A New Supervisory Fault Tolerant output Regulation Scheme for Nonlinear Systems

Hao Yang, Bin Jiang, and Vincent Cocquempot

Abstract—The fault tolerant output regulation problem for a class of nonlinear systems is considered from hybrid system point of view. The faults are generated by the exogenous systems that belong to a certain pre-specified set of models. The novelty is to design the fault tolerant control (FTC) scheme for the overall system process where different faults may occur respectively at different time instants of the process, which is called “the successional faulty case”. The proposed FTC framework only relies on a simple supervisory switching among a family of pre-computed candidate controllers without any additional model/filter or adaptive scheme. A DC motor example illustrates the efficiency of the proposed method.

Index Terms—Fault tolerant control; Supervisory control; Output regulation; Hybrid systems.

I. INTRODUCTION

Fault detection and isolation (FDI) and fault tolerant control (FTC) are aimed at guaranteeing the system goal to be achieved in spite of faults [1]. Most of existing works design FDI and FTC separately, and assume that the fault occurs only for one time throughout the overall system process as illustrated in the classical faulty case of Fig. 1, where the fault occurs at \( t = t_f \) and the FTC law is applied at \( t = t_{ftc} \).

Appropriate FDI/FTC design indeed maintains the stability of the system in \([t_f, \infty)\) in spite of faults. However, in many practical situations, different faults may occur successively in one system process at different time instants, which we call the successional faulty case (former definition will be given later) as in Fig. 1. Such system behavior can be modeled by a hybrid system [2] where each mode represents a faulty situation. It should be pointed out that even if the FDI/FTC scheme stabilizes the faulty system in each time interval, e.g. \([t_{f1}, t_{f2}) \), \([t_{f2}, t_{f3})\) in Fig. 1, the overall system process may still be unstable as indicated in [14]. The FTC for overall system process deserves further investigations.

On the other hand, only a few literatures model faults by the exogenous signals [1], [3]. Faults modeled by signals generated by exosystems are very general and enables to describe many types of faults [1].

Fig. 1. FTC process

This work is partially supported by National Natural Science Foundation of China (60874051,60811120024), Natural Science Foundation of Jiangsu Province (BK2007195) and Graduate innovation research funding of Jiangsu Province (CX07B-112z).

H. Yang is with College of Automation Engineering (CAE), Nanjing University of Aeronautics and Astronautics (NUAA), 29 YuDao Street, Nanjing, 210016, China and LAGIS-CNRS, UMR 8146, Université des Sciences et Technologies de Lille (USTL), 59655 Villeneuve d’Ascq cedex, France. Email: younghao82@yahoo.com.cn.

B. Jiang is with CAE, NUAA, China. Email: binjiang@nuaa.edu.cn.

V. Cocquempot is with LAGIS-CNRS, UMR 8146, USTL, France. Email: vincent.cocquempot@univ-lille1.fr

The classical faulty case

\[ t_f \]

The successional faulty case

\[ t_{f1} \quad t_{f2} \quad t_{f3} \quad t_{f4} \quad \ldots \]

In this paper, we address the FDI and FTC issues for a class of nonlinear systems with faults modeled by the exogenous signals. We do not explicitly design the FTC laws in each faulty situation since this can be found in many literatures, e.g., [4]-[7], etc. We assume that the plant model belongs to a pre-specified set of models, including the nominal situation and all possible faulty situations, and that there exists a finite family of candidate controllers such that the output regulation problem of each plant model is solvable when controlled by at least one of those candidate controllers. The main contribution of this paper is to propose a supervisory FDI/FTC scheme to achieve the output regulation in the overall system process, i.e., the output of the system asymptotically tracks prescribed trajectories in the successional faulty case.

We first provide a time varying threshold to detect the fault, then propose a novel supervisory controller switching scheme. After a finite number of switchings, the fault can be isolated, and the correct controller relevant to the current situation can be selected and applied.

The novelty of this approach is twofold:

1) Unlike the multiple model FDI/FTC method [8], [9] or supervisory control technique [4], we do not need a series of models or filters to work concurrently with the plant in order to identify the current situation. We also do not design any adaptive scheme to estimate the exosystem of faults as in [5] and [10]. The proposed method only relies on a simple switching scheme among candidate controllers and a family of fictitious fault signals.

