Asian Journal of Control, Vol. 00, No. 0, pp. 1–11, Month 2008
Published online in Wiley InterScience (www.interscience.wiley.com) DOI: 10.1002/asjc.0000

Fault-tolerant control allocation for overactuated nonlinear systems

Andrea Cristofaro*, Marios M. Polycarpou and Tor Arne Johansen

ABSTRACT

This paper addresses the problem of fault-tolerant control allocation for input affine nonlinear systems. The proposed scheme is divided in three main tasks: fault detection and estimation using a nonlinear observer, fault isolation through a bank of unknown input observers with a resetting policy to reduce the effects of nonlinearities and control reconfiguration based on reduced order allocation. Analytical results regarding the isolability and reconfigurability of actuator faults are derived and a simulation example is used to illustrate the the proposed fault tolerant control methodology.

Key Words: Control allocation, fault-tolerant control, nonlinear systems

I. Introduction

Mechanical systems are often equipped with a redundant number of control devices in order to enhance the manoeuvrability capabilities and achieve satisfactory performances. The main objective of control allocation is to determine how to generate a desired control effect from a redundant set of actuators and effectors. Due to input redundancy, several configurations leading to the same generalized force are admissible and for this reason the control allocation schemes commonly incorporate additional secondary objectives [2] [20], such as the minimization of power consumption. On the other hand, having a large number of degrees of freedom in the control input design is a useful feature in handling the typical limitation factors arising in the mechanical applications [3] [7] [15] [18] [25], such as actuators/effectors dynamics, input saturation and other physical or operational constraints. One further advantage of actuator and effector redundancy is the possibility to reconfigure the control in order to cope with unexpected changes on the system dynamics, such as failures or malfunctions. In particular, if the set of actuators and effectors is partially affected by faults, one can modify the control allocation scheme by preventing the use of inefficient/ineffective devices in the generation of control effect or compensating for the loss of efficiency. However, one key point for successfully re-allocating the control is the availability of adequate information about the faults that have occurred; indeed, some accurate fault estimation and/or a correct isolation of the faulty actuators or effectors is necessary to address the reconfiguration problem. Recent results in the field of fault tolerant control allocation have been proposed based on sliding-mode techniques [8] [17], adaptive control strategies [5] [23] [24] and unknown input observers [10] [11]. Some application-oriented allocation schemes are instead proposed for reconfiguration in flight control [4] [26], and fault accommodation in automated underwater vehicles [9] [22].

This paper deals with the problem of fault-tolerant control allocation for nonlinear systems and, in particular, with the extension of the results on fault detection/isolation/accommodation of linear systems proposed in [10] [11] to nonlinear systems with a redundant set of inputs. An exhaustive fault diagnosis

Manuscript received 2016
* Corresponding author
The material in this paper was partially presented at the 54th IEEE Conference on Decision and Control (CDC), December 15-18, 2015, Osaka, Japan
A. Cristofaro is with the School of Science and Technology – Mathematics Division, University of Camerino, Italy. email: andrea.cristofaro@unicam.it
M.M. Polycarpou is with the KIOS Research Center for Intelligent Systems and Networks and with the Department of Electrical and Computer Engineering, University of Cyprus, Cyprus. email: mpolycar@ucy.ac.cy
T.A. Johansen is with the Department of Engineering Cybernetics, Norwegian University of Science and Technology and with the Centre for Autonomous Marine Operations and Systems (AMOS), Norway. email: tor.arne.johansen@itk.ntnu.no

and fault-tolerant framework for a large class of nonlinear systems has been developed in [27] [28], and the combination of these results with the fault-tolerant control allocation setup constitutes the core of the paper. One of the major challenges towards fault isolation in the presence of redundant inputs is that, due to redundancy, the same anomalous effects on the system dynamics can be produced by failures of different effectors or actuators. Addressing the resolution of this problem in a nonlinear framework is the main contribution of the paper, and to the best of authors' knowledge no other methods for the synthesis of fault-tolerant nonlinear control allocation schemes are available. The proposed architecture is based on unknown input observers together with a logic to recursively re-initialize the estimator design parameters in order to reduce the effects of nonlinearities, and a control re-allocation algorithm to be used in cascade with the fault diagnosis module. The paper is structured as follows. The problem setting is introduced in Section II; the fault detection task is addressed in Section III, while Section IV is dedicated to fault isolation. Moreover, a procedure to apply the proposed isolation scheme in the presence of unmeasured states is discussed in Section V for a class of monotone systems. Some strategies to tackle the problems of fault-tolerant control and control reconfiguration are discussed in Section VI. Finally, a simulation study is reported in Section VII to support and validate the proposed theoretical results.

II. Basic setup and problem formulation

Let us consider the nonlinear redundant control system $\Sigma = (f, g, G)$ given by the state equation

$$\dot{x} = f(x) + g(x)\tau + \eta(x,u,t) + b(t-T_0)\phi(x,u) \quad (1)$$

together with the nonlinear effector model

$$\tau = G(x)u, \quad (2)$$

where $x \in \mathbb{R}^n$, $\tau \in \mathbb{R}^k$, $u \in \mathbb{R}^m$, $k < m$. The vector u represents the redundant control input and τ is the generalized control effect or virtual input; the two variables are related through the matrix function $G(\cdot) : \mathbb{R}^n \to \mathbb{R}^{k\times m}$, which is assumed to be uniformly full-rank. The vector fields $\eta(\cdot,\cdot,\cdot) : \mathbb{R}^n \times \mathbb{R}^m \times \mathbb{R}^+ \to \mathbb{R}^n$ and $\phi(\cdot,\cdot) : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ represent the model uncertainty and the change in system dynamics due to a fault, respectively; the coefficient $b(\cdot) : \mathbb{R}^+ \to \mathbb{R}^+$ is the time profile evolution of the fault and T_0 is the (unknown) fault occurrence time. $\phi(\cdot,\cdot)$ and $b(\cdot)$ will be further described below.

Assumption II.1 *The state x and the redundant input u are assumed to be known for any time $t \geq 0$.*

The plant is assumed to be coupled with the nonlinear controller

$$\begin{aligned} \dot{x}_c &= z(x_c, x, \upsilon) \\ \tau_c &= h(x_c, \upsilon), \end{aligned} \quad (3)$$

where υ is an additional input, and a control allocation scheme is responsible to design the control input u such that the actuator joint effect produces the desired virtual input τ_c while some secondary objectives are possibly achieved. In particular, the control allocation scheme is requested to handle the problem of finding $u \in \mathbb{R}^m$ such that

$$\begin{aligned} & u = \arg \min_{w\in\mathbb{U}\subseteq\mathbb{R}^m} J(x,w) \\ & \text{subject to} \\ & G(x)w = \tau_c, \end{aligned} \quad (4)$$

where $\mathbb{U}$ is a prescribed constraint set and $J(\cdot,\cdot)$ is a suitable cost functional that is used to model secondary objectives. In the simple case of a quadratic functional $J(x,w) = w^T\Omega w$ without additional control constraints, a solution $u = G_\Omega^{-R}(x)\tau_c$ is provided by the weighted right-pseudo inverse of the matrix $G(x)$, this being well defined thanks to the full-rank assumption:

$$G_\Omega^{-R}(x) = \Omega^{-1}G^T(x)(G(x)\Omega^{-1}G^T(x))^{-1}.$$

Assumption II.2 *The model uncertainty η is an unstructured and unknown function of x, u and t; a known bound is supposed to be available $\forall i = 1,...,n$:*

$$|\eta_i(x,u,t)| \leq \bar{\eta}_i(x,t) \quad \forall(x,u) \in \mathbb{R}^n \times \mathbb{U}\, \forall t \geq 0,$$

for a positive, bounded and Lipschitz function $\bar{\eta}_i(\cdot,\cdot)$. For any such disturbance function, it is assumed that the solution of the nominal system (1) with $\phi(x,u) \equiv 0$ and subject to the controller (3) exists, and is unique and bounded for any $t \geq 0$.

The fault time profile $b(\cdot)$ is described by

$$b(t-T_0) = \begin{cases} 0 & t < T_0 \\ 1 - e^{-\alpha(t-T_0)} & t \geq T_0 \end{cases}$$

where $\alpha > 0$ is the (unknown) fault evolution rate.

