polytopic) or discrete; in either case robust control and simultaneous control theories provide useful tools to design a fault-tolerant controller [10], [11], [12], [13]. Among other existing techniques, the paper [14] designs a reliable controller for networked control systems under stochastic sensor and actuator faults and presents a sufficient condition to guarantee the exponentially mean square stability. The work [12] shows that, under mild detectability and stabilizability conditions, it is always possible to design a dynamic controller stabilizing the system under every single failure in the sensors or actuators. Necessary conditions are derived in [15] for the stability of a control system subject to any fixed number of sensor/actuator faults. The works [16] and [17] consider the case when some actuators are always functional, while every combination of the remaining actuators are allowed to fail. They design reliable controllers to guarantee satisfactory linear-quadratic and $H_\infty$ performances under the failure of any subset of susceptible actuators.

Many of the existing works, e.g. [12], [16], [17], assume that either *a few possible combinations* or *all possible combinations* of faults can occur. However, several practical problems do not fit into this framework, such as a power contingency problem that allows up to certain number of faults, say 2 or 3, happen simultaneously. To allow a more general setting, the present paper considers an $m$-actuator control system where each combination of the actuators can fail as long as the set of the remaining actuators includes one of the pre-specified critical subsets of $\{1, 2, ..., m\}$. The objective is to design a controller such that: (i) the closed-loop system remains stable under every permissible combination of faults and (ii) the stability of the control system is improved if any subset of faults is cleared in each possible faulty closed-loop system. Although this paper mainly deals with actuator faults, it can be easily generalized to other types of faults. In this work, a necessary and sufficient condition in the form of a linear matrix inequality (LMI) is derived for the existence of a fault-tolerant state-feedback controller satisfying the two above-mentioned properties. This condition is later transformed into an optimal-control condition, which has an interesting interpretation. The generalization to output feedback and decentralized control cases are also discussed.

The rest of the paper is organized as follows. In Section II,

The authors are with the Department of Control and Dynamical Systems, California Institute of Technology (emails: sojoudi@cds.caltech.edu, lavaei@cds.caltech.edu, murray@cds.caltech.edu).

978-1-4577-0079-8/11/$26.00 ©2011 AACC

the problem is motivated by power and biological systems, and then some illustrative examples are provided. The main results are given in Section III through four subsections. The results are clarified on a power system in Section IV. Finally, some concluding remarks are provided in Section V.

## II. Objective and Motivations

Consider a linear time-invariant (LTI) system $\mathcal{S}$ with the state-space representation

$$\begin{aligned}\dot{x}(t) &= Ax(t) + Bu(t),\\ y(t) &= Cx(t),\end{aligned}$$

where $x(t)$, $u(t)$ and $y(t)$ denote the state, input and output of the system, respectively. The system $\mathcal{S}$ under a given controller could malfunction in practice due to faults in the sensors, actuators or some components of the system, in which case the faulty part is often isolated from the control system. To mathematically capture most of the common faults, assume that the system $\mathcal{S}$ can be subject to $m$ independent faults $\{f_1, f_2, ..., f_m\}$, where each fault changes certain entries of $A$, $B$ and $C$ to zero. Multiple faults can occur simultaneously, but we assume that pre-specified combinations of faults cannot happen. The goal is to design an LTI controller for the system $\mathcal{S}$ such that the following two properties are satisfied:

P1) The closed-loop system remains stable under all permissible combinations of faults.

P2) The stability of the closed-loop system subject to every permissible set of faults is improved if any arbitrary subset of the existing faults is cleared.

### A. Motivation

In this section, we motivate the above-mentioned problem with some examples from power systems and biology.

**Power grids:** In a conventional power system, the required amount of power is generated via large generators and then delivered to consumers through transmission and distribution networks. Since there are more than enough generators, a *unit commitment* problem is solved periodically, on the order of days, to decide what generation units should stay on at any given time. Therefore, when a generator is determined to be in operation, it works for several hours. However, the current trend is to replace most of the conventional generators with small distributed generators relying on renewable resources, such as wind and solar energies. Due to inevitable environmental changes, these small generation units may not be able to stay on for several hours, and hence, they should be allowed to leave and join the network frequently. An important control question is how to design a decentralized controller—a local controller for each distributed generator—such that

- The parameters of the power system (such as frequency, bus voltages, etc.) remain stable if any combination of generators leave/join the network, provided there are a minimum number of generators online.
- The more generators are online, the better the power quality is.

It is evident that if the leaving/joining property of a generator is interpreted as experiencing/clearing a fault, the above power problem can be cast as the control problem under study here.

**Biology:** A biological system, at many levels of organization, consists of numerous distributed parts that cooperatively contribute to perform some function. Several interesting observations have been made in the literature about the robustness of biological systems, some of which are outlined below [18], [19]:

- About only 18% of the yeast genome consists of essential genes and the remaining ones are not required for growth in rich media. This means that if any unnecessary genes are deleted, the resulting strain is still viable on rich media.
- Proteins can tolerate thousands of amino acid changes.
- Metabolic networks can continue to live after removal of several chemical reactions or metabolic pathways.
- Gene regulation networks perform the same function after altering many gene interactions.

These observations imply that biological systems are sufficiently robust that they achieve their goals even after experiencing several faults/changes. In addition, it is known that the larger the number of duplicates a yeast gene has, the faster the gene evolves [19], which suggests that "the fewer faults, the better performance". As motivated by synthetic biology, whose objective is to build artificial biological systems, it is important to study how to design a control system with two properties: (i) it survives under an unknown set of faults with an exponential number of possibilities, (ii) it has a better performance in presence of fewer faults.

### B. Illustrative Examples

Two examples will be provided in the sequel, where Example 1 deals with faults in the system itself and Example 2 is concerned with faults in the actuators. These examples shed light on the importance of the two (stability and performance) properties P1 and P2 mentioned in the objective of this work.

*Example 1:* Consider the system $\dot{x}(t) = Ax(t) + Bu(t)$, where

- $A$ is a $4 \times 4$ matrix whose entries are sampled from a uniform distribution on the interval $[0, 2]$.
- $B$ is a $4 \times 3$ matrix whose entries are sampled from the standard normal distribution.
- $x(0)$ is a random variable with zero mean and the identity covariance matrix.