2) Under the proposed supervisory FTC scheme, the states are ensured to be bounded and the output regulation performance is maintained throughout the overall system process in the successional faulty case.

The rest of the paper is organized as follows: Section II gives some preliminaries and the problem formulation. In section III, the proposed supervisory FDI/FTC method is
presented. A DC motor example illustrates the approach in Section IV, followed by conclusions in Section V.

II. PRELIMINARIES

Let \( \mathbb{R} \) denote the field of real numbers, \( \mathbb{R}^r \) the \( r \)-dimensional real vector space. \( \cdot \) \( \cdot \) denotes the Euclidean norm. \( C^k \) denotes the set of all functions with continuous \( k \)th derivatives. \( t^- \) denotes the left limit time instant of \( t \).

A. FTC in the classical faulty case

The considered system takes the general nonlinear form
\[
\dot{x}(t) = G(x(t), u(t), f(t))
\]
\[
y(t) = H(x(t), f(t))
\]
\[
\dot{f}(t) = S(f(t)) \quad \forall t \geq t_f, \quad \text{with } f(t) = 0 \quad \forall t \in [0, t_f)
\]
\[
e(t) = y(t) - y_r(x(t))
\]
with measurable state \( x \in \mathbb{R}^n \), input \( u \in \mathbb{R}^p \), output \( y \in \mathbb{R}^m \). The regulated error \( e \) denotes the output tracking error between \( y \) and the continuous reference signal \( y_r(x) : \mathbb{R}^n \rightarrow \mathbb{R}^m \). The vector fields \( G, H \) are smooth and known.

Once the fault occurs at \( t = t_f \), the fault signal \( f \in \mathcal{F} \subset \mathbb{R}^r \) is generated by the \textit{neurally stable} exosystem (3), i.e., \( \partial S(0)/\partial f \) has all its eigenvalues on the imaginary axis [6], which means that \( f \) is always bounded. The initial fault \( f(t_f) \) is supposed to be a known value \( f_{in} \). The function \( S \) is also assumed to be smooth and known. Such model effectively describes process, actuator and sensor faults [1].

**Assumption 1**: There exist some \( u = \alpha(x,f) \) with \( f = 0 \) such that \( x = 0 \) of the healthy system (1) \( \dot{x} = G(x, \alpha(x,0), 0) \) is asymptotically stable.

**Remark 1**: Assumption 1 is a basic requirement for the state feedback output regulation design [6]. For the affine form \( G(x, \alpha(x,0), 0) = G_1(x) + G_2(x)\alpha(x,0) \), Assumption 1 also means that the pair \( (G_1(x), G_2(x)) \) has a stabilizable linear approximation at \( x = 0 \).

**Definition 1**: Fault tolerant regulation problem (FTRP) for system (1)-(4) is to find a FTC law \( u = \alpha(x,f) \) such that \( \forall x(0) \in \mathcal{X} \) with \( \mathcal{X} \subset \mathbb{R}^n \) a neighborhood of \( 0 \) and \( \forall f \in \mathcal{F} \), the trajectory of the closed-loop system (1) is bounded \( \forall t \geq 0 \) and \( \lim_{t \to \infty} e(t) = 0 \).

**Theorem 1**: Suppose that the fault \( f \) can be approximated without any error, and there exists a \( u = \alpha(x,f) \) satisfying Assumption 1. The FTRP for system (1)-(4) is solvable if and only if there exists a \( C^k \) mapping \( \pi = \pi(f) \) with \( \pi(0) = 0 \) defined for \( (x,f) \in \mathcal{X} \times \mathcal{F} \) satisfying
\[
\frac{\partial \pi}{\partial f} S(f) = G(\pi(f), \alpha(\pi(f), f), f)
\]
\[
0 = H(\pi(f), f) - y_r(\pi(f))
\]
**Proof**: The proof follows the same way as that of Theorem 8.3.2 in [6], which is thus omitted.

**Remark 2**: The FTRP is similar to the general output regulation problem with disturbances. The existence and the design of \( \pi(f) \) and \( \alpha(x,f) \) have been deeply investigated in many literatures, e.g., [6], [7] and [10], which are not focused on in this work. For the case that states \( x(t) \) is not measured, observer-based FDI and FTC techniques have been also intensively discussed in our previous works, e.g., [5], [13], which is not considered here.