The faults considered in this paper are modeled as actuator/effector loss of efficiency; this performance deterioration may involve single actuators/effectors as well as clusters of them if they share the same auxiliaries. In this regard, let us define the actuator/effector clusters

$$\mathcal{U}_1, \ldots, \mathcal{U}_r \subset [1,...,m]^m,$$

represented as groups of indices: if the index j is included in $\mathcal{U}_i$, then the actuator/effector u_j is part of the i^{th} cluster. For $i = 1, ..., r$ and $j = 1, ..., m$, let us set

$$\chi_{\mathcal{U}_i}(u_j) = \begin{cases} 1 & j \in \mathcal{U}_i \\ 0 & j \notin \mathcal{U}_i \end{cases}$$

and

$$\Delta_{\mathcal{U}_i} = diag(\chi_{\mathcal{U}_i}(u_1), \ldots, \chi_{\mathcal{U}_i}(u_m)).$$

In addition let us define $O_j = diag(\delta_{1j}, \delta_{2j}, ..., \delta_{mj})$, where δ_{ij} is the standard Kronecker symbol. Based on this construction, we define the set of admissible faults, divided into single and cluster for the sake of clarity:

$$\text{single faults} \quad \begin{cases} \bar{\phi}_1(x,u) = -g(x)G(x)O_1 u \\ \bar{\phi}_2(x,u) = -g(x)G(x)O_2 u \\ \vdots \\ \bar{\phi}_m(x,u) = -g(x)G(x)O_m u \end{cases} \tag{5}$$

$$\text{cluster faults} \quad \begin{cases} \bar{\phi}_{m+1}(x,u) = -g(x)G(x)\Delta_{\mathcal{U}_1} u \\ \bar{\phi}_{m+2}(x,u) = -g(x)G(x)\Delta_{\mathcal{U}_2} u \\ \vdots \\ \bar{\phi}_{m+r}(x,u) = -g(x)G(x)\Delta_{\mathcal{U}_r} u \end{cases} \tag{6}$$

Assumption II.3 *The fault $\phi(x,u)$ is assumed to belong to the finite set of $q = m + r$ admissible functions:*

$$\phi(\cdot,\cdot) \in \mathcal{F}, \quad \mathcal{F} := \{\theta_1\bar{\phi}_1(\cdot,\cdot), \ldots, \theta_q\bar{\phi}_q(\cdot,\cdot)\},$$

where, for any $i = 1, ..., q$, θ_i is an unknown magnitude parameter with $\theta_i \in (0, 1]$, and $\bar{\phi}_i$ is an admissible fault structure according to (5)-(6).

Problem statement. The main objective of this paper is to address the fault isolation problem for a nonlinear system with redundant inputs and to define a robust control allocation scheme towards maintaining system stability and recovering performances in spite of single or multiple actuator faults. Three fundamental issues have to be addressed: fault detection (FD), fault isolation (FI) and control reconfiguration (CR).

- FD: a full-state observer $\hat{x}^{(0)}$ is designed and, monitoring the residual $|x(t) - \hat{x}^{(0)}(t)|$, a fault is detected whenever this signal exceeds a given threshold.
- FI: a bank of q full-state observers $\hat{x}^{(s)}$, indexed by s, are designed such that the combined behavior of residuals allows us to identify the faulty actuator or the faulty actuator cluster.
- CR: the control allocation policy is updated such that the actuators that are identified as faulty are not used or strongly weighted, this leading to a reconfigured input signal $\tilde{u}$ with $G(x)\tilde{u} \to \tau_c$.

III. Fault detection

Following the methodology developed in [27], the FD observer $\hat{x}^{(0)}$ is chosen as follows:

$$\dot{\hat{x}}^{(0)} = -\Lambda^{(0)}(\hat{x}^{(0)} - x) + f(x) + g(x)\tau_c + \hat{\phi}(x, u, \zeta^{(0)}) \tag{7}$$

where $\hat{\phi}(\cdot,\cdot,\cdot) : \mathbb{R}^n \times \mathbb{R}^m \times \mathbb{R}^q \to \mathbb{R}^n$ is a fault approximation model, $\zeta^{(0)}$ is a vector of adjustable weights and $\Lambda^{(0)} = diag(\lambda_1^{(0)}, ..., \lambda_n^{(0)})$ with $-\lambda_i^{(0)} < 0$ for any $i = 1, ..., n$. The initial weight vector $\zeta^{(0)}(0)$ is chosen such that $\hat{\phi}(x, u, \zeta^{(0)}(0)) = 0$ for any $(x, u) \in \mathbb{R}^n \times \mathbb{R}^m$, corresponding to the fault-free condition.
The fault estimator $\hat{\phi}$ is defined as a linear combination of the admissible faults $\phi \in \mathcal{F}$, where the coefficients of the combination are given by the entries of $\zeta^{(0)}$:

$$\hat{\phi}(x, u, \zeta^{(0)}) := \sum_{j=1}^{q} \zeta_j^{(0)}\bar{\phi}_j(x, u). \tag{8}$$

Setting $\epsilon^{(0)} = x - \hat{x}^{(0)}$, the weight vector $\zeta^{(0)}$ is updated according to a learning algorithm based on Lyapunov synthesis methods [27]:

$$\dot{\zeta}^{(0)} = \Pi_{\mathcal{Z}}\left\{\Gamma^{(0)}Y^T D[\epsilon^{(0)}]\right\} \tag{9}$$

where Π is a projection operator that restricts the parameter estimation vector $\zeta^{(0)}$ to a prescribed compact and convex domain $\mathcal{Z} \subset \mathbb{R}^q$, $\Gamma^{(0)}$ is a symmetric positive definite learning rate matrix and Y is the gradient matrix of the estimator (8) with respect to the weight, i.e. $Y := \left[\bar{\phi}_1(x,u) \ \cdots \ \bar{\phi}_q(x,u)\right]$. The dead-zone operator is described by the expression

$$D[\epsilon^{(0)}(t)] := \begin{cases} 0 & |\epsilon_i^{(0)}(t)| \le \epsilon_i^\star(t), \ i = 1, ..., n \\ \epsilon^{(0)}(t) & \text{otherwise} \end{cases}$$

where $\epsilon_i^\star$ is a suitable time-varying threshold to be specified. The dead-zone is introduced in order to prevent adaptation of the weight due to the presence of the modeling errors $\eta(x, u, t)$, these causing generally nonzero state estimation errors; in this regard, according to Assumption II.2, the detection thresholds can be defined as follows:

$$\begin{aligned} \epsilon_i^*(t) \ &:= \int_0^t e^{-\lambda_i^{(0)}(t-\sigma)}\bar{\eta}_i(x(\sigma), \sigma)d\sigma \\ &\ge \left|\int_0^t e^{-\lambda_i^{(0)}(t-\sigma)}\eta_i(x(\sigma), u(\sigma), \sigma)d\sigma\right|. \end{aligned}$$

This threshold correspond to the forced response of the observer $\epsilon^{(0)}$ to the input given by the upper bound

$\bar{\eta}(x,t)$, and it can be straightforwardly implemented as a filter with transfer function $1/(s+\lambda_i^{(0)})$ with zero initial conditions.

Theorem III.1 *A fault is detectable when $|\epsilon_i^{(0)}(t)| > \epsilon_i^\star(t)$ for some $i = 1,...,n$. Accordingly, we define the fault detection time T_d as the infimum*

$$T_d := \inf \bigcup_{i=1}^{n} \{t \geq T_0 : |\epsilon_i^{(0)}(t)| > \epsilon_i^\star(t)\}. \qquad (10)$$

We notice that, by construction, the fault estimator (8)-(9) begins to be updated only for $t \geq T_d$.

