Proceedings of the
44th IEEE Conference on Decision and Control, and
the European Control Conference 2005
Seville, Spain, December 12-15, 2005



# Conditions for Detecting and Isolating Sets of Faults in Nonlinear Systems

Raffaella Mattone Alessandro De Luca

*Abstract*— **Consider a nonlinear dynamic system affected by possibly concurrent faults (and disturbances). If we wish to detect and isolate each single fault from all other, possibly concurrent faults and disturbances (i.e., to solve the standard Fault Detection and Isolation (FDI) problem), some necessary conditions of differential geometric nature should be satisfied. To deal with cases when these conditions are structurally violated, we introduce a more general class of FDI problems, referred to as Fault Set Detection and Isolation (FSDI), where the focus of the isolation issue is moved from single to sets of faults. Different formulations of FSDI problems are given, necessary and sufficient conditions for their solution are provided, and the design of a hybrid residual generator is presented. For the case of non-concurrent faults, it is possible to detect and isolate even single faults under weaker necessary conditions, by processing output residuals that solve suitable FSDI problems. A robotic example is presented to illustrate the theory.**

*Index Terms*— **Fault detection and isolation, fault sets, residual matrix, isolation logics, nonlinear control.**

## I. Introduction

Fault tolerant operation of complex dynamic plants requires embedding in the automatic control system a scheme for detecting the occurrence of faults and for isolating each of them from other possible faults and from disturbances (the standard FDI problem) [1].

The FDI problem for systems modeled by nonlinear affine dynamics has recently received special attention [2], [3], [4]. In [2], necessary and sufficient conditions for detection and isolation of single or multiple concurrent faults have been determined, using a differential geometric approach. When the stated necessary conditions are satisfied, under some additional technical assumptions, this approach enables the design of residual generators that solve the standard FDI problem. However, these conditions may be violated in many cases of practical interest, e.g., when the number of possible faults affecting the system exceeds the dimension of the state space. Thus, in order to be solvable, the FDI problem must be given a different formulation, in particular, moving the focus of the isolation issue from single to sets of faults. This can be done in several ways and we refer to this more general class of FDI problems as *Fault Set Detection and Isolation* (FSDI).

A first formulation in the FSDI class is characterized by the ability to recognize the occurrence of one or more faults in a given set, without distinguishing among the different faults in the set. We refer to this relaxed FDI problem as *Standard Fault Set Detection and Isolation* (SFSDI). This problem is relevant, e.g., when the same recovery procedure applies to different faults that can be thus grouped in a single fault set. A different approach to FSDI consists in trying to identify 'as close as possible', in any faulty situation, the set of faults that is currently affecting the system (set of *active* faults). This is another relaxed version of the standard FDI problem, since it is implicitly accepted that the set of fault *candidates* includes (but, in general, does not coincide) with that of active faults. We refer to this problem as *Candidate Fault Set Detection and Isolation* (CFSDI). Finally, another direction for relaxing the available necessary conditions for FDI exploits the issue of concurrency. In fact, while the general result in [2] allows full concurrency of faults and/or disturbances, most of the times multiple concurrent faults are rare events in practice. We shall see that the necessary conditions for FDI of non-concurrent faults (*Non-Concurrent Fault Detection and Isolation*, or N-CFDI) are considerably weaker than those for standard FDI, and can be obtained as a suitable application of the results on CFSDI. For the actual solution of these fault detection and isolation problems, a hybrid residual generator structure can be used, processing the continuous-time diagnostic signals designed with differential geometric techniques through a combinatorial isolation logics.

The paper is organized as follows. In Sect. II, the conditions for FDI given in [2] are briefly recalled. The three subsections of Sect. III contain the formulations of the SFSDI, CFSDI and N-CFDI problems, and present the main results. A robotic example is analyzed in Sect. IV. Background material is provided in Appendix.

## II. Necessary conditions for FDI

We consider the general nonlinear system

$$\begin{aligned} \dot{x} &= g_0(x) + \sum_{k=1}^{m} g_k(x)u_k + \sum_{i=1}^{s} l_i(x)f_i + \sum_{j=1}^{d} n_j(x)w_j \\ y &= h(x), \end{aligned} \tag{1}$$

with state $x \in \mathbb{R}^n$, inputs $u_k$, $k = 1, \ldots, m$ (controls), $f_i$, $i = 1, \ldots, s$ (faults), and $w_j$, $j = 1, \ldots, d$ (disturbances), measured output $y \in \mathbb{R}^q$, and where $g_0(x), \ldots, g_m(x)$, $l_1(x), \ldots, l_s(x)$, $n_1(x), \ldots, n_d(x)$ are smooth vector fields and $h(x)$ is a smooth mapping.