B. Problem formulation

Now we consider the successional faulty case. Let \( \mathcal{F} = \bigcup_{i \in \mathcal{M} = \{1, \ldots, M\}} \mathcal{F}_i \subset \mathbb{R}^r \) and \( \mathcal{F}_i \) is the set of fault vectors that are associated with fault mode number \( i \). Fault free operation is fault mode \( \mathcal{F}_M = \{0\} \), each fault \( f_i \in \mathcal{F}_i \) is generated by the known exosystem \( f_i = S_i(f_i) \).

**Definition 2**: The system (1)-(4) is in the successional faulty case if there exist a set of faults \( f_i \in \mathcal{F} \) that occur respectively at different time instants in the time interval \([0, \infty)\). Moreover, for any two instants \( t_p \) and \( t_q \) that faults occur, \( t_p \neq t_q \).

It can be seen from Definition 2 that the successional faulty case has several properties.

1) Two faults do not occur simultaneously.

2) The same fault may occur several times throughout the overall process.

3) The sequence of the fault occurrence is random.

The system (1)-(3) in the successional faulty case can be written as a hybrid system
\[
\dot{x}(t) = G_2(x(t), u(t), f_{\rho(t)}(t))
\]
\[
y(t) = H(x(t), f_{\rho(t)}(t))
\]
\[
\dot{f}_{\rho(t)}(t) = S_{\rho(t)}(f_{\rho(t)}(t)) \quad \forall t \geq t_f,
\]
\[
\text{with } f_{\rho(t)}(t) = 0 \quad \forall t \in [0, t_f)
\]
where \( \rho(t) : [0, \infty) \rightarrow \mathcal{M} \) denotes the piecewise constant switching function representing the healthy situation and different fault modes, \( f_{\rho(t)}(t) \in \mathcal{F}_{\rho(t)} \). The initial fault values \( f_{\rho(t)}(t_f) \) are assumed to be \( f_{(in)\rho(t)} \). The hybrid model (7)-(9) clearly captures the behavior of the overall system process in the successional faulty case.

In the considered active fault tolerance, there is a set of control laws \( u_i \) each law being associated with a fault mode \( i \in \mathcal{M} \). The following assumptions define the frame in which the proposed switching scheme is developed, namely all fault modes are recoverable.

**Assumption 2**: There exists a family of controllers \( u_i = \alpha_i(x, f_i) \) for \( f_i \in \mathcal{F}_i, i \in \mathcal{M} \) solving the FTRP for system (4) and (7)-(9) with \( \rho(t) = i \).

**Definition 3**: Overall Fault tolerant regulation problem (OFTRP) for system (4) and (7)-(9) is to find a switching scheme among \( u_i = \alpha_i(x, f_i), i \in \mathcal{M} \) such that \( \forall x(0) \in \mathcal{X} \) and \( \forall f_i \in \mathcal{F}_i \) that occur in the overall system process, the trajectory of the closed-loop system (7) is bounded \( \forall t \geq 0 \) and \( \lim_{t \to \infty} e(t) = 0 \).

Definition 3 is an extension of FTRP to the successional faulty case. The FTC objective in the following discussion is to design a FDI/FTC scheme to solve the OFTRP of system (4) and (7)-(9).

III. SUPERVISIONAL FTC DESIGN

The classical supervisory FTC approach based on a bank of pre-computed control laws \( u_i(t) \) follows three steps [4]:

7814
1) Detect the occurrence of faults; 2) Identify the current fault mode \( i \in \mathcal{M} \); 3) Switch to \( u_i(t) \) as shown by Fig. 2. This scheme obviously introduces a FDI delay to identify the current fault mode. During this delay, the faulty system is controlled using an inappropriate controller, which may result in an unstable behavior. In our proposed scheme, a sequence of controllers are switched, until the appropriate one is found (Fig. 3). A delay in selecting the correct controller (selection delay) still exists, but no isolation algorithm is required (only fault detection is needed), which makes the scheme simpler and more easily verifiable. Moreover, this selection delay can be controlled, and conditions for the OFTRP to be solvable can be exhibited, as it will be shown.

\[ |x(t) - \pi_i(f_i(t))| > B_1 e^{-a_i(t-t_{ik})} |x(t_{ik}) - \pi_i(f_i(t_{ik}))| \quad \implies \text{detection} \]  

Proposition 1: Under Assumption 3, the fault detection law (11) is implementable.