IV. Fault isolation

One major challenge in the design of fault isolation scheme for systems with redundant inputs is superposition of fault effects. Specifically, due to redundancy, for any $i \neq j$ a non-empty sub-domain $\mathcal{D}_{ij} \subset \mathbb{R}^n \times \mathbb{R}^m$ may exist such that

$$g(x)G(x)(I_m - O_i)u = g(x)G(x)(I_m - O_j)u$$

$\forall (x,u) \in \mathcal{D}_{ij}$, where $I_m \in \mathbb{R}^{m\times m}$ denotes the identity matrix and the equality $\tau_c = G(x)u$ has been used.
We propose a switching architecture based on unknown input observes (UIO) [6] [13] [19] [21]. Let us denote by $B(x)$ the matrix function

$$B(x) = g(x)G(x),$$

select a vector $\bar{x} \in \mathbb{R}^n$ to be specified later, and apply the decomposition

$$B(x) = W_{\bar{x}} + B_{\bar{x}}(x), \qquad (11)$$

where $W_{\bar{x}} = B(\bar{x})$ and $B_{\bar{x}}(x) = B(x) - B(\bar{x})$. Accordingly, for an input signal $B(x(t))\sigma(t)$, we will refer to $W_{\bar{x}}\sigma(t)$ as the *linear part* of the signal.
Let us then consider the following nonlinear UIO structure:

$$\begin{aligned} \dot{\omega} &= F_{\bar{x}}\omega + R_{\bar{x}}g(x)\tau_c + f(x) - H_{\bar{x}}f(x) + (K_{\bar{x}} - R_{\bar{x}})x \\ z &= \omega + H_{\bar{x}}x \end{aligned} \qquad (12)$$

with

$$\begin{aligned} K_{\bar{x}} &= K_{\bar{x},1} + K_{\bar{x},2} && (13)\\ R_{\bar{x}} &= I_n - H_{\bar{x}} && (14)\\ F_{\bar{x}} &= R_{\bar{x}} - K_{\bar{x},1}, \quad spec(F_{\bar{x}}) \subset \mathbb{C}^- && (15)\\ K_{\bar{x},2} &= F_{\bar{x}}H_{\bar{x}} && (16) \end{aligned}$$

and where the parameters have to be designed according to the choice of $\bar{x}$ and the set of admissible faults. Let us stress that the parameter $H_{\bar{x}}$ has not been fixed at this stage, and that some degrees of freedom exist for the tuning of $K_{\bar{x},1}$, which is used to place the eigenvalues of $F_{\bar{x}}$ once a proper choice for $H_{\bar{x}}$ has been made. To this end, exploiting the matrix structure, one has

$$W_{\bar{x}} = [W_{\bar{x},1} \ \cdots \ W_{\bar{x},m}];$$

in addition, for $j = 1,...,r$ we denote by $W_{\bar{x},\mathcal{U}_j}$ the sub-matrix obtained from $W_{\bar{x}}$ picking the columns corresponding to the indices included in $\mathcal{U}_j$ only.

Lemma IV.1 *Suppose that matrices $W_{\bar{x},s}, W_{\bar{x},\mathcal{U}_s}$ are full column rank* and define $\{H_{\bar{x}}^{(s)}\}$, $s = 1,...,q$ as follows:*

$$\begin{aligned} H_{\bar{x}}^{(s)} &:= W_{\bar{x},s}(W_{\bar{x},s}^T W_{\bar{x},s})^{-1}W_{\bar{x},s}^T && s = 1,...,m \\ H_{\bar{x}}^{(m+s)} &:= W_{\bar{x},\mathcal{U}_s}(W_{\bar{x},\mathcal{U}_s}^T W_{\bar{x},\mathcal{U}_s})^{-1}W_{\bar{x},\mathcal{U}_s}^T && s = 1,...,r. \end{aligned}$$

Then the resulting estimation error $\epsilon^{(s)} := x - z^{(s)}$, with $z^{(s)}$ assigned by (12), is decoupled from the linear part of faults of the type $\bar{\phi}_s(x,u)$.

Proof. By construction, the following identity holds true for $R_{\bar{x}}^{(s)}$ defined by (14) when $H_{\bar{x}}$ is replaced by $H_{\bar{x}}^{(s)}$:

$$\begin{aligned} R_{\bar{x}}^{(s)}W_{\bar{x},s} &= 0 && s = 1,...,m \\ R_{\bar{x}}^{(s)}W_{\bar{x},\mathcal{U}_{s-m}} &= 0 && s = m+1,...,q. \end{aligned} \qquad (17)$$

As a consequence the dynamics of the estimation error $\epsilon^{(s)} := x - z^{(s)}$, where $z^{(s)}$ is the state of the unknown input observer (12)-(16) with $H_{\bar{x}}$ replaced by $H_{\bar{x}}^{(s)}$, is assigned by

$$\begin{aligned} \dot{\epsilon}^{(s)} &= f(x) + g(x)\tau_c + \eta(x,u,t) + b(t-T_0)\phi(x,u) \\ &\quad - F_{\bar{x}}^{(s)}z^{(s)} + F_{\bar{x}}^{(s)}H_{\bar{x}}^{(s)}x - R_{\bar{x}}^{(s)}g(x)\tau_c - f(x) \\ &\quad + H_{\bar{x}}^{(s)}f(x) + R_{\bar{x}}^{(s)}x - K_{\bar{x}}^{(s)}x - H_{\bar{x}}^{(s)}\dot{x} \\ &= F_{\bar{x}}^{(s)}\epsilon^{(s)} + R_{\bar{x}}^{(s)}\eta(x,u,t) + b(t-T_0)R_{\bar{x}}^{(s)}\phi(x,u), \end{aligned} \qquad (18)$$

where the identity $\dot{z}^{(s)} = \dot{\omega}^{(s)} - H_{\bar{x}}^{(s)}\dot{x}$ has been used. Choose now $\phi \in \mathcal{F}$, say $\phi(x,u) = \theta\bar{\phi}_1(x,u)$ for sake of simplicity, with $\theta \in (0,1]$. Then, by construction, the error dynamics reduces to

$$\begin{aligned} \dot{\epsilon}^{(1)} &= F_{\bar{x}}^{(1)}\epsilon^{(1)} + R_{\bar{x}}^{(1)}\eta + b\theta R_{\bar{x}}^{(1)}(W_{\bar{x}} + B_{\bar{x}}(x))O_1u \\ &= F_{\bar{x}}^{(1)}\epsilon^{(1)} + R_{\bar{x}}^{(1)}\eta + b\theta R_{\bar{x}}^{(1)}B_{\bar{x},1}(x)u_1 \end{aligned}$$

*A sufficient condition for preventing rank deficiency and guaranteeing the feasibility of observer design is selecting the vector $\bar{x}$ such that the matrix $W_{\bar{x}}$ attains a uniform sub-rank [10, 11] not smaller than the number of elements included in the largest actuator cluster.

where the arguments in $\eta(\cdot,\cdot,\cdot)$ and $b(\cdot)$ have been omitted and the identities $R^{(1)}_{\bar{x}} W_{\bar{x},1} = 0$ and $B_{\bar{x}}(x)O_1 u = B_{\bar{x},1}(x)u_1$ have been used, $W_{\bar{x},1} + B_{\bar{x},1}(x)$ being the first column of $B(x)$. The case $s = 2, ..., q$ can be established using similar arguments. □

Roughly speaking, Lemma IV.1 guarantees that the error only depends on the fault through the nonlinear part of the vector field $B(x)$, i.e. $B_{\bar{x}}(x)$ according to our notation: this means that, as long as such nonlinear part is negligible, the error $\epsilon^{(s)}$ remains substantially decoupled from the fault $\bar{\phi}_s$. For any $s = 1, ..., q$ let us choose

$$K^{(s)}_{\bar{x},1} = R^{(s)}_{\bar{x}} + \Lambda,$$

with $-\Lambda$ a diagonal Hurwitz matrix: this guarantees observer stability since $F^{(s)}_{\bar{x}} = -\Lambda$ for any $s = 1, ..., q$. Without loss of generality one can assume $\Lambda = \Lambda^0$, as defined in Sec. III for the case of fault detection.