Let $G \in \mathbf{R}^{3\times 4}$ be designed in such a way that the controller $u(t) = Gx(t)$ minimizes the performance index

$$\mathcal{E}\left\{\int_0^\infty \left(x(t)^T x(t) + u(t)^T u(t)\right) dt\right\}. \qquad (1)$$

($\mathcal{E}\{\cdot\}$ represents the mathematical expectation operator.) Assume that the system $\dot{x}(t) = Ax(t)+Bu(t)$ can be subject to a fault, which makes the $(1, 1)$ and $(1, 2)$ entries of the open-loop matrix $A$ change to zero. Apply the optimal controller $u(t) = Gx(t)$ to both of the faultless and faulty systems, and denote the resulting performance values as $J_{\text{opt}}$ and $J_f$, respectively. We generated 1000 systems in the form of $\dot{x}(t) = Ax(t) + Bu(t)$ by randomly choosing the pair $(A, B)$ and observed the following: *for more than* 60% *of the systems, the closed-loop system subject to the fault was stable and, besides, the performance index $J_f$ was less than $J_{opt}$.* This implies that although the controller $u(t) = Gx(t)$ is optimal for the healthy system, there is a high likelihood that this controller works better for the faulty system. In the same line, one can design a system subject to multiple faults so that the control system has a better performance in presence of more faults. This phenomenon can turn into an undesirable property, because clearing a fault worsens the performance. The next example demonstrates this fact in more details.

*Example 2:* Consider the system $\dot{x}(t) = Ax(t) + Bu(t)$ with the state-space matrices

$$A = \begin{bmatrix} 2.0227 & 1.8592 & 5.0898 & 1.4987 & 3.5266 \\ 3.3674 & 1.1746 & 4.4604 & 5.7557 & 3.7338 \\ 4.2868 & 1.5336 & 5.1105 & 5.6965 & 5.1306 \\ 1.2209 & 5.6477 & 2.9707 & 4.5873 & 0.8194 \\ 3.9992 & 4.5601 & 2.8080 & 4.5864 & 3.9581 \end{bmatrix},$$

$$B = \begin{bmatrix} 0.8925 & 0.4626 & 0.1701 & 0.8925 \\ 0.5588 & 0.0205 & 0.1716 & 0.1335 \\ 0.7667 & 0.0685 & 0.8098 & 0.1701 \\ 0.1236 & 0.9371 & 0.1203 & 0.2527 \\ 0.7300 & 0.3687 & 0.3092 & 0.9688 \end{bmatrix}.$$

Note that these matrices are chosen at random. Design a controller $u(t) = Gx(t)$ for this system to minimize the performance index $\int_0^\infty \left(x(t)^T x(t) + u(t)^T u(t)\right) dt$. Denote the $i^{\text{th}}$ row of $G$ as $G_i$ and the $i^{\text{th}}$ entry of $u(t)$ as $u_i(t)$, for every $i \in \{1, 2, 3, 4\}$. Regard the controller $u(t) = Gx(t)$ as the composition of four sub-controllers $u_i(t) = G_i x(t)$, $i = 1, 2, 3, 4$, where the output of each sub-controller is applied to the system through an actuator that can fail to work. Assume that whenever an actuator is faulty, the corresponding sub-controller is isolated. Now, suppose that the control system initially experiences two faults at the third and forth actuators, and later the fault at the forth actuator is cleared. Interestingly, the closed-loop system maintains stability when both faults occur, but it becomes unstable when one of the faults is cleared. To avoid this undesirable behavior, the controller to be designed in this work is required to satisfy the property P2 given earlier, stating that *the stability of the closed-loop system subject to every permissible set of faults is improved if any subset of the existing faults is cleared.*

## III. Main Results

In the statement of the objective of this work, we assumed that each fault changes certain entries of $A, B, C$ to zero. However, in order to simplify the presentation, we develop the main results only for the specific case of actuator faults where each fault converts some columns of $B$ to zero. The results being presented here can be easily extended to the general case.

Assume that the system $\mathcal{S}$ is associated with $m$ separate actuators, implying that the input vector $u(t)$ and the matrix $B$ are decomposable as

$$u(t) = \begin{bmatrix} u_1(t)^T & u_2(t)^T & \cdots & u_m(t)^T \end{bmatrix}^T, \tag{2a}$$

$$B = \begin{bmatrix} B_1 & B_2 & \cdots & B_m \end{bmatrix}, \tag{2b}$$

where $u_i(t) \in \mathbf{R}^{r_i}$ and $B_i \in \mathbf{R}^{n \times r_i}$, for every $i \in \{1, 2, ..., m\}$. With no loss of generality, suppose that $m \geq 2$ and that $B_1, B_2, ..., B_m$ all have full column rank. Given some matrices $G_i \in \mathbf{R}^{r_i \times n}$, $i = 1, 2, ..., m$, consider the sub-controllers

$$u_i(t) = G_i x(t), \quad i = 1, 2, ..., m,$$

where the output of each sub-controller is applied to the system via an actuator that can fail to work properly. In the next two subsections, the goal is to design $(G_1, G_2, ..., G_m)$ such that the properties P1 and P2 are satisfied. The results will be later extended to the output feedback and decentralized cases.

### A. Totally Fault-Tolerant Controllers

A controller $(G_1, G_2, ..., G_m)$ satisfying the properties P1 and P2 is said to be *totally fault tolerant* if the only impermissible set of faults is the entire set $\{1, 2, ..., m\}$. In other words, any combination of the sub-controllers can be isolated as long as there is at least one sub-controller online (operational). To formalize the objective precisely, we need to define some notion of stability improvement.