Proof: Note that the state is measurable. Without loss of generality, suppose that there is no fault at the beginning of the system process. The healthy system (7)-(9) with \( \rho(t) = 0 \) is controlled by \( u = \alpha_0(x, 0) \). According to Assumption 2 and (10), we have

\[ |x(t)| \leq B_0 e^{-\alpha_0 t} |x(0)|, \quad t \geq 0 \]  

Once a fault occurs at \( t = t_f \), Assumption 3 ensures that (12) is violated. The following inequality holds

\[ |x(t_{fd})| > B_0 e^{-\alpha_0 t_{fd}} |x(t_{fd})| \]  

where \( t_{fd} \geq t_f \), thus the fault can be detected using the detection law (11) at \( t = t_{fd} \). Note that \( x \) is still bounded at \( t = t_{fd} \).

Next consider \( t \geq t_{ik} \) at which the system (7)-(9) has the fault \( f_i \) and is controlled by \( u = \alpha_i(x, f_i) \) (the accurate value of \( f_i \) can be approximated via the proposed supervisory FTC scheme as in Section III.C). Inequality (10) holds for \( t \geq t_{ik} \). Once a fault occurs at \( t = t_f \geq t_{ik} \), we can also find a \( t_{fd} \geq t_f \) such that (10) is violated for \( t \geq t_{fd} \), which implies that the fault can be detected at \( t = t_{fd} \).

In the following discussion, we assume that there is no fault detection delay, i.e., \( t_{fd} = t_f \). For the case that \( x \) may diverge during the delay, the transient technique in [13] can be applied to ensure the boundedness of \( x \).

B. Ideal supervisory FTC

Let us first consider an ideal case that is each fault can be isolated without any delay. This means that the related FTC law can be applied simultaneously at \( t = t_f \) when the fault occurs and is detected. We denote by \( t_{ik} \), \( k = 0, 1, 2, ... \) the \( k \)th switching instant of fault modes \( \rho(t) \), \( t_0 = 0 \), and by \( \sigma(t) \): \([0, \infty) \rightarrow \mathcal{M} \) the piecewise constant switching function of the controller \( u \). Since the switchings of controllers are in parallel with that of the fault modes, it holds that \( \sigma(t) = \rho(t) \) in the ideal case.

Definition 3 [12]: Let \( N_\rho(T, t) \) denote the number of switchings of \( \rho \) over the interval \((t, T)\), if there exists a positive number \( \tau_\alpha \) such that

\[ N_\rho(T, t) \leq N_0 + \frac{T-t}{\tau_\alpha}, \quad \forall T \geq t \geq 0 \]  

where \( N_0 > 0 \) denotes the chattering bound, then the positive constant \( \tau_\alpha \) is called average dwell time (a.d.t.) of \( \rho \) over \((t, T)\).

Definition 3 means that there may exist some switchings separated by less than \( \tau_\alpha \), but the average dwell period among switchings of fault modes is not less than \( \tau_\alpha \).

The following theorem establishes the sufficient conditions to solve OFTRP in ideal case.

A. Fault detection

It can be seen from Theorem 1 and Assumption 2 that under the FTC law \( u_i \), the system (7)-(9) with \( f_i \) has a center manifold \( x = \pi_i(f_i) \) [6]. Eq.(6) means that the equilibrium \( (x, f_i) = (0, 0) \) of system (7) and (9) is stable and this center manifold is locally attractive, i.e.,

\[ |x(t) - \pi_i(f_i(t))| \leq B_1 e^{-a_i(t-t_{ik})} |x(t_{ik}) - \pi_i(f_i(t_{ik}))| \quad (10) \]

where \( B_1, a_i > 0 \), \( t_{ik} \) denotes the time at which controller \( u_i(t) \) is applied for the \( k \)th time.

Assumption 3: Inequality (10) does not hold if the system (7)-(9) with \( \rho(t) = i \) is controlled by \( u_j \), \( \forall j \in \mathcal{M} \setminus \{i\} \).