The basic idea is to adapt the isolation algorithm proposed in [11] for the case of linear systems and therefore one aims at maintaining the size of $B_{\bar{x}}(x)$ as small as possible; on the other hand, since we do not mean to influence the system dynamics while preforming fault isolation, a feasible way to limit the size of $B_{\bar{x}}(x)$ is to reconfigure and re-initialize the observers by linearizing $B(x)$ around a new fixed point if $B_{\bar{x}}(x)$ becomes too large. To this end, let us set $\varrho > 0$ as an indicator of the maximum admissible size for $B_{\bar{x}}(x)$, this meaning that whenever $\max_{i,j} |B_{\bar{x},ij}(\bar{\bar{x}})| \geq \varrho$ for some $\bar{\bar{x}}$, then the decomposition of $B(x)$ needs to be updated as

$$B(x) = W_{\bar{\bar{x}}} + B_{\bar{\bar{x}}}(x).$$

A general rule for the selection of a suitable $\varrho > 0$ is proposed at the end of the section (Remark IV.1). Referring to the thresholds $\epsilon^{\star}_i(t)$, we consider a larger bound given by $\mu^{(s)}_i(t) := \epsilon^{\star}_i(t) + \bar{\mu}^{(s)}_i(t),\ i = 1, ..., n$ with $\bar{\mu}^{(s)}_i(\cdot)$ a positive function to be specified. To this end we observe that, by integration, when $\phi(x,u) = \theta\bar{\phi}_1(x,u)$ the error $\epsilon^{(1)}(t)$ verifies

$$|\epsilon^{(1)}_i(t)| = \left| \int_0^1 e^{-\lambda_i(t-\sigma)} [R^{(1)}_{\bar{x}} \eta_i(x(\sigma),u(\sigma),\sigma) + b(\sigma)\theta\nu^{(1)}_i(\sigma)] d\sigma \right|$$

where $\nu^{(1)}_i$ is the i^{th} component of $R^{(1)} B_{\bar{x},1}(x)u_1$. Now the following bound is in force as long as $B_{\bar{x}}(x)$ is ϱ-limited:

$$|\nu^{(1)}_i| = \left| \sum_{\ell=1}^n R^{(1)}_{i\ell} B_{\bar{x},\ell 1}(x) u_1 \right| \leq \varrho \sum_{\ell=1}^n \left| R^{(1)}_{i\ell} \right| |u_1| =: \varrho\psi^{(1)}_i |u_1|.$$

Setting $\bar{\mu}^{(1)}_i(t) := \int_0^t e^{-\lambda_i(t-\sigma)} \varrho\psi^{(1)}_i |u_1(\sigma)| d\sigma$ and recalling that both θ and $b(t)$ are bounded by 1, it is straightforward to verify that

$$|\epsilon^{(1)}_i(t)| < \epsilon^{\star}_i(t) + \bar{\mu}^{(1)}_i(t) = \mu^{(1)}_i(t) \qquad (19)$$

for $\phi(x,u) = \theta\bar{\phi}_1(x,u)$ and $\max_{i,j} |B_{\bar{x},ij}(\bar{x})| \leq \varrho$. Let us generalize the construction and set

$$\psi^{(s)}_i = \sum_{\ell=1}^n \left| R^{(s)}_{i\ell} \right|, \quad s = 1, ..., m$$

and

$$\bar{\mu}^{(s)}_i(t) = \begin{cases} \int_0^t e^{-\lambda_i(t-\sigma)} \varrho\psi^{(s)}_i |u_s(\sigma)| d\sigma & s = 1, ..., m \\ \int_0^t e^{-\lambda_i(t-\sigma)} \varrho \sum_{j \in \mathcal{U}_{s-m}} \psi^{(j)}_i |u_j(\sigma)| d\sigma & s = m+1, ..., q \end{cases}$$

Lemma IV.2 *Assume that a fault has been detected by the FD module at $t = T_{det}$, and suppose that there exist $T^{\star} > T_{det}$ and $s^{\star} \in \{1, ..., q\}$ such that*

- $\max_{i,j} |B_{\bar{x},ij}(x(t))| < \varrho \quad \forall t \in [T_{det}, T^{\star}]$
- *for each $s \in \{1, ..., q\} \setminus \{s^{\star}\}$ there exists $i_s \in \{1, ..., n\}$ with*

$$|\epsilon^{(s)}_{i_s}(T^{\star})| > \mu^{(s)}_{i_s}(T^{\star}) \qquad (20)$$

- *for each $i = 1, ..., n$, one has*

$$|\epsilon^{(s^{\star})}_i(t)| \leq \mu^{(s^{\star})}_i(t) \quad \forall t \in [T_{det}, T^{\star}].$$

Then we can isolate the faults using the decision algorithm:

$$\textit{The fault is in} \begin{cases} \textit{input } u_{s^{\star}} & \textit{if } s^{\star} \in \{1, ..., m\} \\ \textit{cluster } \mathcal{U}_{s^{\star}-m} & \textit{if } s^{\star} \in \{m+1, ..., q\} \end{cases} \qquad (21)$$

In the following we will refer to residual $\epsilon^{(s)}(t)$ as in *alarm mode* if condition (20) is satisfied for some $t \geq 0$.

Proof. In order to prove the statement, it is sufficient to consider inequality (19) for a generic $s = 1, ..., q$: as long as $B_{\bar{x}}(x(t))$ is ϱ−limited, if $\phi(x,u) = \theta\phi_s(x,u)$ then $|\epsilon^{(s)}_i(t)| < \epsilon^{\star}_i(t) + \bar{\mu}^{(s)}_i(t) = \mu^{(s)}_i(t)\ \forall i = 1, ..., n$. Consequently, the only admissible condition to realize a configuration with all residuals except $\epsilon^{(s^{\star})}(t)$ in alarm mode, is that the fault is of type $\phi(x,u) = \theta\phi_{s^{\star}}(x,u)$ for some $\theta \in (0,1]$ □

We point out that Lemma IV.2 holds true if and only if $B_{\bar{x}}$ is ϱ−limited. In order to obtain a global decision algorithm, we need to merge (21) with an iterative linearization scheme for $B(x)$.

Theorem IV.1 *Set $\bar{x} = x(T_{det})$ and design the observers according to (17) with $W_{\bar{x}} = B(x(T_{det}))$. There exists a subdivision of the interval $[T_{det}, +\infty) = \bigcup_{p\in\mathbb{N}} [T_p, T_{p+1})$ with $T_1 = T_{det}$ such that, for any $p \in \mathbb{N}$, either one of the following conditions is verified:*

A) There exist $T_{isol} \in (T_p, T_{p+1})$ and $s^\star$ satisfying the conditions of Lemma IV.2, and $B_{\bar{x}}(x(t)) = B(x(t)) - W_{\bar{x}}$ is $\varrho-$limited in $[T_p, T_{p+1})$.

B) The total number of residuals in alarm mode is less than $q-1$ for any $t \in [T_p, T_{p+1})$ and there exist i, j such $|B_{\bar{x},ij}(x(T_{p+1}))| = \varrho$. The observers are re-initialized with $W_{\bar{x}} = B(x(T_{p+1}))$.

If case A) occurs, the fault can be correctly isolated according to the rule (21).

It is worth to mention that, for the iterative procedure of Theorem IV.1 to converge to an isolation time T_{isol}, the rate of variation of $B(x)$ must be negligible with respect to the size and rate of the residuals. In other words, on the one hand $B(x(t))$ is required to be slowly-variant, and on the other hand the fault rate α and the size of the faulty inputs must be sufficiently large to allows $\epsilon^{(s)}(t)$ overpass the threshold as fast as possible: in certain cases, this may require the fulfillment of a PE condition. In this regard, the following statement can be given.