*Definition 1:* Given two $n^{\text{th}}$-order autonomous systems $\mathbf{S}_1$ and $\mathbf{S}_2$ described as $\dot{x}(t) = \mathbf{A}_1 x(t)$ and $\dot{x}(t) = \mathbf{A}_2 x(t)$, respectively, it is said that $\mathbf{S}_1$ *is more stable than* $\mathbf{S}_2$ *with respect to a Lyapunov (symmetric, positive-definite) matrix* $P \in \mathbf{R}^{n \times n}$ if

$$P\mathbf{A}_1 + \mathbf{A}_1^T P \leq P\mathbf{A}_2 + \mathbf{A}_2^T P < 0.$$

In other words, $\mathbf{S}_1$ is more stable than $\mathbf{S}_2$ with respect to $P$ if the Lyapunov function $x(t)^T P x(t)$ decreases faster along the trajectories of $\mathbf{S}_1$ than along the trajectories of $\mathbf{S}_2$.

Order (arbitrarily) all nonempty subsets of $\{1, 2, ..., m\}$ and denote them as $I_1, I_2, ..., I_p$, where $p := 2^m - 1$. For every $i \in \{1, 2, ..., m\}$ and $j \in \{1, 2, ..., p\}$, define $\alpha_i^j$ as 1 if $i \in I_j$ and 0 otherwise. Given some matrices $G_i \in \mathbf{R}^{r_i \times n}$, $i = 1, 2, ..., m$, define

$$\mathbf{G} := \begin{bmatrix} G_1 & G_2 & \cdots & G_m \end{bmatrix},$$

$$\mathbf{G}_j := \begin{bmatrix} \alpha_1^j G_1 & \alpha_2^j G_2 & \cdots & \alpha_m^j G_m \end{bmatrix}, \quad j = 1, 2, ..., p.$$

Throughout this subsection, $u(t) = \mathbf{G}x(t)$ is the ideal controller designed for $\mathcal{S}$, while $u(t) = \mathbf{G}_j x(t)$ is a faulty controller obtained from $u(t) = \mathbf{G}x(t)$ by zeroing all inputs $u_i(t)$ such that $i \notin I_j$. The objective is to address the following problem.

*Problem 1:* Design a controller $\mathbf{G}$ and a Lyapunov matrix $P$ associated with it such that the two properties given below are satisfied:

i) The system $\mathcal{S}$ is stable under all controllers $u(t) = \mathbf{G}_j x(t)$, $j = 1, 2, ..., p$.

ii) For every two distinct indices $j_1, j_2 \in \{1, 2, ..., p\}$, if $I_{j_2}$ is a subset of $I_{j_1}$, then the system $\mathcal{S}$ under $u(t) = \mathbf{G}_{j_1} x(t)$ is more stable than the system $\mathcal{S}$ under $u(t) = \mathbf{G}_{j_2} x(t)$ with respect to $P$.

*Remark 1:* To understand the usefulness of the properties given in Problem 1, consider a solution $(G_1, ..., G_m)$ to this problem and assume that the system $\mathcal{S}$ starts working under a nonempty subset of the sub-controllers $u_i(t) = G_i x(t),\ i = 1, 2, ..., m$. Due to Properties (i) and (ii), the closed-loop system is stable and, in addition, the signal $x(t)^T P x(t)$ converges monotonically to zero. Now, if any combination of offline (faulty) sub-controllers joins the control process, the signal $x(t)^T P x(t)$ still continues decreasing (possibly faster than before) without any transient overshoot. In other words, letting more sub-controllers join the control system asynchronously and at any given time does not slow down the state regulation of the system.

In what follows, we provide a necessary and sufficient condition under which Problem 1 has a solution.

*Theorem 1:* Problem 1 has a solution if and only if there exist symmetric matrices $H_i \in \mathbf{R}^{r_i \times r_i}$, $i = 1, 2, ..., m$, and $M \in \mathbf{R}^{n \times n}$ such that the LMI problem

$$AM + MA^T < 2B_i H_i B_i^T, \quad i = 1, 2, ..., m, \tag{3a}$$

$$H_i \geq 0, \quad i = 1, 2, ..., m, \tag{3b}$$

$$M > 0, \tag{3c}$$

is feasible. Moreover, in the case when this LMI problem has a feasible solution $(H_1, ..., H_m, M)$, a solution to Problem 1 is as follows:

$$P = M^{-1}, \quad G_i = -H_i B_i^T M^{-1}, \quad i = 1, 2, ..., m. \tag{4}$$

*Proof of Sufficiency:* Take the Lyapunov matrix $P$ as $M^{-1}$ and the controller $\mathbf{G}$ as the one given in (4), for some matrices $H_i \in \mathbf{R}^{r_i \times r_i}$, $i = 1, 2, ..., m$, and $M \in \mathbf{R}^{n \times n}$ satisfying the LMI problem (3). In order to show that Property (i) given in Problem 1 holds, consider an index $j \in \{1, 2, ..., p\}$ and write

$$\begin{aligned}(A + B\mathbf{G}_j)P^{-1} + P^{-1}(A + B\mathbf{G}_j)^T &= AP^{-1} + P^{-1}A^T \\ &+ \sum_{i=1}^{m} \alpha_i^j B_i G_i P^{-1} + \sum_{i=1}^{m} \alpha_i^j (B_i G_i P^{-1})^T \\ &= AP^{-1} + P^{-1}A^T - 2\sum_{i=1}^{m} \alpha_i^j B_i H_i B_i^T\end{aligned}$$

Since $I_j$ is assumed to be nonempty, there exists an index $k \in \{1, 2, ..., m\}$ such that $\alpha_k^j \neq 0$. Hence, (3a) and (3b) yield that

$$\begin{aligned}(A + B\mathbf{G}_j)P^{-1} + P^{-1}(A + B\mathbf{G}_j)^T &\leq AP^{-1} + P^{-1}A^T \\ &-2B_k H_k B_k^T < 0\end{aligned}$$