Assumption 3 means that all modes are discernable. Consider a time window where the control law \( u_i \) and the fault \( f_i \) are in adequacy, therefore (10) holds, and a simple fault detection law is given by

\[ |x(t) - \pi_i(f_i(t))| > B_1 e^{-a_i(t-t_{ik})} |x(t_{ik}) - \pi_i(f_i(t_{ik}))| \quad \implies \text{detection} \]  

FrB14.3

Fig. 2. The classical FTC framework

Fig. 3. The proposed FTC framework

7815
Theorem 2: Consider a system (4) and (7)-(9) satisfying Assumption 2. Suppose that each fault can be isolated without delay, each FTC law $u_i$ is applied once a fault $f_i$ occurs. The OFTRP is solvable if

1. $\tau_0 > \ln B^a / a$, where $B \triangleq \max_{i \in M} B_i$, $a \triangleq \min_{i \in M} a_i$, and either C2) or C3) holds for $k = 1, 2, \ldots$
2. $\pi(\rho(t_k) - (f_p(t_{k-1})(t_k))) = \pi(\rho(t_k))(f_p(t_k)(t_k))$
3. $(a - \ln B / \tau_0) \leq \lambda k < -a t^* \leq t_k$ for $t \geq t_k$ and $a > 0$.

Remark 3: We provide some insight into the conditions C1)-C3): C1) requires that the switching of the fault modes is slow averagely, i.e., the frequency of fault occurrences is not too high. C2) imposes a condition on the mapping $\pi$, and the fault value $f_i$. If there is a common mapping $x = \pi(f_i)$ for all modes, and $f_p(t_{k-1})(t_k) = 0$, then C2) holds. Generally, C2) is hard to satisfy even in the linear case [11]. In the absence of C2), C3) requires that the dwell period of each fault mode is long enough, which can be verified by checking whether $\ln k + (a - \ln B / \tau_0) k < (a - \ln B / \tau_0 - a^*) t$ holds or not for $t \in [t_k, t_{k+1})$.

Proof of Theorem 2 (sketch): In the ideal case, mode $\rho(t_k)$ in the time interval $[t_k, t_{k+1})$ is controlled by $u_p(t_k)$, thus its FTRP is solved from Assumption 2. According to Theorem 8.3 in [6], a center manifold $x = \pi(\rho(t_k))(f_p(t_k))$ of mode $\rho(t_k)$ is locally attractive, i.e., $\forall t \in [t_k, t_{k+1})$

$$|x(t) - \pi(\rho(t_k))(f_p(t_k)(t_k))| \leq B e^{-a(t-t_k)}|x(t_k) - \pi(\rho(t_k))(f_p(t_k)(t_k))|$$

Similarly, in $[t_k, t_{k+1})$ one has

$$|x(t) - \pi(\rho(t_k))(f_p(t_k)(t_k))| \leq B e^{-a(t-t_k)}|x(t_k) - \pi(\rho(t_k))(f_p(t_k)(t_k))|$$

Combining (15) with (16) yields

$$|x(t) - \pi(\rho(t_k))(f_p(t_k)(t_k))| \leq B e^{-a(t-t_k)}|x(t_k) - \pi(\rho(t_k))(f_p(t_k)(t_k))|$$

By induction, we obtain

$$|x(t) - \pi(\rho(t_k))(f_p(t_k)(t_k))| \leq B e^{-a(t-t_k)}|x(0) - \pi(\rho(0))(0)|$$

$$+ \sum_{s=1}^{k} \left( B e^{-a(t-t_k-1)}|x(t_k) - \pi(\rho(t_k))(f_p(t_k)(t_k))| 
+ B e^{-a(t-t_k)}|\pi(\rho(t_k))(f_p(t_k)(t_k)) - \pi(\rho(t_k))(f_p(t_k)(t_k))| \right)$$

From C1), we can pick $\lambda = a - \ln B / \tau_0$, we have $\tau_0 = \ln B / (a - \lambda)$. Based on (14), we have

$$B^{k+1} e^{-at} \leq B^{N_0 + 1} e^{-\lambda t} \leq B^{N_0 + 1} e^{-\lambda t}$$

If C2) holds, each term of the sum in (17) is zero. Substituting (18) into (17), we further have

$$|x(t) - \pi(\rho(t_k))(f_p(t_k)(t_k))| \leq B^{N_0 + 1} e^{-\lambda t}$$

Inequality (19) means that $x - \pi(\rho(t_k))(f_p(t_k))$ still converges to zero $\forall t \geq t_k$, $\forall x(0) \in X$ and $f_p(t_k) \in F$ that occur in $[0, t)$. By continuity of $H$ and $y_r$ in each $[t_k, t_{k+1})$, it follows that $\lim_{t \to t_k} \pi(t_k) = 0$.