For system (1), affected by the possibly concurrent faults $f_1, \ldots, f_s$, the standard *Fault Detection and Isolation* (FDI) problem can be concisely formulated as that of designing a

Work supported by the EU project EU-IST-2001-32122 *IFATIS*

R. Mattone and A. De Luca are with Dipartimento di Informatica e Sistemistica, Università di Roma "La Sapienza", Via Eudossiana 18, 00184 Roma, Italy {deluca,mattone}@dis.uniroma1.it

bank of $s$ *filters* (referred to as *residual generators*), having as inputs the $u_k$'s, $k = 1, \ldots, m$ and $y$ of eq. (1), and with outputs $r_1, \ldots, r_s$ (the *residuals*), such that, for each $\kappa = 1, \ldots, s$, residual $r_\kappa$ is affected by $f_\kappa$, is decoupled from the other faults $f_i$ ($i \neq \kappa$) and disturbances $w_j$, and asymptotically converges to zero whenever $f_\kappa \equiv 0$.

Necessary conditions for the solvability of the stated problem have been proven in [2] and are briefly recalled here. Let $P_\kappa$ be the distribution generated by the vector fields $l_i$, $i \neq \kappa$, and $n_j$, $j = 1, \ldots, d$, i.e.,

$$P_\kappa = \text{span}\,\{l_1, \ldots, l_{\kappa-1}, l_{\kappa+1}, \ldots, l_s, n_1, \ldots, n_d\}\,, \quad (2)$$

and define $\Sigma_*^{P_\kappa}$ as the smallest involutive distribution containing $P_\kappa$ and conditioned invariant for system (1) in the absence of faults and disturbances ($l_i \equiv 0$, $n_j \equiv 0$).

Following the differential geometric approach of [2], let $\text{o.c.a.}\left(\left(\Sigma_*^{P_\kappa}\right)^\perp\right)$ be the result of the *observability codistribution algorithm* applied to the codistribution $(\Sigma_*^{P_\kappa})^\perp$ (see Appendix). Then, a solution to the standard FDI problem exists only if

$$\text{span}\,\{l_\kappa\} \not\subseteq \left[\text{o.c.a.}\left((\Sigma_*^{P_\kappa})^\perp\right)\right]^\perp, \quad \kappa = 1, \ldots, s. \quad (3)$$

Condition (3) implies the weaker necessary condition

$$\text{span}\,\{l_\kappa\} \not\subseteq P_\kappa, \quad \kappa = 1, \ldots, s. \quad (4)$$

It is clear that condition (4) cannot be verified for more than $n$ faults at the same time (in the best case, i.e., when no disturbances affect the system), being $n$ the dimension of the state space. Thus, the maximum number of possibly concurrent faults that can be detected and isolated is certainly less than or equal to $n$.

Under suitable technical assumptions (see [2, Proposition 5 and Assumption II]), the necessary condition (3) is also sufficient (and constructive) for the solution of the stated FDI problem. The following hypothesis is then useful to simplify the statement of most results in this paper.

**Hypothesis 1:** Consider system (1) with state $x \in I\!R^n$, a generic fault vector field $l$ and a generic distribution $\Delta$ both defined on $I\!R^n$. Whenever

$$\text{span}\,\{l\} \not\subseteq \left[\text{o.c.a.}\left((\Sigma_*^{\Delta})^\perp\right)\right]^\perp, \quad (5)$$

then it is possible to design a residual generator that detects and isolates the fault $f$ associated to vector field $l$ from any fault and disturbance whose vector fields lie in $\Delta$. ◇

Hypothesis 1 is verified, e.g., every time the whole state is measurable ($h(x) = x$).

## III. Fault Set Detection and Isolation

For the nonlinear system (1), the violation of the necessary condition (3) for some $\kappa$ implies that not every fault can be detected and isolated from *all* other possibly *concurrent* fault inputs and disturbances. It is then natural to ask *i)* if it is still possible to detect when some fault is affecting the system (*detection* issue) and *ii)* how it is possible to characterize the different faulty situations that the system may experience (*isolation* issue). Clearly, the isolation problem at item *ii)*, independently of its precise formulation, only makes sense when fault detection is feasible, i.e., when all faults $f_1, \ldots, f_s$ can be at least discriminated from disturbances. Therefore, we make here a well-posedness assumption.

**Assumption 1:** All faults $f_1, \ldots, f_s$ are *detectable*, i.e., it holds

$$\text{span}\,\{l_\kappa\} \not\subseteq \left[\text{o.c.a.}\left((\Sigma_*^{\mathcal{N}})^\perp\right)\right]^\perp, \quad \kappa = 1, \ldots, s, \quad (6)$$

where $\mathcal{N} = \text{span}\{n_1, \ldots, n_d\}$. ◇

In order to overcome the violation of condition (3), the original FDI problem formulation in [2] should be relaxed. Hereafter, we move the focus of the isolation issue from single to suitable sets of faults in different ways.