Proposition IV.1 *Let us denote by $\gamma_B(x(t))$ the rate of change of $B(x(t))$, i.e. $\gamma_B(x(t)) := |\nabla_x B(x(t))\dot{x}(t)|$. Based on the mean-value theorem, a sufficient condition for fault isolability is then provided by the existence of a time interval $[t_1, t_2]$ with $\max_{t\in[t_1,t_2]} \gamma_B(x(t))|t_2 - t_1| \le \varrho$ and $\min_{t\in[t_1,t_2]} |\dot{\epsilon}_i(t)||t_2 - t_1| \ge \max_{t\in[t_1,t_2]} \bar{\mu}_i(t)$.*

Remark IV.1 *The selection of the optimal tolerance ϱ raises the following trade-off: on the one hand ϱ has to be small to guarantee that the decoupling condition (17) to be used for fault isolation holds true in spite of nonlinearities, on the other hand a very small ϱ may lead to a vary fast residual resetting with a consequent possible delay in the achievement of isolation. A general rule for tuning the parameter is to choose ϱ such that the threshold $\bar{\mu}_i^{(s)}(t)$ are small enough to prevent hiding of faults whose severity is classified as a potential hazard for the overall system safety: this can be easily carried out by comparing the size of the isolation thresholds $\bar{\mu}_i^{(s)}(t)$ with the size of the forced response of the error systems (18) to the estimated fault $\hat{\phi}(x, u, \zeta^{(0)})$ defined by the estimator (8).*

V. Unmeasured states

The extension of the proposed results to the case of nonlinear systems with unmeasured states is considered in this section. We consider plants of the form

$$\begin{aligned} \dot{x} &= Ax + Q\rho(Nx) + f(y) + g(y)\tau \\ &\quad + \eta(x, u, t) + b(t - T_0)\phi(x, u) \\ y &= Cx, \end{aligned} \tag{22}$$

with effector model $\tau = G(y)u$, where A, Q, N, C are matrices with appropriate dimensions and ρ is a smooth funtion. We notice that (22) is a special case of the original system (1), where the known nonlinearities of the model are limited to involve the measured variables y only, except for the term $Q\rho(Nx)$ that is allowed to depend on the whole state x. Accordingly, it is assumed the availability of a bound on the perturbation term $\eta(\cdot,\cdot,\cdot)$ uniform with respect to the unmeasured states.

Assumption V.1 *There exist positive and bounded functions $\bar{\eta}_i(y, t)$, for $i = 1, ..., n$, with*

$$|\eta_i(x, u, t)| \le \bar{\eta}_i(Cx, t) \quad \forall (x, u) \in \mathbb{R}^n \times \mathbb{U}\, \forall t \ge 0.$$

For systems of the class (22), unknown input observers can be designed using the circle criterion under a fairly general monotonicity assumption on the function $\rho(\cdot)$ [16] [19].

Assumption V.2 *The function $\rho(\zeta)$ satisfies the monotonicity condition*

$$\frac{\partial \rho}{\partial \zeta} + \frac{\partial \rho^T}{\partial \zeta} \ge 0\, \forall \zeta$$

Finally, in order to guarantee isolability of faults, the range of the vector field $g(y)$ must be included in a suitable linear subspace, as exploited in the next assumption.

Assumption V.3 *There exists a constant matrix $E \in \mathbb{R}^{n\times d}$ with $k \le d < n$ such that, for any fixed $\bar{y} \in \mathbb{R}^p$ one has*

$$Im(g(\bar{y})) \subseteq Im(E).$$

Let H be a matrix selected such that $(I + HC)E = 0$, where a possible, simple choice is

$$H = E[(CE)^T(CBE)]^{-1}(CE)^T.$$

Define then the observer candidate

$$\begin{aligned} \dot{\omega} &= (I - HC)A(\omega + Hy) \\ &\quad + L1(y - C(\omega + Hy)) + (I - HC)(f(y) + g(y)\tau_c) \\ &\quad + (I - HC)Q\rho(E(\omega + Hy) + K(y - C(\omega - Hy))) \\ z &= \omega + Hy \end{aligned} \tag{23}$$

and assume that a symmetric matrix $P > 0$ and a scalar $\kappa > 0$ exist such that the following LMI is feasible

$$\begin{bmatrix} A_1^T P + PA_1 + \kappa I & PRQ + (N - KC)^T \\ Q^T R^T P + (N - KC) & 0 \end{bmatrix} \leq 0$$

where $R = (I - HC)$ and $A_1 = RA - L_1 C$. Then, thanks to Assumption V.2, (23) is an unknown input observer [19, Theorem 4.2], and the estimation error dynamics $\tilde{x} = x - z$ is governed by the equation

$$\begin{aligned} \dot{\tilde{x}} &= (A_1 + (I - HC)Q(N - KC))\tilde{x} \\ &+ R(\eta(x, u, t) + b(t - T_0)\phi(x, u)). \end{aligned}$$

and, in the absence of disturbances and faults, it results to be UGES. Having established this result accounting for the whole space spanned by the columns of $g(y)$ (see Assumption V.3), it is then guaranteed the existence of unknown input observers of the form (23) featuring the weaker decoupling property $(I - HC)E_\star$ where $E_\star$ is any reduced-order matrix with $Im(E_\star) \subset Im(E)$. It is then possible to extend in a natural way the results of Theorem IV.1 to system (22), by letting $E_\star$ vary among all the directions associated to single and cluster faults as defined in (5)-(6) and considering the bound given in Assumption V.1 to compute the detection thresholds.

Remark V.1 *An alternative approach to deal with unmeasured states, based on a special change of coordinates, might be adopted in the case of Lipschitz nonlinearities [29] [30].*

VI. Control reconfiguration

Suppose that either one actuator, say $u_{i_\sharp}$ with $i_\sharp \in \{1, ..., m\}$, or one cluster of actuators/effectors, say $\mathcal{U}_{j_\sharp}$ with $j_\sharp \in \{1, ..., r\}$, has been identified as faulty by the FDI module. For the sake of simplicity the dependency of the effector matrix G on the state x is dropped throughout the section. Denote by $\tilde{G}_{i_\sharp}$ and $\tilde{G}_{\mathcal{U}_{j_\sharp}}$ the matrices obtained from G by removing, respectively, the column $i_\sharp$ and the columns corresponding to the actuators/effectors included in the cluster $\mathcal{U}_{j_\sharp}$. The reconfiguration can be performed by different methods, depending on several factors such as secondary objectives, actuator dynamics, limited control inputs rates or other control constraints. It is worth to note that in some cases, due to the adverse effects of faults, also the desired control effect $\tau_c(t)$ might be requested to change with respect to the original one in order to recover the deteriorated system performances, this corresponding to update the controller structure (3).

6.1. Reduced-order allocation

Necessary conditions for having enough degrees of freedom to perform an exact re-allocation are:

$$rank\,\tilde{G}_{i_\sharp} \geq k, \quad rank\,\tilde{G}_{\mathcal{U}_{j_\sharp}} \geq k. \tag{24}$$

We notice that, while the first inequality is guaranteed by the assumption $m > k$, the second one has to be carefully checked as it depends on the cardinality of the particular cluster $\mathcal{U}_{j_\sharp}$. Usually this is taken care of in the actuator/effector system design by considering its redundancy and clusters defined by common mode faults. The reconfiguration can be regarded as a reduced-order control allocation in which some of the inputs are neglected or strongly penalized. For example, in the case of the quadratic cost functional $J(w)$ with $\mathbb{U} = \mathbb{R}^m$, assuming that the actuator cluster $\mathcal{U}_{j_\sharp}$ is faulty, one has to solve the reduced-order optimization problem

$$\begin{aligned} & u^T \Omega u = \min_{w \in \mathbb{R}^m} w^T \Omega w \\ & \text{subject to} \\ & \begin{cases} u_i = 0 \text{ if } i \in \mathcal{U}_{j_\sharp} \\ \tau_c = Gu \end{cases} \end{aligned} \tag{25}$$

that yields a reduced vector

$$\tilde{u} = \tilde{G}_{\tilde{\Omega}}^{-R} \tau_c \in \mathbb{R}^{m - \aleph_{j_\sharp}},$$

where $\aleph_{j_\sharp}$ is the cardinality of the cluster $\mathcal{U}_{j_\sharp}$ and $\tilde{G}_{\tilde{\Omega}}^{-R}$ is the weighted pseudo inverse of the matrix $\tilde{G}_{\mathcal{U}_{j_\sharp}}$, i.e.

$$\tilde{G}_{\tilde{\Omega}}^{-R} = \tilde{\Omega}^{-1} \tilde{G}_{\mathcal{U}_{j_\sharp}}^T (\tilde{G}_{\mathcal{U}_{j_\sharp}} \tilde{\Omega}^{-1} \tilde{G}_{\mathcal{U}_{j_\sharp}}^T)^{-1}$$

with $\tilde{\Omega} \in \mathbb{R}^{(m - \aleph_{j_\sharp}) \times (m - \aleph_{j_\sharp})}$ obtained from Ω by reducing the dimension according to $\tilde{G}_{\mathcal{U}_{j_\sharp}}$.