The above inequality, together with the positive definiteness of $P$, proves that $\mathcal{S}$ is stable under the controller $u(t) = \mathbf{G}_j x(t)$. In order to show the validity of Property (ii) in Problem 1, consider two distinct indices $j_1, j_2 \in \{1, 2, ..., p\}$ such that $I_{j_2}$ is a subset of $I_{j_1}$. It can be easily justified that it is enough to only study the case $|I_{j_1}| - |I_{j_2}| = 1$. Let $l$ be an index in the set $\{1, 2, ..., m\}$ such that $I_{j_1} = I_{j_2} \cup \{l\}$. One can write:

$$\begin{aligned}&\Big((A + B\mathbf{G}_{j_1})P^{-1} + P^{-1}(A + B\mathbf{G}_{j_1})^T\Big) - \\ &\quad \Big((A + B\mathbf{G}_{j_2})P^{-1} + P^{-1}(A + B\mathbf{G}_{j_2})^T\Big) = \\ &\qquad B_l G_l P^{-1} + (B_l G_l P^{-1})^T = -2B_l H_l B_l^T \leq 0.\end{aligned} \tag{5}$$

By Definition 1, this implies that the system $\mathcal{S}$ under $u(t) = \mathbf{G}_{j_1} x(t)$ is more stable than the system $\mathcal{S}$ under $u(t) = \mathbf{G}_{j_2} x(t)$ with respect to $P$.

*Proof of Necessity:* Assume that Problem 1 has a feasible solution $(\mathbf{G}, P)$. The goal is to show that the LMI problem (3) is feasible. To this end, consider an arbitrary number $i \in \{1, 2, ..., m\}$. There exist three indices $j_1, j_2, j_3$ such that

$$i \notin I_{j_2}, \quad I_{j_1} = I_{j_2} \cup \{i\}, \quad I_{j_3} = \{i\}. \tag{6}$$

Property (ii) of Problem 1 yields that

$$\begin{aligned}&\Big((A + B\mathbf{G}_{j_1})P^{-1} + P^{-1}(A + B\mathbf{G}_{j_1})^T\Big) - \\ &\quad \Big((A + B\mathbf{G}_{j_2})P^{-1} + P^{-1}(A + B\mathbf{G}_{j_2})^T\Big) = \\ &\qquad B_i G_i P^{-1} + (B_i G_i P^{-1})^T \leq 0.\end{aligned} \tag{7}$$

or equivalently

$$B_i B_i^T + P^{-1} G_i^T G_i P^{-1} \leq \left(B_i - P^{-1} G_i^T\right)\left(B_i - P^{-1} G_i^T\right)^T$$

There exists a matrix $E \in \mathbf{R}^{n \times (n - r_i)}$ with orthogonal columns such that $\left(B_i - P^{-1} G_i^T\right)^T E = 0$. Pre-multiplying and post-multiplying the above inequality by $E^T$ and $E$, respectively, gives rise to

$$B_i^T E = 0, \quad G_i P^{-1} E = 0.$$

Since $B_i$ has full column rank, this simply implies that every row of $G_i P^{-1}$ is in the row space of $B_i^T$. Hence, there exists a matrix $Y_i$ such that $G_i P^{-1} = -Y_i B_i^T$. Now, it follows from (7) that

$$-B_i(Y_i + Y_i^T)B_i^T \leq 0.$$

Due to the matrix $B_i$ having full column rank, the above inequality is tantamount to $H_i := \frac{1}{2}(Y_i + Y_i^T) \geq 0$ or equation (3b). On the other hand, the stability of $\mathcal{S}$ under the controller $u(t) = G_{j_3} x(t)$ (see Property (i) of Problem 1) can be cast as the inequality (3a) for $M := P^{-1}$. This completes the proof of this part. ■

Theorem 1 provides a necessary and sufficient LMI condition for the solvability of Problem 1. It is noteworthy that although there are an exponential number of fault combinations, the size of the given LMI problem is a polynomial in $m$ and $n$. Whenever Problem 1 has at least one solution, it must have an infinite number of solutions (see Remark 2). However, the set of all solutions to Problem 1 can be characterized using the argument made in the proof of necessity. This is carried out below.

*Corollary 1:* A given pair $(\mathbf{G}, P)$ is a solution to Problem 1 if and only if there exist matrices $Y_1, Y_2, ..., Y_m$ and symmetric matrices $H_1, H_2, ..., H_m$ of appropriate dimensions such that the LMI problem (3) is satisfied for $(H_1, H_2, ..., H_n, M)$, where $M = P^{-1}$, $H_i = \frac{1}{2}(Y_i + Y_i^T)$ and $G_i = -Y_i B_i^T M^{-1}$, $\forall i \in \{1, 2, ..., m\}$.

Although the LMI condition given in Theorem 1 can be efficiently handled numerically, its purely algebraic structure is an obstacle to gaining insight into the solvability of Problem 1 and the properties of the controller $\mathbf{G}$. We provide an equivalent condition below, which can be more easily interpreted.

*Theorem 2:* Problem 1 has a solution if and only if there exist positive definite matrices $Q_1, ..., Q_m, R_1, ..., R_m, P$ such that for every initial state $x_0 \in \mathbf{R}^n$, the optimal control problem

$$\begin{aligned} &\min_{u_i(t)} \int_0^\infty \Big( x(t)^T Q_i x(t) + u_i(t) R_i u_i(t) \Big) dt \\ &\quad \text{subject to} \quad \dot{x}(t) = Ax(t) + B_i u_i(t), \quad x(0) = x_0, \end{aligned} \tag{8}$$

has the same optimal value $x_0^T P x_0$ for all numbers $i \in \{1, 2, ..., m\}$.