### A. Standard Fault Set Detection and Isolation

**SFSDI problem:** Let $S = \{f_{k_1}, \ldots, f_{k_\nu}\}$ be a given subset of the fault inputs $f_1, \ldots, f_s$ possibly affecting system (1). Find, if possible, a dynamic system whose output $r$ is affected by *each* fault in $S$, is *not* affected by any other fault $f_i$, $i \notin \{k_1, \ldots, k_\nu\}$ or disturbance $w_j$, $j = 1, \ldots, d$, and asymptotically converges to zero whenever all fault inputs in $S$ are zero. If the stated problem is solvable for $S$, we call $S$ an *FDI-set* and say that it is *detected and isolated* by residual $r$. ◇

The following result can be readily established for the solvability of SFSDI problem.

**Proposition 1:** Let $S = \{f_{k_1}, \ldots, f_{k_\nu}\}$, and $P = \text{span}\,\{l_i,\ i \notin \{k_1, \ldots, k_\nu\}, n_1, \ldots, n_d\}$. The SFSDI problem is solvable for $S$ (i.e., $S$ is an FDI-set) if and only if (sufficiency holds under Hypothesis 1)

$$\text{span}\,\{l_k\} \not\subseteq \left[\text{o.c.a.}\left((\Sigma_*^{P})^\perp\right)\right]^\perp, \ \forall k \in \{k_1, \ldots, k_\nu\}. \quad (7)$$

*Proof:* The necessity of (7) directly follows from the general necessary condition (3). For the sufficiency, if Hypothesis 1 and condition (7) hold, then for any fault $f_k \in S$ a residual $r_k$ can be found, which is affected by $f_k$ and not affected by any fault or disturbance out of $S$, so that the set $S$ is detected and isolated by the residual

$$r = r_{k_1}^2 + \ldots + r_{k_\nu}^2. \quad (8)$$

■

We give now a structural characterization of *all* sets $S$ for which the solvability of the SFSDI problem can be guaranteed, i.e., that turn out to be FDI-sets[1]. For this, the following definition is needed.

**Definition 1 (Minimal FDI-Set):** Let $S = \{f_{k_1}, \ldots, f_{k_\nu}\}$ be a given subset of the fault inputs $f_1, \ldots, f_s$ possibly affecting system (1). We say that $S$ is a *minimal FDI-set* if *i)* it is an FDI-set, and *ii)* does not strictly include any other FDI-set. ◇

For system (1), minimal FDI-sets are a finite number $N_r$ and constitute a basis for determining all possible FDI-sets. In fact, the following result can be readily established.

[1]Under Assumption 1 and Hypothesis 1, note that at least one FDI-set always exists, i.e., the trivial set of all faults $\{f_1, \ldots, f_s\}$.

**Proposition 2:** Any FDI-set $S$ for system (1) can be written as

$$S = \bigcup_{k=1}^{N_r} \alpha_k \, S_k^{\min}, \quad \alpha_k \in \{0,1\}, \tag{9}$$

where $S_k^{\min}$, $k = 1, \ldots, N_r$, are all minimal FDI-sets for system (1). ■

For the actual computation of the list $S_{\text{list}}$ of all minimal FDI-sets $S_1^{\min}, \ldots, S_{N_r}^{\min}$ for system (1), a recursive algorithm having the structure of a tree exploration can be devised. The *root* of the tree corresponds to the trivial FDI-set $\{f_1, \ldots, f_s\}$. The *children* of each node are all subsets obtained by removing one element from the parent set. The exploration proceeds in depth as far as the current set/node includes at least one fault that can be isolated from all faults and disturbances outside the set. When this does not hold anymore, the algorithm steps back to the parent node and explores the other children. When no child allows the prosecution of the search, then the current node necessarily corresponds to a minimal FDI-set. This algorithm can be compactly described by the following pseudo-code (symbol $\backslash$ denotes set difference operation).

**Minimal FDI-sets Algorithm:**

$L = L_0 = \{l_1, \ldots, l_s\}$;
$S_{\text{list}} = \{\emptyset\}$;
$k = 0$;
$[S_{\text{list}}, N_r] = \text{explore}(L, S_{\text{list}}, k)$;

with

function $[S_{\text{list}}, k] = \text{explore}(L, S_{\text{list}}, k)$
{ $k_{loc} = k$;
$P = \text{span}\{n_1, \ldots, n_d\} + \text{span}\{L_0 \backslash L\}$;
if $\exists\, l_\sigma \in L : \quad \text{span}\{l_\sigma\} \not\subseteq \left[\text{o.c.a.}\left((\Sigma_*^P)^\perp\right)\right]^\perp$
{ for $l_i \in L$
$[S_{\text{list}}, k] = \text{explore}(L \backslash l_i, S_{\text{list}}, k)$;
if $k == k_{loc}$
{ $k = k + 1$;
$S_k^{\min} = \{f_j : \quad l_j \in L\}$;
$S_{\text{list}} = \{S_{\text{list}}, S_k^{\min}\}$;
};
};
}.