6.2. Actuator dynamics

A different and more sophisticated approach is needed in the presence of actuator dynamics. Suppose for instance that the actuator states $u \in \mathbb{R}^m$ are assigned by the dynamical relationships

$$\dot{u}_i = -\kappa_i u_i + v_i$$

with $\kappa_i \geq 0$ and v_i actuator control inputs. As a matter of fact, within this extended framework, the faults may affect the actuator dynamics through modification of the nominal drift coefficients κ_i. Since the actuator states can only be changed dynamically by means of the input v_i, zeroing the latter does not always ensure that the corresponding u_i converges to the origin, and actuators may approach some non zero steady-state. While this fact does not compromise the fault detection and isolation procedures, it constitutes an additional challenge towards addressing control reconfiguration. A possible solution to this problem has been proposed in [12], consisting in two main steps: estimation of the faulty actuators steady-state (if any) using residuals and finite-time control reconfiguration [1], i.e. determination of a reduced-order actuator input $\tilde{v}(t)$ able to guarantee convergence in a finite time $\tau^\star > 0$ of the safe actuator states to the desired control input

$$\lim_{t\to\tau^\star} |\tilde{G}\tilde{u}(t) - \tilde{\tau}_c(t)| = 0,$$

where $\tilde{\tau}_c(t) = \tau_c(t) - G_{i_\sharp} u^\flat_{i_\sharp}$, $u^\flat_{i_\sharp}$ being the estimate of the faulty actuator steady-state.

6.3. Dynamic weighting

As already highlighted, exact control reconfiguration is achievable only when the rank condition (24) is fulfilled; however, in some circumstances, this condition may be too restrictive, and hence some techniques to handle the case $rank\ \tilde{G}_{\mathcal{U}_{j_\sharp}} < k$ are needed. A first approach, leading to approximate solutions, is to penalize the faulty actuators $\mathcal{U}_{j_\sharp}$ by rescaling (non uniformly) the weighting matrix Ω. For example, assuming $\Omega = diag(\omega_1, ..., \omega_m)$, the allocation problem reads as

$$\begin{aligned} & u = \arg \min_{w\in\mathbb{U}\subseteq\mathbb{R}^m} w^T \Xi \Omega w \\ & \text{subject to} \\ & \tau_c = Gw, \end{aligned}$$

where $\Xi = diag(\xi_1, ..., \xi_m)$ is a diagonal positive definite matrix such that

$$\begin{cases} \xi_j = 1 & j \notin \mathcal{U}_{j_\sharp} \\ \xi_j >> 1 & j \in \mathcal{U}_{j_\sharp} \end{cases}$$

As proposed in [9], the weights ξ_j might also be defined dynamically with a rate depending on the fault severity, which can be inferred from the size of residuals. A simple dynamic updating scheme for the weights is the following:

$$\begin{aligned} \dot{\xi}_j &= 0 & j \notin \mathcal{U}_{j_\sharp} \\ \dot{\xi}_j &= -\upsilon(t)\xi_j & j \in \mathcal{U}_{j_\sharp}, \end{aligned}$$

where $\upsilon(t)$ is the measure of fault severity computed as

$$\upsilon(t) = \frac{1}{q}\sum_{s=1}^{q}\sum_{i=1}^{n} \max\{0, |\epsilon_i^{(s)}(t)| - \mu_i^{(s)}(t)\},$$

which corresponds to the average offset of active residuals with respect to thresholds.

6.4. Switching schemes

An alternative and possibly more robust strategy is to adopt the robust framework proposed in [28]. Based on Lyapunov techniques and relying on the FDI module, the controller is designed to robustly stabilize the plant during all the three fault-related phases: before fault occurrence (α), after fault detection (β), after fault isolation (γ). This can be done through a switching term $\dot{x}_c = z_\diamond(t, x_c, x, \upsilon)$ depending on the fault estimation and on the particular phase $\diamond = \alpha, \beta, \gamma$. We notice that, in order to adapt this approach to the input redundancy framework, the switching term $z_\diamond(\cdot,\cdot,\cdot,\cdot)$ must be first incorporated in the controller definition (3) and then accordingly commanded to the actuators through the allocation scheme. In conclusion, let us state the following general rule.

Rule VI.1 *Assume that the actuator cluster $\mathcal{U}_{j_\sharp}$ has been identified as faulty. There are two options for performing control reconfiguration:*

A) The rank condition (24) is satisfied. The controller structure (3) does not change, unless for the case of actuator dynamics with non zero steady-sates, and the control input is reallocated according to the reduced-order scheme (25).

B) The rank condition (24) is not fulfilled. The allocation scheme (4) does not change, and the controller structure (3) is updated by incorporating a switching term $z_\diamond(t, x_c, x, \upsilon)$ that can be designed following the procedure presented in [28].

VII. A simulation study

Let us consider the following nonlinear system as a working example:

$$\begin{aligned} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= x_3 + sign(x_2)\sqrt{|x_2|} + g_0(x_1)\tau_1 \\ \dot{x}_3 &= -x_1x_3 + g_0(x_1)\tau_1 + \tau_2 \end{aligned}$$

with

$$g(x) = \begin{bmatrix} 0 & 0 \\ g_0(x_1) & 0 \\ g_0(x_1) & 1 \end{bmatrix}, \quad g_0(x_1) = \frac{1}{1+x_1^2}.$$

The desired control effect $\tau = [\tau_1\ \tau_2]^T$ is assigned by a feedback linearizing law which ensures the regulation of the state x_1 to the setpoint $r_1 = -1.5$, i.e.

$$\begin{aligned} \tau_1 &= -g_0^{-1}(x_1)sign(x_2)\sqrt{|x_2|} \\ \tau_2 &= x_1x_3 - g_0(x_1)\tau_1 - Kx + K_r r_1 \end{aligned}$$

with $K = [6 \quad 11 \quad 6]^T$ and $K_r = 6$. The control allocation scheme is defined as

$$\tau = G(x)u, \quad u = [u_1\ u_2\ u_3\ u_4]^T$$

$$G(x) = \left[\begin{array}{cccc} 1 & 1 & 1 & 0 \\ \frac{x_1}{\sqrt{1+x_1^2}} & -1 & 0 & -2 \end{array} \right].$$

The input disturbance has been chosen as an oscillating signal with state-dependent amplitude:

$$\eta(x, u, t) = [0\ 0.2\sin(t)x_2\ 0.2\cos(t^2)x_1]^T.$$

A fault detection observer has been implemented according to (7) with $\Lambda^{(0)} = diag(-3, -5, -7)$. An fault is supposed to affect actuator u_4 for $t \geq T_0 = 20s$, fading in with a fast evolution rate $\alpha = 20$. On the other hand, we point out that the proposed architecture can successfully handle the case of incipient faults too, i.e. faults with a small rate α can still be correctly isolated. The efficiency of the proposed fault detection technique is illustrated in Fig. 1 and Fig. 2, where the residual size is markedly larger than the detection thresholds for $t \geq T_0$. The fault approximation performance is shown in Fig. 12, representing the norm of the actual fault versus its estimation. Once the fault has been detected, four isolation observers have been implemented: as $rank\ G(x) = 2\ \ \forall x$, no actuator clusters have been taken into account. The observers have been designed according to (12), with matrices $F_i = diag(-3, -5, -7)\ \forall i = 1, .., 4$ and by tuning the tolerance parameter $\varrho = 0.6$. The norm of residuals, together with an overall isolation threshold, is depicted in Figures 4-7: the reset of residuals to the zero level, corresponding to re-inizialize the observer when $|B_{\bar{x}}| = \varrho$, is clearly visible. The isolation task can be successfully addressed: residuals r_1, r_2, r_3 perceptibly exceed the thresholds, while residual r_4 is not larger than ϵ except for a finite number of negligible neighborhoods of the reset instants. The reconfiguration is performed for $t \geq 50s$. The behavior of the state x_1 and of the virtual input τ is shown in Figures 8-10 for the three admissible scenarios, i.e. nominal system, faulty system without accommodation and faulty system with control reconfiguration: it is noticeable that the original behavior is successfully recovered. Note that reconfiguration could have been made shortly after detection at time $t = 20s$ based on the observed residuals, and the reconfiguration at time $t = 50s$ was made to illustrate the successful computation of residuals with the resetting. Finally the evolution of the redundant inputs u_i is depicted in Figure 11: the three different stages, i.e. *before fault, after fault, after reconfiguration*, are clearly distinguishable.

