Available online at www.sciencedirect.com
ScienceDirect
automatica
Automatica 44 (2008) 53 – 62
www.elsevier.com/locate/automatica

Isolation and handling of actuator faults in nonlinear systems ☆

Prashant Mhaskar[a], Charles McFall[b], Adiwinata Gani[b], Panagiotis D. Christofides[b,*], James F. Davis[b]

[a]Department of Chemical Engineering, McMaster University, Hamilton, ON, Canada L8S 4L7
[b]Department of Chemical & Biomolecular Engineering, University of California, Los Angeles, CA 90095-1592, USA

Received 20 July 2006; received in revised form 7 May 2007; accepted 13 May 2007
Available online 13 August 2007

Abstract

This work considers the problem of control actuator fault detection and isolation and fault-tolerant control for a multi-input multi-output nonlinear system subject to constraints on the manipulated inputs and proposes a fault detection and isolation filter and controller reconfiguration design. The implementation of the fault detection and isolation filters and reconfiguration strategy are demonstrated via a chemical process example.

Keywords: Fault-tolerant control; Fault detection and isolation; Input constraints; Stability region; Lyapunov-based control

1. Introduction

The operation of chemical processes is characterized by the complexity of the individual units together with an intricate interconnection of these geographically distributed units via a network of material and energy streams, and control loops. The nonlinear behavior exhibited by most chemical processes, together with the presence of constraints on the operating conditions, modeling uncertainty and disturbances, and the lack of availability of state measurements has motivated several research results in the area of nonlinear process control focusing on these issues (see, e.g., El-Farra & Christofides, 2001, 2001; El-Farra, Mhaskar, & Christofides, 2005; Lin & Sontag, 1991; Mhaskar, El-Farra, & Christofides, 2004; Soroush, Valluri, & Mehranbod, 2005 and, for a review of results, Allgöwer & Doyle, 1997; Bequette, 1991; Christofides & El-Farra, 2005; Henson & Seborg, 1997 and the references therein). The development of the advanced control algorithms outlined above (alongside development in sensing, communicating and computing technologies) has led to extensive automation of plant operation. Increased automation, however, also makes the plant susceptible to faults (e.g., defects/malfunctions in process equipment, sensors and actuators, failures in the controllers or in the control loops), which, if not appropriately handled in the control system design, can potentially cause a host of undesired economic, environmental, and safety problems that seriously degrade the operating efficiency of the plant.

The above considerations provide a strong motivation for the development of advanced fault-tolerant controllers that account for system complexities such as nonlinearity, uncertainty and constraints and provide a mechanism for an efficient and timely response to enhance fault recovery. One of the prerequisites for implementing fault-tolerant control is the ability to detect and isolate the faults. Statistical and pattern recognition techniques for data analysis and interpretation (e.g., Aradhye, Bakshi, Davis, & Ahalt, 2004; Davis, Piovoso, Kosanovich, & Bakshi, 1999; Kresta, Macgregor, & Marlin, 1991; Negiz & Cinar, 1997; Nomikos & Macgregor, 1994; Rollins & Davis, 1992) use historical plant-data to construct indicators that identify deviations from normal operation to detect faults. The problem of using fundamental process models for the purpose of detecting faults has been studied extensively in the context of

☆ This paper was not presented at any IFAC meeting. This paper was recommended for publication in revised form by Associate Editor Michael Henson under the direction of Editor Frank Allgöwer. Financial support from the National Science Foundation, CTS-0529295, is gratefully acknowledged.
* Corresponding author. Tel.: +1 3107941015; fax: +1 310206 4107.
E-mail addresses: mhaskar@mcmaster.ca (P. Mhaskar), cmcfall@ucla.edu (C. McFall), agani@ucla.edu (A. Gani), pdc@ucla.edu (P.D. Christofides), jdavis@oit.ucla.edu (J.F. Davis).

doi:10.1016/j.automatica.2007.05.006

linear systems (e.g., Frank, 1990; Frank & Ding, 1997; Massoumnia, Verghese, & Wilsky, 1989; Mehranbod, Soroush, & Panjapornpon, 2005); and more recently, fundamental results in the context of nonlinear systems have been derived (e.g., DePersis & Isidori, 2001; Pisu, Serrani, You, & Jalics, 2006; Saberi, Stoorvogel, Sannuti, & Niemann, 2000).

Fault-tolerant control can be achieved, in one approach, via controller designs using enough actuators to withstand the failure of some of the control actuators (e.g., see Bonivento, Isidori, Marconi, & Paoli, 2004; Yang, Wang, & Soh, 2001) and the robustness of the active control configuration to such faults can be analyzed. Economic considerations (to save on unnecessary control action), however, dictate the use of only as many control loops as is required at a time. In such cases, faults in a control actuator cannot be handled via changing the control algorithm and necessitates control-loop reconfiguration (activating appropriate backup control actuators). Using these approaches, fault-tolerant control has been actively pursued in the context of aerospace engineering applications (see, e.g., Patton, 1997; Zhou & Frank, 1998). Recently it has also gained attention in the context of chemical process control; however, most available results are based on the assumption of a linear process description (e.g., Bao, Zhang, & Lee, 2003; Wu, 2004) and do not account for process nonlinearity, constraints and lack of state measurements.