In general, minimal FDI-sets have different cardinalities and may have non-empty intersections. Furthermore, under Assumption 1, each fault $f_\kappa$ is contained in at least one minimal FDI-set. In particular, if the standard FDI problem given in [2] is solvable for $f_\kappa$, then the only minimal FDI-set containing $f_\kappa$ is the set $\{f_\kappa\}$ itself. Finally, for minimal FDI-sets, the associated SFSDI problem is solved by any single residual signal in the rhs of eq. (8) (as opposed to their squared sum). In fact, every residual $r_k$ that detects and isolates a fault in a minimal FDI-set $S_k^{\min}$ from all faults and disturbances out of $S_k^{\min}$, is necessarily affected by all faults in $S_k^{\min}$.

Due to the structure (9), it follows also that every FDI-set $S$ is detected and isolated by the residual $r = \sum_{k=1}^{N_r} \alpha_k \, r_k^2$, such that $r_k$ is any diagnostic signal that detects and isolates $S_k^{\min}$. Thus, any set of residuals $\mathcal{R} = \{r_1, \ldots, r_{N_r}\}$, with $r_k$ designed to detect and isolate $S_k^{\min}$, provides all available information about detection and isolation of (sets of) faults for system (1). Such information can be completely summarized by a *residual matrix*, i.e., a binary matrix $RM$ whose entry $RM(i,k)$ is '1' if fault $f_i$ is in the minimal FDI-set $S_k^{\min}$, or, equivalently, if $f_i$ affects the corresponding residual $r_k$. In the following, we refer to such a set $\mathcal{R} = \{r_1, \ldots, r_{N_r}\}$ as a *residual basis* for system (1).

**Remark 1:** The definition of the residual matrix $RM$ only relies on the knowledge of the system vector fields, which are sufficient to compute all minimal FDI-sets, and is therefore independent of the particular residual basis $\mathcal{R}$. This means that the whole analysis can be performed without the need of actually designing the specific residual generators (see Sect. IV).

### *B. Candidate Fault Set Detection and Isolation*

Assume that a faulty situation is caused by the (yet unknown) set of active faults $S_a = \{f_{a_1}, \ldots, f_{a_\nu}\}$. In order to identify as close as possible the set $S_a$, we have to look at the behavior of a residual basis $\mathcal{R} = \{r_1, \ldots, r_{N_r}\}$. In fact, such basis provides all available information that can be used for isolation purposes. In particular, if a residual $r_k \in \mathcal{R}$ is being affected by the current faulty situation, we can conclude that one or more faults of the associated minimal FDI-set $S_k^{\min}$ are in the active set $S_a$. On the other hand, if a residual $r_j$ is not being affected, we can certainly exclude the occurrence of any of the faults in the associated minimal FDI-set $S_j^{\min}$. This *exonerating* logics suggests the introduction of a further class of fault sets that extends the structure (9) of FDI-sets.

**Definition 2 (Exonerated FDI-set):** We define as an *exonerated FDI-set* for system (1) any fault set $S^{\text{exo}}$ that can be written in the form

$$S^{\text{exo}} = \left\{ \bigcup_{k=1}^{N_r} \alpha_k \, S_k^{\min} \right\} \setminus \left\{ \bigcup_{k=1}^{N_r} \bar{\alpha}_k \, S_k^{\min} \right\}, \quad \alpha_k \in \{0,1\}, \tag{10}$$

being $S_1^{\min}, \ldots, S_{N_r}^{\min}$ all minimal FDI-sets for system (1), and $\bar{\alpha}_k = 1 - \alpha_k$. ◇

As a result, a possible set of fault candidates that can be associated to a set $S_a$ of active faults is given by the smallest exonerated FDI-set that includes $S_a$. Correspondingly, we can formulate the following relaxed FDI problem.

**CFSDI problem:** Let $S_a = \{f_{a_1}, \ldots, f_{a_\nu}\}$ be any (possibly empty) set of active faults affecting system (1), and let $\mathcal{C}(S_a)$ be the smallest exonerated FDI-set that includes $S_a$ (referred to as *candidate fault set*). Design a FDI system with inputs $u_1, \ldots, u_m$ and $y$, and outputs $r_{f_1}, \ldots, r_{f_s}$, such that $r_{f_i}$ is affected if $f_i \in \mathcal{C}(S_a)$, is decoupled from all disturbances $w_j$, $j = 1, \ldots, d$, and asymptotically converges to zero whenever $f_i \notin \mathcal{C}(S_a)$. ◇

Based on the arguments presented in Sect. III-A, we can immediately provide a solution to this problem. The residual generator solving the CFSDI problem has the general *hybrid*