*Sketch of Proof:* By Theorem 1, Problem 1 has a solution if and only if the LMI problem (3) is feasible. On the other hand, the inequality sign in the constraint (3b) of this LMI can be replaced by the strict inequality sign. In fact, if $(H_1, ..., H_m, M)$ is a feasible point of the LMI problem (3), $(H_1 + \varepsilon I, ..., H_m + \varepsilon I, M)$ is a strictly feasible solution of this LMI for every $\varepsilon > 0$. As a result, Problem 1 has a solution if and only if there exist matrices $W_1, ..., W_m, H_1, ..., H_m, M$ such that

$$AM + MA^T + W_i = 2B_i H_i B_i^T, \quad i = 1, 2, ..., m, \tag{9a}$$

$$W_1, ..., W_m, H_1, ..., H_m, M > 0. \tag{9b}$$

Given $i \in \{1, 2, ..., m\}$, the equality (9a) can be rearranged as

$$\begin{aligned} M^{-1}A + A^T M^{-1} + M^{-1} W_i M^{-1} \\ - M^{-1} B_i (2H_i) B_i^T M^{-1} = 0. \end{aligned}$$

By regarding the above equation as an algebraic Riccati equation, it can be argued that $(M, W_i, H_i)$ satisfies this equation if and only if the optimal control problem

$$\begin{aligned} &\min_{u_i(t)} \int_0^\infty \Big( x(t)^T (M^{-1} W_i M^{-1}) x(t) + \frac{1}{2} u_i(t) H_i^{-1} u_i(t) \Big) dt \\ &\quad \text{subject to} \quad \dot{x}(t) = Ax(t) + B_i u_i(t), \quad x(0) = x_0, \end{aligned}$$

has the optimal value $x_0^T M^{-1} x_0$. To complete the proof of Theorem 2, it is enough to define $P := M^{-1}$, $Q_i := M^{-1} W_i M^{-1}$ and $R_i := \frac{1}{2} H_i^{-1}$. ■

Let $u_i(t) = -H_i B_i^T M^{-1} x(t)$, $i = 1, 2, ..., m$, be a totally fault-tolerant controller, where $(H_1, ..., H_m, M)$ satisfies the LMI problem of Theorem 1. Notice that the optimal controller minimizing the performance index (8) is given by $u_i(t) = -R_i^{-1} B_i^T P x(t) = -2H_i B_i^T M^{-1} x(t)$, $i = 1, 2, ..., m$. It is a direct consequence of Remark 3 (given later in the paper) that this set of optimal sub-controllers also constitutes a totally fault-tolerant controller with respect to $P$. In other words, there exists at least one totally fault-tolerant controller if and only if there exists a set of sub-controllers such that each sub-controller is optimal with respect to some linear quadratic performance index and that they all lead to the same optimal performance value.

We make some important remarks in the sequel.

*Remark 2:* Problem 1 is either infeasible or has an infinite number of solutions. One can exploit this degree of freedom (associated with the non-uniqueness of the solution) and impose extra constraints to satisfy more specifications. For instance, note that if $(H_1, ..., H_m, M)$ is a feasible solution of the LMI problem (3), $(H_1 + \mu I, ..., H_m + \mu I, M)$ and $(\mu H_1, ..., \mu H_m, \mu M)$ are both solutions of the same LMI, for every $\mu > 0$. Now, notice that $G_i = -(H_i + \mu I) B_i^T M^{-1}$, $i = 1, 2, ..., m$, is also a totally fault-tolerant controller and pushing $\mu$ towards infinity makes it high gain. One can minimize $\sum_{i=1}^m \|H_i\|$ subject to the LMI problem (3) as well as the redundant constraint $M \succeq I$ to avoid designing a high-gain controller (due to the homogeneity of the LMI (3), the new constraint $M \succeq I$ does not affect the feasibility of the problem).

*Remark 3:* Given an arbitrary feasible point $(H_1, ..., H_m, M)$ of the LMI problem (3), it can be verified that the infinite set

$$\big\{ (\mu H_1, ..., \mu H_m, M) \bigm| \mu \geq 1 \big\}$$

is contained in the feasibility region of this LMI problem. It follows from this observation and Corollary 1 that if $(\mathbf{G}, P)$ is a solution to Problem 1, then there are an infinite number of totally fault-tolerant controllers with respect to $P$, which are given by the set

$$\big\{ u(t) = \mu \mathbf{G} x(t) \bigm| \mu \geq 1 \big\}.$$

*Remark 4:* The stability improvement after clearing every subset of faults is measured with respect to a Lyapunov matrix $P$. However, an arbitrary feasible solution of the LMI problem (3) might not lead to a desirable Lyapunov matrix $P = M^{-1}$ for performance evaluation. To remedy this issue, one can either fix $M$ (or $P$) at the beginning or impose certain constraints on its entries so that $x^T M^{-1} x$ becomes an acceptable measure of performance for the corresponding application.

### *B. Partially Fault-Tolerant Controllers*

In a totally fault-tolerant controller, every sub-controller must be able to stabilize the system if all other sub-controllers fail. This at least requires the stabilizability of all pairs $(A, B_1), ..., (A, B_m)$. To make the problem more pragmatic, consider some distinct sets $I_{g_1}, I_{g_2}, ..., I_{g_h} \subsetneqq \{1, 2, ..., m\}$. We assume that every arbitrary combination of faults can occur as long as the set of the healthy actuators contains at least one of the sets $I_{g_1}, I_{g_2}, ..., I_{g_h}$. In other words, these $h$ sets determine some critical control configurations such that at least one of them must be present in the overall faulty control structure. If these sets are considered as

$\{1\}, \{2,\}, ..., \{m\}$, the associated controller will be a totally fault-tolerant controller; however, the controller corresponding to some general sets $I_{g_1}, I_{g_2}, ..., I_{g_h}$ can be regarded as a partially fault-tolerant controller. To let every actuator have the possibility of failure, assume that the intersection of the sets $I_{g_1}, I_{g_2}, ..., I_{g_h}$ is empty. The objective of this subsection is to address a general version of Problem 1, as given below.

*Problem 2:* Design a controller $\mathbf{G}$ and a Lyapunov matrix $P$ associated with it such that the following two properties are satisfied:

i) The system $\mathcal{S}$ is stable under the controller $u(t) = \mathbf{G}_j x(t)$ for every $j \in \{1,2,...,p\}$ such that $I_j$ includes at least one of the sets $I_{g_1}, I_{g_2}, ..., I_{g_h}$.

ii) For every two distinct indices $j_1, j_2 \in \{1,2,...,p\}$, if $I_{j_2} \subset I_{j_1}$ and $I_{j_2}$ includes at least one of the sets $I_{g_1}, I_{g_2}, ..., I_{g_h}$, then the system $\mathcal{S}$ under $u(t) = \mathbf{G}_{j_1} x(t)$ is more stable than the system $\mathcal{S}$ under $u(t) = \mathbf{G}_{j_2} x(t)$ with respect to $P$.