Controller reconfiguration to achieve fault-tolerant control via switching to well-functioning control actuators makes the closed-loop system a hybrid system, since the closed-loop system exhibits discrete transitions between continuous modes of operations. While a large number of research works have focused on a diverse array of hybrid system problems (e.g., DeCarlo, Branicky, Pettersson, & Lennartson, 2000; El-Farra & Christofides, 2003b; El-Farra et al., 2005; Garcia-Onorio & Ydstie, 2004), the use of a hybrid system framework for the study of fault-tolerant control problems has received limited attention. Under the assumption of state feedback and knowledge of fault, in El-Farra, Gani, and Christofides (2005), a hybrid systems approach to fault-tolerant control was employed where upon occurrence of a fault, stability region-based reconfiguration is done to achieve fault-tolerant control and in Mhaskar, Gani, and Christofides (2006), performance and robustness considerations were incorporated in the fault-tolerant control structure. In Mhaskar et al. (2006) the problem of fault detection and fault-tolerant control for single input systems was considered and the problem of deciding which backup control configuration should be implemented to preserve closed–loop stability was addressed. In Mhaskar et al. (2006), however, only single input systems were considered which did not require isolating the fault in a given control configuration. In a multi-input system, where the faults can occur in any of the actuators, the inability to isolate which actuator has failed can negatively impact the selection of the backup control configuration, and if incorrectly chosen, may fail to preserve closed–loop stability (due to the fact that the faulty actuator may be a member of the backup control configuration).

Motivated by these considerations, this work considers the problem of implementing fault-tolerant control on a multi-input multi-output nonlinear system subject to faults in the control actuators and constraints on the manipulated inputs. The case where all the states of the system are measured is first considered. The state measurements and the model is used to design filters that essentially capture the difference between fault-free evolution and the observed evolution of the system to detect and isolate faults. In the event of a fault, a configuration is chosen that (1) does not use the failed control actuator, and (2) guarantees stability of the closed-loop system starting from the system state at the time of the failure. To be able to ascertain the second condition, Lyapunov-based controllers, which provide an explicit characterization of the closed-loop stability region, are used in designing the control laws for the individual control configurations. Next the problem where not all the system states are measured is considered. First, output-feedback controllers are designed that allow for an explicit characterization of the output-feedback stability region. The state estimates are employed in implementing the fault detection and isolation filters, and the reconfiguration rule. While this work focusses on the rigorous development of fault-detection and isolation filter designs for the state and output-feedback cases, other practical issues such as uncertainty, disturbances, measurement noise and sampling delays are investigated in the implementation of the fault detection and isolation filters and reconfiguration strategy on a chemical process example.

2. Preliminaries

Consider nonlinear systems with input constraints, described by

$$\begin{aligned}&\dot{x} = f(x) + G_{k(t)}(x)(u_{k(t)}(y) + \tilde{u}_{k(t)}(t)),\\ &y(x) = h(x), \quad u_k(y) \in \mathbf{U}_k, \quad (u_{k(t)}(y) + \tilde{u}_{k(t)}(t)) \in \mathbf{U}_k,\\ &k(t) \in \mathbf{K} = \{1, \ldots, N\}, \quad N < \infty, \end{aligned} \tag{1}$$

where $x \in \mathbb{R}^n$ denotes the vector of state variables, $y \in \mathbf{R}^m$ denotes the vector of measured variables and $u_{k(t)}(y) \in \mathbb{R}^m$ denotes the control action prescribed by the control law for the vector of constrained manipulated inputs under the kth configuration. $\tilde{u}_{k(t)}$ denotes the unknown fault vector with $u_{k(t)}(y) + \tilde{u}_{k(t)}$ taking values in a non-empty convex subset $\mathbf{U}_k$ of $\mathbb{R}^m$, where $\mathbf{U}_k = \{u_k + \tilde{u}_k \in \mathbb{R}^m : \|u_k + \tilde{u}_k\| \leqslant u_k^{\max}\}$, $\|\cdot\|$ is the Euclidean norm of a vector, $u_k^{\max} > 0$ is the magnitude of input constraints and $f(0) = 0$. The vector function $f(x)$ and the matrices $G_k(x) = [g_{1,k}(x) \cdots g_{m,k}(x)]$ are assumed to be sufficiently smooth on their domains of definition. $k(t)$, which takes values in the finite index set $\mathbf{K}$, represents a discrete state that indexes the matrix $G_k(\cdot)$ as well as the manipulated input $u_k(\cdot)$ and the possible faults in the manipulated inputs $\tilde{u}_k(\cdot)$. For each value that k assumes in $\mathbf{K}$, the process is controlled via a different set of manipulated inputs which defines a given control configuration. The notation $L_f h$ denotes the standard Lie derivative of a scalar function $h(\cdot)$ with respect to the vector function $f(\cdot)$ and the notation $x(T^+)$ denotes the limit of the trajectory $x(t)$ as T is approached from the right, i.e., $x(T^+) = \lim_{t \to T^+} x(t)$.

Throughout the manuscript, it is assumed that for any $u_k \in \mathbf{U}_k$ the solution of the system of Eq. (1) exists and is