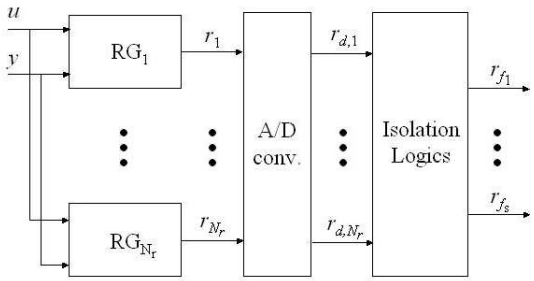


Fig. 1. Structure of a hybrid residual generator solving FSDI problems

structure given in Fig. 1, namely a bank of dynamic filters providing a residual basis $\mathcal{R} = \{r_1, \ldots, r_{N_r}\}$ for system (1), an analog-to-digital conversion block, providing a binary version[2] $\mathcal{R}^d = \{r_1^d, \ldots, r_{N_r}^d\}$ of the basis $\mathcal{R}$, and a combinatorial logics applied to $\mathcal{R}^d$. In particular, each output $r_{f_i}$, $i = 1, \ldots, s$, of this *isolation logics* is active when all minimal FDI-sets including $f_i$ have the corresponding residual affected, i.e.,

$$r_{f_i} = \bigwedge_{f_i \in S_k^{\min}} r_k^d, \tag{11}$$

where the symbol $\bigwedge$ indicates the logical AND operator.

The candidate fault set returned by the above FDI system is

$$\mathcal{C}(S_a) = \left\{ \bigcup_{S_k^{\min} \cap S_a \neq \emptyset} S_k^{\min} \right\} \setminus \left\{ \bigcup_{S_j^{\min} \cap S_a = \emptyset} S_j^{\min} \right\}, \tag{12}$$

i.e., in the form (10) of an exonerated FDI-set, with $\alpha_k = 1$ if $S_k^{\min} \cap S_a \neq \emptyset$. In general, $\mathcal{C}(S_a)$ does not coincide with the set $S_a$ of active faults, but it only satisfies $\mathcal{C}(S_a) \supseteq S_a$. Then, it is natural to ask in which cases $\mathcal{C}(S_a)$ actually coincides with $S_a$ or, equivalently, what are the conditions for $S_a$ to be an exonerated FDI-set. The following result holds.

**Proposition 3:** Let $S_a = \{f_{a_1}, \ldots, f_{a_\nu}\}$ be a set of active faults, and let distribution

$$P_a = \mathrm{span}\{l_{a_1}, \ldots, l_{a_\nu}, n_1, \ldots, n_d\}.$$

The set of fault candidates $\mathcal{C}(S_a)$ coincides with $S_a$, i.e., $S_a$ is an exonerated FDI-set, if and only if

$$\forall i: \; f_i \notin S_a, \quad \mathrm{span}\,\{l_i\} \not\subseteq \left[\text{o.c.a.}\left((\Sigma_*^{P_a})^{\perp}\right)\right]^{\perp}. \tag{13}$$

*Proof:* Violation of (13) implies that, for some 'inactive' fault $f_i$, all minimal FDI-sets including $f_i$ also include some active fault, so that $f_i$ necessarily results to be in the fault candidate set. On the other hand, fulfillment of condition (13) guarantees that, for each inactive fault $f_i$, at least a minimal FDI-set exists, that includes $f_i$ and does not include any active fault. Thus, all inactive faults can be excluded from the fault candidate set and sufficiency holds. ■

**Remark 2:** Note that the geometric condition (13) for exonerated FDI-sets in the form (10) is the equivalent of condition (7) for FDI-sets in the form (9). From an operative point of view, condition (13) may be used in two different ways: *a posteriori*, i.e., after a faulty situation has been detected, for refining the candidate fault set $\mathcal{C}$ provided by the hybrid system in Fig. 1, since the current set $S_a$ of active faults verifies $S_a \not\subseteq \mathcal{C}' \subset \mathcal{C}$, being $\mathcal{C}'$ an exonerated FDI-set itself; or *a priori*, in order to establish off-line for which sets $S_a$ of active faults the FDI problem is still *exactly* solvable, despite of the violation of the general necessary condition (3).

### C. Non-Concurrent Fault Detection and Isolation

The case of non-concurrent faults (i.e., when the set $S_a$ of active faults is always constituted by at most one element) has a special relevance in the framework of the CFSDI problem. In this case, condition (13) can be easily tested for all possible sets of active faults $S_a = \{f_k\}$, $k = 1, \ldots, s$, so as to guarantee that the candidate fault set always coincides with $S_a$, i.e., that each single fault can be isolated from the other faults and disturbances.

**N-CFDI problem:** Assume that, at any time instant, at most one of the $s$ faults $f_1, \ldots, f_s$ can affect system (1) (*non-concurrency* of faults). Then find, if possible, a residual generator that is able to detect and isolate any single fault $f_i$, $i = 1, \ldots, s$, from the other faults $f_k$, $k \neq i$, and the disturbances $w_1, \ldots, w_d$. ◇

The following result immediately follows from the application of Proposition 3 to the case of $S_a$ constituted by at most one fault input.

**Proposition 4:** For each $k = 1, \ldots, s$, define distribution $P_k = \mathrm{span}\{l_k, n_1, \ldots, n_d\}$. The N-CFDI problem is solvable for system (1) if and only if (sufficiency holds under Hypothesis 1)

$$\mathrm{span}\,\{l_i\} \not\subseteq \left[\text{o.c.a.}\left((\Sigma_*^{P_k})^{\perp}\right)\right]^{\perp}, \quad \forall i, k, \; i \neq k. \tag{14}$$

■

**Remark 3:** Condition (14) implies that, for each couple of faults $f_i$ and $f_k$, there always exists a minimal FDI-set that includes $f_i$ but not $f_k$, so that the corresponding rows of the residual matrix $RM$ are certainly different (there is a column with a '1' at row $i$ and a '0' at row $k$) and non-zero.