Theorem 1, Corollary 1 and Theorem 2 that were derived for Problem 1 can all be extended to tackle Problem 2. In the sequel, we explain this generalization only for Theorem 1.

*Theorem 3:* Problem 2 has a feasible solution if and only if there exist symmetric matrices $H_i \in \mathbf{R}^{r_i \times r_i}$, $i = 1,2,...,m$, and $M \in \mathbf{R}^{n \times n}$ such that the LMI problem

$$AM + MA^T < 2\sum_{i=1}^{m} \alpha_i^{g_j} B_i H_i B_i^T, \quad j = 1,2,...,h, \tag{10a}$$

$$H_i \geq 0, \quad i = 1,2,...,m, \tag{10b}$$

$$M > 0, \tag{10c}$$

is feasible. Moreover, in the case when this LMI problem has a feasible solution $(H_1, ..., H_m, M)$, a solution to Problem 2 is as follows:

$$P = M^{-1}, \quad G_i = -H_i B_i^T M^{-1}, \quad i = 1,2,...,m. \tag{11}$$

*Sketch of Proof:* Given an index $i \in \{1,2,...,m\}$, there is a set $I_{g_k}$, $k \in \{1,2,...,h\}$, which does not contain $\{i\}$ (because the intersection of the sets $I_{g_1}, I_{g_2}, ..., I_{g_h}$ is empty). Now, one can follow the proof of necessity for Theorem 1 with the only modification that the sets $I_{j_1}$, $I_{j_2}$ and $I_{j_3}$ should be taken as

$$I_{j_1} = I_{g_k} \cup \{i\}, \quad I_{j_2} = I_{g_k}, \quad I_{j_3} = I_{g_k},$$

as opposed to the ones given in (6). ■

### C. Output-Feedback Fault-Tolerant Controllers

In this and the next subsections, we present some important generalizations for designing only totally fault-tolerant controllers, as partially fault-tolerant controllers can be tackled similarly. So far, it was assumed that the state of the system $\mathcal{S}$ is available to all sub-controllers. Now, assume that the sub-controllers have access to $y(t) = Cx(t)$ rather than $x(t)$ directly. Given $i \in \{1,2,...,m\}$, let $z_i(t) = f_i(y(t), u(t); t)$ denote a Luenberger observer for the $i^{\text{th}}$ sub-controller, meaning that $z_i(t) - x(t) \to 0$ as $t$ goes to infinity. Note that the observers $f_1(y(t), u(t); t), ..., f_m(y(t), u(t); t)$ may not be distinct, but each sub-controller can potentially have its own observer to increase the redundancy in the control mechanism.

Assume that $(G_1, G_2, ..., G_m)$ and $P$ is a solution to Problem 1, and consider the output feedback controllers $u_i(t) = G_i f_i(y(t), u(t); t)$, $i = 1,2,...,m$. Since the estimation error of every observer only depends on the observer gain as well as the parameters $(A, C)$, it is easy to verify that the separation principle holds as far as the stability is concerned. Hence, every nonempty combination of these output-feedback sub-controllers can stabilize the system. On the other hand, if the observers are made sufficiently fast, then the statement *"the more sub-controllers online, the better stability"* will be mostly true.

### D. Decentralized Fault-Tolerant Controllers

In this subsection, the objective is to design *decentralized* fault-tolerant controllers for interconnected systems. As before, we only consider totally fault-tolerant controllers here as the generalization to partially fault-tolerant controllers is straightforward. To this end, assume that the LTI system $\mathcal{S}$ is composed of $m$ interacting subsystems $S_1, S_2, ..., S_m$. Suppose that the dynamics of $S_i$, $i = 1, ..., m$, is governed by

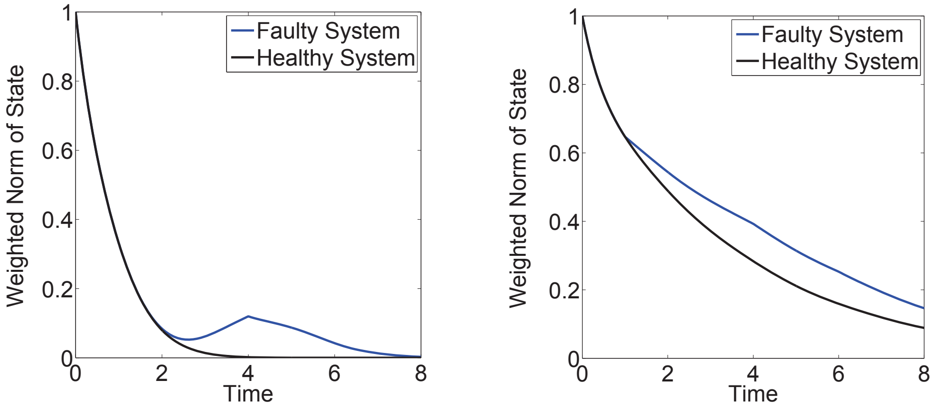
$$\begin{aligned} \dot{x}_i(t) &= \sum_{j=1}^{m} A_{ij} x_j(t) + B_{ii} u_i(t), \\ y_i(t) &= C_i x_i(t), \end{aligned}$$

where $x_i(t) \in \mathbf{R}^{n_i}$, $u_i(t) \in \mathbf{R}^{r_i}$ and $y_i(t) \in \mathbf{R}^{\bar{r}_i}$ denote the state, input and output of the $i^{\text{th}}$ subsystem, respectively. Define $A$ as a matrix whose $(i,j)$ block entry is equal to $A_{ij}$ for every $i, j \in \{1,2,...,m\}$. Moreover, define $B$ as a block diagonal matrix with the block diagonal entries $B_{11}, ..., B_{mm}$. Denote the $i^{\text{th}}$ block column of $B$ as $B_i \in \mathbf{R}^{n \times r_i}$ for every $i \in \{1,2,...,m\}$ (note that $n = n_1 + \cdots + n_m$).