Besides the mere validation of the theoretical results, it might be interesting to the test the proposed approach in a more practical scenario. While modeling errors can be treated in a natural way by incorporating them in the nonlinear uncertainty $\eta(\cdot, \cdot, \cdot)$, the presence of noisy measurements provides additional challenges [11] [14]. To this end, the robustness of the method with respect to noise has been successfully tested by injecting a zero-mean random signal in the system, and the corresponding isolation residuals are reported in Figures 12-15, which show the effectiveness of the scheme. The isolation thresholds are also affected by the presence of the noise due to the state-dependent bounds $\bar{\eta}(x, t)$. It is worth to notice that the fault diagnosis performances might be further improved by filtering the measured states prior to feed them to the observers.

VIII. Conclusions

In this paper the problem of fault-tolerant control allocation has been addressed for nonlinear systems with a redundant set of actuators. The proposed scheme consists of three main steps: fault detection/approximation, fault isolation and control reconfiguration. Based on the fault diagnosis approach for nonlinear systems introduced in [27] [28], the construction extends to the nonlinear case some fault isolation techniques obtained by the authors in the framework of linear systems with redundant inputs [11]. The key point of the method is the use of a family of unknown input observers that are designed to decouple faults affecting selected actuators or clusters of actuators, the latter corresponding to common mode faults. The observers' parameters design is based on linear algebraic rules, and a logic is provided for resetting the estimators when the magnitude of nonlinearities become too large to be neglected and treated as a disturbance. Once the faults are detected and isolated, the control reconfiguration module is activated and, thanks to the input redundancy, a reduced-order control application policy is enforced: the actuators that are identified as faulty are not used or strongly weighted, i.e. the desired control effect is produced by the joint action of the healthy devices only. A procedure dedicated to generalize the results to the challenging case of unmeasured states is also provided. A simulation study has been included to validate the theoretical results and illustrate the efficiency of the proposed fault diagnosis method for nonlinear overactuated systems in the presence of uncertainties.

Acknowledgments

This work is part of the work carried out at AMOS. It is supported by the Research Council of Norway through the Centres of Excellence funding scheme, project No. 223254 - AMOS.

REFERENCES

1. S.P. Bhat and D.S. Bernstein (2000), Finite-time stability of continuous autonomous systems, *SIAM J. Control Optimization*, 38, 751-766.
2. M. Bodson (2002), Evaluation of optimization methods for control allocation, *J. of Guidance, Control and Navigation*, 25, 703-711.
3. J.M. Buffington and D.F. Enns (1996), Lyapunov stability analysis of daisy chain control allocation, *J. of Guidance, Control and Navigation*, 19, 1226-1230.
4. J.J. Burken, P. Lu, Z.L. Wu and C. Bahm (2001), Two reconfigurable flight control design methods: robust servomechanisms and control allocation, *J. of Guidance, Control and Navigation*, 24, 482-493.
5. A. Casavola and E. Garone (2010), Fault-tolerant adaptive control allocation schemes for overactuated systems, *Int. J. Robust and Nonlinear Control*, vol. 20, 1958-1980.
6. J. Chen, R.J. Patton and H.Y. Zhang (1996), Design of unknown input observers and robust detection filters, *Int. J. of Control*, 63, 85-105.
7. M. Cocetti, A. Serrani and L. Zaccarian (2016), Dynamic input allocation for uncertain linear over-actuated systems. *American Control Conference*, 2906-2911.
8. M.L. Corradini, G. Orlando and G. Parlangeli (2005), A fault tolerant sliding mode controller for accommodating actuator failures, *Proc. 44th IEEE Conf. on Decision and Control*, 3091-3097.
9. M.L. Corradini and A. Cristofaro (2016), A non-linear fault-tolerant thruster allocation architecture for underwater remotely operated vehicles, *IFAC PapersOnLine*, 49(23), 285-290.
10. A. Cristofaro and T.A. Johansen (2013), Fault-tolerant control allocation: an Unknown Input Observer based approach with constrained output fault directions, *Proc. 52nd IEEE Conf. on Decision and Control*, 3818-3824.
11. A. Cristofaro and T.A. Johansen (2014), Fault-Tolerant Control Allocation using Unknown Input Observers, *Automatica*, 50 (7), 1891-1897.
12. A. Cristofaro and T.A. Johansen (2014), Fault-tolerant control allocation with actuator dynamics: finite-time control reconfiguration, *Proc. 53rd IEEE Conf. on Decision and Control*, 4971-4976.
13. A. Cristofaro and M. Sassano (2016), Design of unknown input observers for nonlinear systems with full and partial information, *55th IEEE Conf. on Decision and Control*, 7129-7134.
14. A. Ditkowski, A. Bhandari, and B.W. Sheldon (2008), Computing derivatives of noisy signals using orthogonal functions expansions, Journal of Scientific Computing, 36(3), 333-349.
15. W.C. Durham (1993), Constrained control allocation, *J. of Guidance, Control and Navigation*, 16, 717-725.
16. X. Fan and M. Arcak (2003), Observer design for systems with multivariable monotone nonlinearities, *Systems & Control Letters* 50(4), 319-330.
17. M.T. Hamayun, C. Edwards and H. Alwi (2013), A fault tolerant control allocation scheme with output integral sliding modes, *Automatica*, 49, 1830-1837.
18. O. Härkegård (2004), Dynamic control allocation using constrained quadratic programming, *J. of Guidance, Control and Navigation*, 27, 1028-1034.
19. L. Imsland, T.A. Johansen, H.F. Grip and T.I. Fossen (2007), On non-linear unknown input observers – applied to lateral vehicle velocity estimation on banked roads, *Int. J. of Control*, 80(11), 1741-1750.
20. T.A. Johansen and T.I. Fossen (2013), Control allocation: A survey, *Automatica*, 49, 1087-1103.
21. Z. Luo and H. Fang (2013), Fault detection for nonlinear systems with unknown input, *Asian Journal of Control*, 15(5), 1503-1509.
22. N. Sarkar, T.K. Podder and G. Antonelli (2002), Fault-accommodating thruster force allocation for an AUV considering thruster redundancy and saturation, *IEEE Trans. on Robotics and Automation*, 18, 223-233.
23. J. Tjønnås and T.A. Johansen (2007), Optimizing adaptive control allocation with actuator dynamics, *Proc. 46th IEEE Conf. on Decision and Control*, 3780-3785.
24. J. Tjønnås and T.A. Johansen (2008), Adaptive control allocation, *Automatica*, 44, 2754-2766.
25. L. Zaccarian (2009), Dynamic allocation for input redundant control systems, *Automatica*, 45, 1431-1438.
26. Y. Zhang, S. Suresh, B. Jiang and D. Theilliol (2007), Reconfigurable control allocation against aircraft control effector failures, *Proc. 16th IEEE Conf. on Control Applications*, 1197-1202.
27. X. Zhang, M.M. Polycarpou and T. Parisini (2002), A robust detection and isolation scheme for abrupt and incipient faults in nonlinear systems, *IEEE Trans. on Automatic Control*, 47(4), 576-593.

28. X. Zhang, T. Parisini and M.M. Polycarpou (2004), Adaptive fault-tolerant control of nonlinear uncertain systems: an information-based diagnostic approach, *IEEE Trans. on Automatic Control*, 49(8), 1259-1274.
29. X. Zhang, M.M. Polycarpou and T. Parisini (2008), Design and analysis of a fault isolation scheme for a class of uncertain nonlinear systems, *Annual Reviews in Control*, 32(1), 107-121.
30. X. Zhang, M.M. Polycarpou and T. Parisini (2010), Fault diagnosis of a class of nonlinear uncertain systems with Lipschitz nonlinearities using adaptive estimation, *Automatica*, 46(2), 290-299.