**Remark 4:** Since the N-CFDI problem can be considered a special instance of CFSDI, the same hybrid residual generator of Fig. 1 can be used for its solution. In this special case, however, the computation of the *whole* residual basis $\mathcal{R} = \{r_1, \ldots, r_{N_r}\}$, of cardinality $N_r$, is not required, in general, to solve the problem. In fact, it can be shown that a number $\sigma$, with $\lceil \log_2 s \rceil \leq \sigma \leq s$, of suitably chosen residuals is always sufficient to solve the N-CFDI problem.

[2]In the simplest case, the digital residual $r_i^d \in \{0, 1\}$, $i = 1, \ldots, s$, is the result of the comparison $|r_i| > T_i$, being $T_i$ a suitable threshold value taking into account the overall level of noise affecting the analogical residual $r_i$.

## IV. A ROBOT EXAMPLE

In this section we will describe the application of the proposed FSDI techniques to a robotic example, a $2R$ planar manipulator under gravity, equipped with a force sensor for measuring possible contacts between the end-effector and the environment. This mechanical system can be modeled by Euler-Lagrange equations of the form

$$B(q)\ddot{q} + c(q,\dot{q}) + e(q) = \tau + J^{\mathrm{T}}(q)F + \sum_{i=1}^{s} \hat{l}_i(q) f_i, \quad (15)$$

where $q \in I\!R^2$ is the joint variable vector, $B(q)$ is the positive definite symmetric inertia matrix, $c(q,\dot{q})$ is the vector of centrifugal and Coriolis terms, $e(q)$ collects the gravitational terms, $\tau \in I\!R^2$ is the vector of control torques, $F \in I\!R^2$ is the vector of external forces acting on the robot end-effector and $J(q)$ is the associated Jacobian matrix (transforming joint to end-effector linear velocities). The expression of the dynamic terms $B(q)$, $c(q,\dot{q})$ and $e(q)$ is

$$B(q) = \begin{bmatrix} a_1 + 2a_2c_2 & a_3 + a_2c_2 \\ a_3 + a_2c_2 & a_3 \end{bmatrix},$$

$$c(q,\dot{q}) = \begin{bmatrix} -a_2\dot{q}_2\,(\dot{q}_2 + 2\dot{q}_1)\,s_2 \\ a_2\dot{q}_1^2 s_2 \end{bmatrix}, \; e(q) = \begin{bmatrix} a_4 s_1 + a_5 s_{12} \\ a_5 s_{12} \end{bmatrix},$$

where a shorthand notation for sine/cosine has been used (e.g., $s_{12} = \sin(q_1 + q_2)$), $(q_1, q_2) = 0$ is the asymptotically stable, free equilibrium configuration, and the dynamic coefficients $a_i$ ($i = 1, \ldots, 5$) depend on the link masses and inertias.

The vector of external forces $F = (F_X, F_Y)$ is naturally expressed in the frame attached to the force sensor, with the $X$-axis rotated by an angle $\alpha$ w.r.t. the second robot link (the reason for this angular displacement will be clear in the following). Accordingly, the Jacobian matrix in eq. (15) takes the form

$$J(q) = \begin{bmatrix} \ell_1 \sin(q_2 + \alpha) + \ell_2 \sin\alpha & \ell_2 \sin\alpha \\ \ell_2 \cos\alpha + \ell_1 \cos(q_2 + \alpha) & \ell_2 \cos\alpha \end{bmatrix}, \quad (16)$$

where $\ell_1$, $\ell_2$ are the lengths of the two robot links.

The last term in eq. (15) models the faults possibly affecting the mechanical system, appearing at the *acceleration level* through smooth vector fields $\hat{l}_i(q)$ that only depend on joint positions $q$. The following faults are considered:

- *Actuator faults:* The actual torque applied by the possibly failed actuators is $\tau = \tau_c + f_\tau$, where $\tau_c$ is the commanded torque. Note that by $f_\tau$ we can capture any type and time profile of actuator faults (see [5] for a complete list). For this kind of fault, the fault vector fields in (15) are $\hat{l}_i(q) = E_i$, $i = 1, 2$, being $E_i$ the $i$-th column of the $(2 \times 2)$ identity matrix.
- *Force sensor faults:* These are defined by $f_F = F - F_m$, where $F$ is the actual vector of external forces applied to the robot end-effector and $F_m$ is the corresponding measure provided by the force sensor. Hence, the fault vector fields in (15) are in this case $\hat{l}_i(q) = j_i^T(q)$, $i = 1, 2$, where $j_i(q)$ is the $i$-th row of the Jacobian $J(q)$.