We aim to design $m$ local controllers (sub-controllers) $u_i(t) = G_i x_i(t)$ to achieve the stability and performance goals stated in Section III-A. To address this problem, consider the LMI condition (3) subject to the extra constraint that $M$ is a block diagonal matrix whose $i^{\text{th}}$ block entry is of dimension $n_i \times n_i$ for every $i \in \{1,2,...,m\}$. This new LMI condition is a sufficient condition for designing a totally fault-tolerant decentralized controller with local controllers $u_i(t) = G_i x_i(t)$, $i = 1, ..., m$. Note that the necessity of the LMI condition breaks down in the decentralized case, which is related to a well-known open problem in the decentralized control theory: *checking the existence of a stabilizing static decentralized controller in polynomial time*. In some special cases, e.g. $r_i = n_i$ and $\det\{G_i\} \neq 0$, $\forall i \in \{1,2,...,m\}$, the proposed LMI condition turns into a necessary and sufficient condition.

Now, assume that the local state $x_i(t)$ is not available for use in the local controller $u_i(t) = G_i x_i(t)$. Notice that the subsystem $S_i$, $i \in \{1,2,...,m\}$, receives the aggregate signal

$$\sum_{j \in \{1,...,m\} \backslash \{i\}} A_{ij} x_j(t)$$



(a) (b)

Fig. 1. (a) The power system under an LQR optimal controller; (b) The power system under a totally fault-tolerant controller.

from the other subsystems of $\mathcal{S}$. If this signal is measurable, one can implement a local Luenberger observer for the $i^{\text{th}}$ subsystem to estimate $x_i(t)$ (under the mild condition of the observability of $(A_{ii}, C_i)$). In this case, a totally/partially fault-tolerant output-feedback decentralized controller can be designed based on the discussion given in the preceding subsection (in other words, a modified separation principle holds).

## IV. Simulation

It is known that the frequency of a power grid must be kept constant, partially because synchronous generators, induction motors and transformers could cause undesirable behaviors under either a fluctuation or a drop in the frequency [20]. This problem has long been studied in the context of frequency synchronization, where the goal is to control the rotor parts of a group of synchronous machines, connected to each other via a network of transmission lines, so that the network frequency reaches a constant value asymptotically. To this end, one can write the swing equation for each generator $i \in \{1, 2, ..., m\}$ as follows:

$$\gamma_i \ddot{\delta}_i(t) = P_{m_i}(t) - P_{e_i}(t), \tag{12}$$

where

- $\gamma_i$ is a constant coefficient,
- $\delta_i$ is the angular displacement of the $i^{\text{th}}$ generator's rotor.
- $P_{m_i}$ is the mechanical power applied to the $i^{\text{th}}$ generator's rotor.
- $P_{e_i}$ is the electrical power transferred from the $i^{\text{th}}$ generator's stator to the rest of the network.

For simplicity and with no loss of generality, we study the swing equation (12) alone without considering the differential equations for other parameters of the network, such as voltages. Assume that the goal is to design a sub-controller for each generator $i \in \{1, 2, ..., m\}$ to control $P_{m_i}$ in such a way that the nonlinear swing equation becomes locally stable around a given nominal frequency. For this purpose, a totally fault-tolerant controller will be designed here.

As an example, consider a network of three generators, where every two generators are connected to each other via a transmission line. To design three speed governors (sub-controllers) for the generators, we write the swing equation for each rotor. The overall interconnected system, after linearization and for a particular operating point, will be

$$\begin{bmatrix} \dot{x}_1(t) \\ \dot{x}_2(t) \\ \dot{x}_3(t) \end{bmatrix} = A \begin{bmatrix} x_1(t) \\ x_2(t) \\ x_3(t) \end{bmatrix} + B \begin{bmatrix} P_{m_1}(t) \\ P_{m_2}(t) \\ P_{m_3}(t) \end{bmatrix}$$

where $x_i(t) = \begin{bmatrix} \delta_i(t) & \dot{\delta}_i(t) \end{bmatrix}^T$, $i = 1, 2, 3$,

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ -5 & -0.1 & 2 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & -3.5 & -0.15 & 2.5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & \frac{5}{3} & 0 & -\frac{8}{3} & -\frac{5}{3} \end{bmatrix},$$

and

$$B = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad x(0) = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$

Since the power system is observable from the output of every generator, we design three full-state sub-controllers with the understanding that their implementation in practice is based on state observers, as explained in Section III-C (see the recent work [20] for the possibility of reducing the orders of the observers). By solving the LMI given in Theorem 1, a solution to Problem 1 will be obtained as the one given in (13). Let $(G_1^{\text{opt}}, G_2^{\text{opt}}, G_3^{\text{opt}})$ be an optimal controller obtained by minimizing the performance

$$\begin{aligned}
G_1 &= \left[\begin{array}{cccccc} -0.0053 & -0.0991 & -0.0183 & -0.1327 & -0.0366 & -0.1999 \end{array}\right], \\
G_2 &= \left[\begin{array}{cccccc} -0.0091 & -0.1327 & -0.0398 & -0.3040 & -0.0736 & -0.4068 \end{array}\right], \\
G_3 &= \left[\begin{array}{cccccc} -0.0140 & -0.1999 & -0.0572 & -0.4068 & -0.1133 & -0.6465 \end{array}\right], \\
P &= \left[\begin{array}{cccccc} 15.3622 & 0.5286 & -5.5384 & 0.9051 & -6.8092 & 1.4047 \\ 0.5286 & 9.9093 & 1.8267 & 13.2721 & 3.6618 & 19.9895 \\ -5.5384 & 1.8267 & 13.1163 & 3.9809 & -2.4162 & 5.7219 \\ 0.9051 & 13.2721 & 3.9809 & 30.4040 & 7.3622 & 40.6828 \\ -6.8092 & 3.6618 & -2.4162 & 7.3622 & 16.8408 & 11.3304 \\ 1.4047 & 19.9895 & 5.7219 & 40.6828 & 11.3304 & 64.6594 \end{array}\right].
\end{aligned} \tag{13}$$

index $\int_0^\infty \left(x(t)^T x(t) + u(t)^T u(t)\right) dt$, associated with the Lyapunov function $P^{\text{opt}}$. To demonstrate the superior properties of the controller $(G_1, G_2, G_3)$, we analyze the performance of the power system under both $(G_1, G_2, G_3)$ and $(G_1^{\text{opt}}, G_2^{\text{opt}}, G_3^{\text{opt}})$ in the following "fault" situation:

- At time $t = 0$, all speed governors start working.
- At time $t = 1$, the speed governors of the second and third generators both stop working.
- At time $t = 4$, the speed governor of the second generator resumes its operation.
- At time $t = 6$, the speed governor of the third generator resumes its operation.