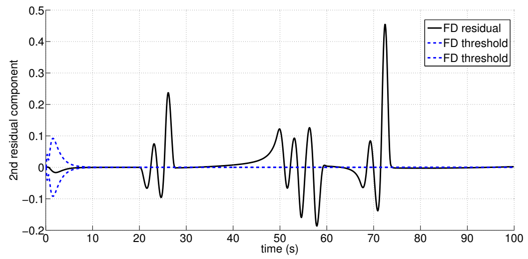

Fig. 1. Fault detection residual: state x_2 (without reconfiguration)

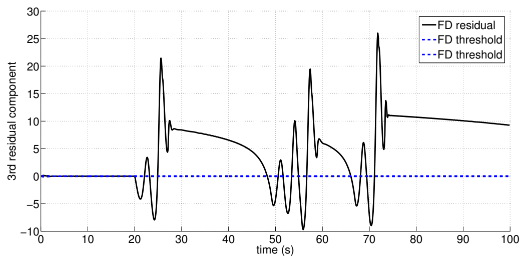

Fig. 2. Fault detection residual: state x_3 (without reconfiguration)

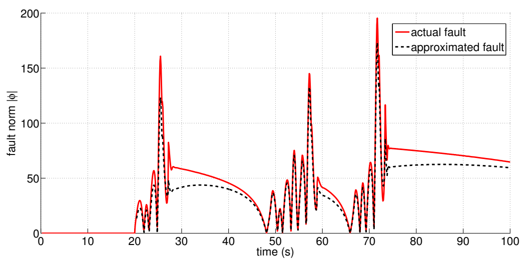

Fig. 3. Norm of the actual fault $\phi(x, u, t)$ and norm of the approximated fault $\hat{\phi}(x, u, t)$ (without reconfiguration)

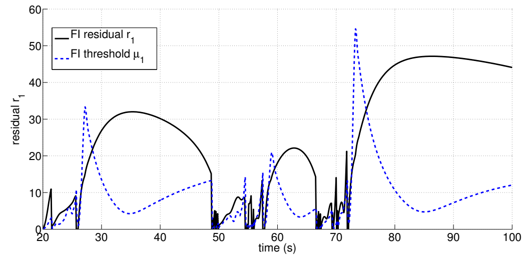

Fig. 4. Fault isolation: norm of residual r_1

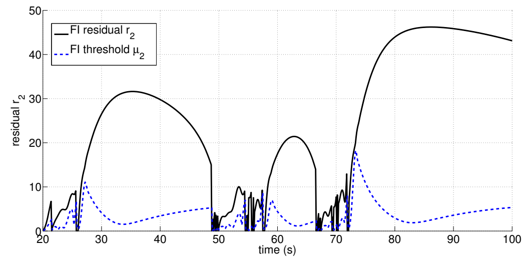

Fig. 5. Fault isolation: norm of residual r_2

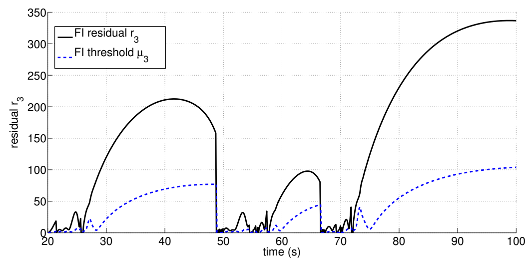

Fig. 6. Fault isolation: norm of residual r_3

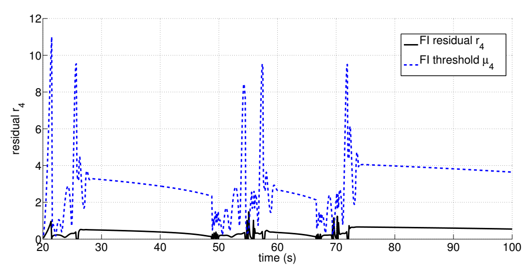

Fig. 7. Fault isolation: norm of residual r_4

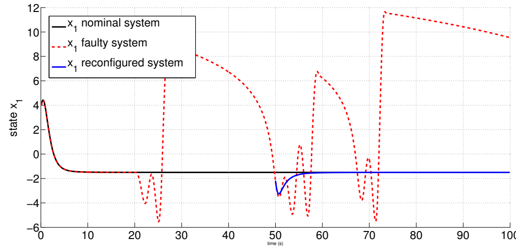

Fig. 8. State x_1 for the three scenarios: nominal system, faulty actuator u_4 and control reconfiguration at $t = 50$

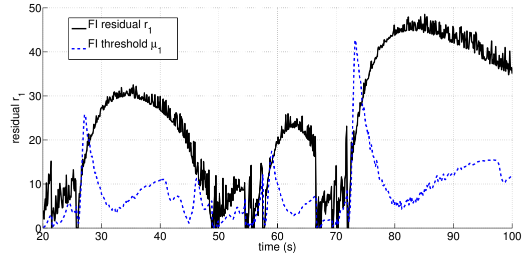

Fig. 12. Fault isolation: norm of residual r_1 subject to output noise

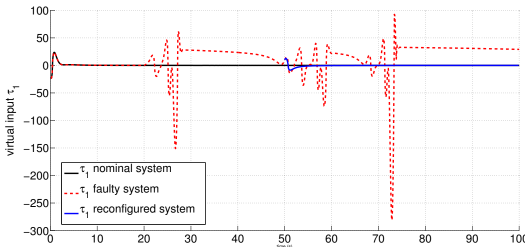

Fig. 9. Virtual input τ_1 for the three scenarios: nominal system, faulty actuator u_4 and control reconfiguration at $t = 50$

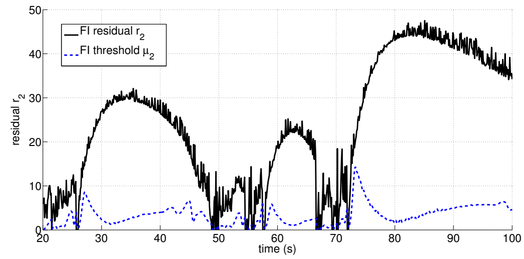

Fig. 13. Fault isolation: norm of residual r_2 subject to output noise

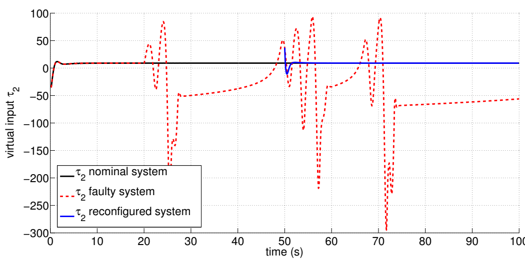

Fig. 10. Virtual input τ_2 for the three scenarios: nominal system, faulty actuator u_4 and control reconfiguration at $t = 50$

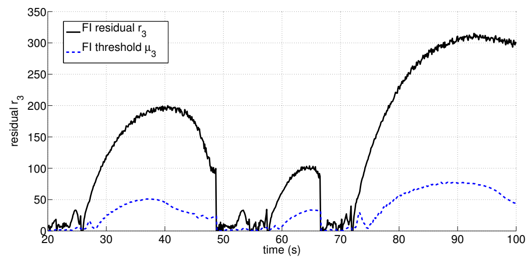

Fig. 14. Fault isolation: norm of residual r_3 subject to output noise

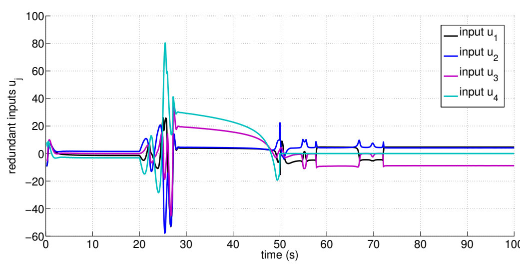

Fig. 11. Redundant control inputs u_1, u_2, u_3, u_4

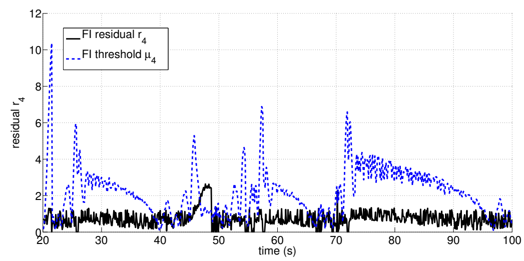

Fig. 15. Fault isolation: norm of residual r_4 subject to output noise