TABLE I
RESIDUAL MATRIX ASSOCIATED TO SYSTEM (17–19)

| minimal FDI-set (residual) / fault | $S_1^{\min}$ ($r_1$) | $S_2^{\min}$ ($r_2$) | $S_3^{\min}$ ($r_3$) | $S_4^{\min}$ ($r_4$) |
|---|---|---|---|---|
| $f_1 = f_{\tau_1}$ | 1 | 0 | 1 | 1 |
| $f_2 = f_{\tau_2}$ | 0 | 1 | 1 | 1 |
| $f_3 = f_{F_X}$ | 1 | 1 | 1 | 0 |
| $f_4 = f_{F_Y}$ | 1 | 1 | 0 | 1 |

Considering the possible occurrence of all the above faults ($s = 4$) and the absence of any further disturbance ($d = 0$), the robot model (15) rewritten in the state-space form (1) becomes

$$\dot{x} = g_0(x) + \sum_{k=1}^{m} g_k(x) u_k + \sum_{i=1}^{s} l_i(x) f_i, \quad (17)$$

with state $x = (x_1, x_2) = (q, \dot{q})$ of dimension $n = 4$, input vector $u = (\tau_c, F_m)$ of dimension $m = 4$, and where

$$g_0(x) = \begin{bmatrix} x_2 \\ -B^{-1}(x_1)\,[c(x) + e(x_1)] \end{bmatrix}. \quad (18)$$

The other vector fields $g_k$ and $l_i$ have the first $N = 2$ components equal to zero. In particular, it is

$$l_i(x) = \begin{bmatrix} \mathrm{O}_N \\ B^{-1}(x_1) \end{bmatrix} \hat{l}_i(x_1), \quad i = 1, \ldots, 4. \quad (19)$$

Correspondingly, it is $f_{1,2} = f_{\tau_1,\tau_2}$ and $f_{3,4} = f_{F_X,F_Y}$. As for the system output, the full robot state is assumed measurable (joint positions and velocities are measured, respectively, by encoders and tachometers), so that $y = x \in I\!R^4$ and Hypothesis 1 holds.

For a nonlinear mechanical system in the form (17–19), the necessary (and sufficient, by virtue of the full state availability) condition (3) for the detection and isolation of possibly concurrent faults coincides with condition (4), since $\left[\text{o.c.a.}\left((\Sigma_*^{P_\kappa})^\perp\right)\right]^\perp \equiv P_\kappa$.

It is readily verified that condition (4) is generically violated for any $l_\kappa$, $\kappa = 1, \ldots, 4$. Thus, none of the faults possibly affecting the robot system can be exactly isolated from *all* other, possibly concurrent, faults. Then, the first step for applying the results of Sect. III consists in the computation of all minimal FDI-sets $S_i^{\min}$, and thus of the system residual matrix. In particular, for $\alpha \notin \{0, \pi\}$, the application of the Algorithm presented in Sect. III-A yields $N_r = 4$ minimal FDI-sets

$$\begin{aligned} S_1^{\min} &= \{f_1, f_3, f_4\}, \quad S_2^{\min} = \{f_2, f_3, f_4\}, \\ S_3^{\min} &= \{f_1, f_2, f_3\}, \quad S_4^{\min} = \{f_1, f_2, f_4\}, \end{aligned} \quad (20)$$

corresponding to the residual matrix of Table I.

All possible FDI-sets are those in (20), plus the trivial FDI-set $\{f_1, \ldots, f_4\}$ (see eq. (9)). According to eq. (10), all possible exonerated FDI-sets are:

$$\begin{aligned} S_1^{\text{exo}} &= \{f_1\}, \quad S_2^{\text{exo}} = \{f_2\}, \\ S_3^{\text{exo}} &= \{f_3\}, \quad S_4^{\text{exo}} = \{f_4\}, \\ S_5^{\text{exo}} &= \{f_1, f_2, f_3, f_4\}. \end{aligned} \quad (21)$$

The sets in (21) show that, for the considered robotic system, only non-concurrent faults can be isolated, while any set $S_a$ of multiple concurrent faults necessarily results in the 'trivial' set of fault candidates $\mathcal{C}(S_a) = S_5^{\text{exo}} = \{f_1, f_2, f_3, f_4\}$, i.e., the only exonerated FDI-set that includes more than one fault input. As a consequence, only the N-CFDI problem is of interest for the presented case study. With this respect, Table I shows that this problem is solved by the residuals $r_1, \ldots, r_3$ (in fact, columns 1 to 3 of the residual matrix have all different and non-zero rows —see Remarks 3 and 4). Although the implementation of the whole residual basis $\mathcal{R} = \{r_1, \ldots, r_4\}$ is not required to solve the problem, the inclusion of residual $r_4$ guarantees that all rows of the residual matrix differ for at least two elements, instead of just one, and allows to recognize also the violation of the non-concurrency assumption (when all residuals are excited), thus increasing the overall robustness of the FDI system. The isolation logics in Fig. 1 is based on Table I.