The signal $x(t)^T P^{\text{opt}} x(t)$ (after normalizing its maximum to 1) is plotted in Figure 1(a) for the power system under $(G_1^{\text{opt}}, G_2^{\text{opt}}, G_3^{\text{opt}})$ in both "no fault" and "fault" situations. It can be observed that although the norm of the state decreases monotonically in the absence of faults, it has an unwanted overshoot in presence of faults. On the other hand, the signal $x(t)^T P x(t)$ (after a normalization) is plotted in Figure 1(b) for the power system under $(G_1, G_2, G_3)$. It can be seen that when the first two faults occur simultaneously, the state regulation rate decreases a little, but the convergence to zero is still monotonic; besides, the rate increases after clearing each fault, meaning that clearing faults improves the performance.

## V. Conclusions

This paper is concerned with the fault-tolerant control of a multi-actuator linear time-invariant system, where multiple independent faults can occur in the actuators. Motivated by both biological and electric power systems, the objective is to design a controller for the system such that the closed-loop system satisfies two properties: (i) stability under all permissible sets of faults (some combinations of faults are assumed not to happen), (ii) better state regulation after clearing an arbitrary subset of faults from every admissible set of faults. It is shown that such a fault-tolerant state-feedback controller exists if and only if a linear matrix inequality (LMI) problem is feasible. An equivalent optimal-control condition is then derived based on this LMI condition. The results are also generalized to output-feedback and decentralized cases.

## References

[1] L. H. Chiang, E. L. Russell and R. D. Braatz, "Fault detection and diagnosis in industrial systems," *London, UK: Springer*, 2001.

[2] M. Blanke, M. Kinnaert, J. Lunze and M. Staroswiecki, "Diagnosis and fault-tolerant control," *Berlin, Germany: Springer*, 2006.

[3] M. Steinberg, "Historical overview of research in reconfigurable flight control," *Proceedings of the Institution of Mechanical Engineers, Part G: Journal of Aerospace Engineering*, vol. 219, no. 4, pp. 263-275, 2005.

[4] R. J. Patton, " Fault-tolerant control: The 1997 situation," in *Proceedings of the 3rd IFAC symposium on fault detection, supervision and safety for technical processes*, 1997.

[5] Y. Kobayashi, M. Ikeda and Y. Fujisaki, "Stability of large space structures preserved under failures of local controllers," *IEEE Transactions on Automatic Control*, vol. 52, no. 2, pp. 318-322, 2007.

[6] M. Staroswiecki, D. Berdjag, B. Jiang and K. Zhang, "PACT : a PAssive / ACTive approach to fault tolerant stability under actuator outages," in *Proceedings of the 48th IEEE Conference on Decision and Control Conference*, Shanghai, china, 2009.

[7] F. Caliskan and I. Genc, "A robust fault detection and isolation method in load frequency control loops," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1756-1767, 2008.

[8] J. Jiang, "Fault-tolerant control systems—an introductory overview," *Acta Automatica Sinica*, vol. 31, no. 1, pp. 161-174, 2005.

[9] Y. Zhang and J. Jiang, "Bibliographical review on reconfigurable fault-tolerant control systems," *Annual Reviews in Control*, vol. 32, no. 2, pp. 229-252, 2008.

[10] F. Liao, J. L. Wang and G. H. Yang, "Reliable robust flight tracking control: an LMI approach," *IEEE Transactions on Control Systems Technology*, vol. 10, no. 1, pp. 76-89, 2002.

[11] J. Lavaei and A. G. Aghdam, "Robust stability of LTI systems over semi-algebraic sets using sum-of-squares matrix polynomials," *IEEE Transactions on Automatic Control*, vol. 53, no. 1, pp. 417-423, 2008.

[12] J. Stoustrup and V. D. Blondel, "Fault tolerant control: a simultaneous stabilization result," *IEEE Transactions on Automatic Control*, vol. 49, no. 2, pp. 305-310, 2004.

[13] J. Lavaei and A. G. Aghdam, "Simultaneous LQ control of a set of LTI systems using constrained generalized sampled-data hold functions," *Automatica*, vol. 43, pp. 274-280, 2007.

[14] E. Tian, D. Yue and C. Peng, "Reliable control for networked control systems with probabilistic sensors and actuators faults," *IET Control Theory and Applications*, vol. 4, no. 8, pp. 1478-1488, 2010.

[15] A. N. Gundes, "Stability of feedback systems with sensor or actuator failures: analysis," *International Journal of Control*, vol. 56, no. 4, pp. 735-753, 1992.

[16] R. J. Veillette, J. V. Medanid and W. R. Perkins, "Design of reliable control systems," *IEEE Transactions on Automatic Control*, vol. 37, no. 3, pp. 290-304, 1992.

[17] R. J. Veillette, "Reliable linear-quadratic state-feedback control," *Automatica*, vol. 31, no. 1, pp. 137-143, 1995.

[18] A. Brady, K. Maxwell, N. Daniels and L. J. Cowen, "Fault tolerance in protein interaction networks: stable bipartite subgraphs and redundant pathways," *PLoS ONE*, vol. 4, no. 4, 2009.

[19] A. Wagner, "Distributed robustness versus redundancy as causes of mutational robustness," *BioEssays*, vol. 27, no. 2, pp. 176-188, 2005.

[20] J. Liu, B. H. Krogh and M. D. Ilić, "Robust control design for frequency regulation in power systems with high wind penetration," in *Proceedings of 2010 American Control Conference*, Baltimore, MD, 2010.