The whole analysis has been performed independently of the actual design of the residual generators. Residuals can be generated following the general method in [5]. For example, a possible residual $r_2$ for the set $S_2^{\min}$ is

$$r_2 = k_2 \left[ \int (\tau_{c2} - \phi_2 - r_2) dt - p_2 \right], \qquad (22)$$

for $k_2 > 0$, with

$$\phi_2 = a_2 \dot{q}_1 (\dot{q}_1 + \dot{q}_2) s_2 + a_5 s_{12} - \ell_2 (F_{Xm} \sin\alpha + F_{Ym} \cos\alpha),$$

and with the second component of the generalized momentum vector [6]

$$p_2 = (a_3 + a_2 c_2)\dot{q}_1 + a_3 \dot{q}_2.$$

The dynamics of this residual is

$$\dot{r}_2 = -k_2 r_2 + k_2 \left[ f_{\tau_2} + E_2^T B^{-1}(q) J^T(q) f_F \right]. \qquad (23)$$

Finally, note that when $\alpha = 0$ in eq. (16), i.e., when the $X$-axis of the force sensor frame is aligned with the second robot link, it is span$(l_3) \subseteq$ span$(l_1)$, so that condition (14) is certainly violated (in particular, for $i = 3$ and $k = 1$), and a fault of the force device in the $X$-direction cannot be distinguished from a fault of the first joint actuator, even in case of non-concurrency of these two faults.

## V. Conclusions

We have presented different instances of fault set detection and isolation (FSDI) problems in nonlinear systems, providing necessary and sufficient conditions for their solution, based on differential geometric and combinatorial techniques.

The proposed FSDI formulations relax in different ways the standard FDI problem considered in [2] and the obtained generalized conditions are relevant when the original necessary ones fail to be satisfied. The results in this paper can be used for detecting and isolating the occurrence of faults belonging to given sets or for determining the smallest set of candidate faults covering the actual faults that are active in the system. A general characterization of all fault sets for which these problems can be solved has also been given. For the non-concurrent case, a weaker necessary condition for isolating single faults is obtained as a by-product of the FSDI analysis. The design of the diagnostic system is based on the logical processing of continuous-time residuals and results in a hybrid structure.

In [7], the efficiency and achieved performance of the proposed techniques have been tested with experiments on a robot arm, in the presence of measurement and input noise.

## Appendix

In order to compute $\Sigma_*^P$, the smallest involutive distribution containing $P$ and conditioned invariant for system (1) in the absence of faults and disturbances, consider the following nondecreasing sequence of distributions:

$$S_0 = \bar{P}$$
$$S_{k+1} = \bar{S}_k + \sum_{i=0}^{m} \left[ g_i, \bar{S}_k \cap Ker\{dh\} \right]$$

where $\bar{\Delta}$ denotes the involutive closure of a distribution $\Delta$. If there exists an integer $k^*$ such that $S_{k^*+1} = S_{k^*}$ , then $\Sigma_*^P = S_{k^*}$.

For a given codistribution $\Theta$, the observability codistribution algorithm generates the following nondecreasing sequence of codistributions:

$$Q_0 = \Theta \cap \text{span}\{dh\}$$
$$Q_{k+1} = \Theta \cap \left( \sum_{i=0}^{m} L_{g_i} Q_k + \text{span}\{dh\} \right).$$

Suppose that all codistributions of the above sequence are nonsingular, so that there is an integer $k^* \leq n-1$ such that $Q_k = Q_{k^*}$, for all $k > k^*$. Then, we define o.c.a.$(\Theta) = Q_{k^*}$.

## References


[1] P. M. Frank, "Diagnosis in dynamic systems using analytical and knowledge-based redundancy—A survey," *Automatica*, vol. 26, pp. 459–474, 1990.

[2] C. De Persis and A. Isidori, "A geometric approach to nonlinear fault detection and isolation," *IEEE Trans. on Automatic Control*, vol. 46, no. 6, pp. 853–865, 2001.

[3] H. Hammouri, M. Kinnaert, and E. H. El Yaagoubi, "Observer-based approach to fault detection and isolation for nonlinear systems," *IEEE Trans. on Automatic Control*, vol. 44, no. 10, pp. 1879–1884, 1999.

[4] X. Zhang, M. M. Polycarpou, and T. Parisini, "A robust detection and isolation scheme for abrupt and incipient faults in nonlinear systems," *IEEE Trans. on Automatic Control*, vol. 47, no. 4, pp. 576–593, 2002.

[5] R. Mattone and A. De Luca, "Fault detection and isolation in mechanical systems," Dipartimento di Informatica e Sistemistica, Università di Roma "La Sapienza", June 2004.

[6] A. De Luca and R. Mattone, "Actuator failure detection and isolation using generalized momenta," *2003 IEEE Int. Conf. on Robotics and Automation*, pp. 634–639, 2003.

[7] R. Mattone and A. De Luca, "Relaxed fault detection and isolation: An application to a nonlinear case study," submitted to *Automatica*, 2005.