If C2) does not hold, one has from C1) and (14) that

$$B^{N_0 + 1} e^{-\lambda t} \leq B^{N_0 + 1} e^{-\lambda t}$$

Since each $f_i$ is bounded due to the neural stable exosystem, there exist a constant $\xi > 0$ such that $\forall k = 1, 2, \ldots$, and $1 \leq s \leq k$

$$\frac{|\pi(\rho(t_k))(f_p(t_k)(t_k))|}{|\pi(\rho(t_k))(f_p(t_k)(t_k))|} \leq \xi$$

It follows from (21) and C3) that

$$\sum_{s=1}^{k} \left( B^{N_0 + 1} e^{-\lambda t} |x(t_k) - \pi(\rho(t_k))(f_p(t_k)(t_k))| 
+ B^{N_0 + 1} e^{-\lambda t} |\pi(\rho(t_k))(f_p(t_k)(t_k)) - \pi(\rho(t_k))(f_p(t_k)(t_k))| \right)$$

Substituting (18) and (22) into (17). We can also conclude that $x - \pi(\rho(t_k))(f_p(t_k))$ converges to zero $\forall t \geq t_k$, $\forall x(0) \in X$ and $\forall f_p(t_k) \in F$ that occur in $[0, t)$. The result follows.

C. Supervisory FTC with integrated fault isolation

Now we consider a more practical case that the fault can not be isolated rapidly. In most existing fault isolation works e.g. [1], [8] and [9], a series of filters are designed such that each filter is sensitive to one certain kind of faults and not affected by other faults. Another idea is to estimate the current fault mode adaptively as in [5] and [10]. These methods may impose some particular conditions on the structure of the plant and the faults.

We propose a novel fault isolation method based on control switching. When a series of controllers have been designed a priori for the plant with different faults, the fault isolation problem boils down to the problem of finding the correct controller. Such fault isolation approach also integrates the FTC, since the correct controller can be directly applied.

Denote by $t_0^i, t_1^i, t_2^i, \ldots$ the switching instants of $\sigma(t)$, the switching function of controllers. To exhaustively span all controllers, we will pick a non-repeated switching sequence of controllers as in the following definition based on which the switching law is designed.

Definition 4: A switching sequence of controllers is said to be non-repeated if $\sigma(t_0^i) \neq \sigma(t_0^j)$ for $i \geq 0$, $j \geq 0$, and $i \neq j$.

We first consider the classical faulty case, then extend the results to the successional one.

Theorem 3: Consider a system (4), (7)-(9) and a family of controllers $u_i$ satisfying assumptions 2, 3. In the classical faulty case, suppose that a fault $f \in F_i, i \in M$ occurs and
is detected simultaneously at \( t = t_f \) via the threshold (11),
then there exists a control switching scheme such that the FTRP of system (4) and (7)-(9) is solvable \( \forall t \geq t_f \).

**Proof:** Choose a constant \( \beta > 1 \). The switching law is designed as:

Algorithm 1 (Switching law of the controllers)

1. Denote \( t_0^n = t_f \); Let \( s = 0 \); Define \( M^* = M - \{ \sigma(t^n) \} \); Set \( \sigma(t^n_0) = i^* \) where

\[
i^* = \arg \min_{i \in M^*} \left( y(t^n_0) - y_r(\pi_i(\hat{f}_i(t^n_0))) \right)
\]  

(23)

with \( \hat{f}_i \) the fictitious fault generated from the system \( \hat{f}_i = \hat{S}_i(\hat{f}_i) \) with the function \( S_i(\cdot) = S(\cdot) \), the initial \( \hat{f}_i(t^n_0) = f_{(in)i} \).

2. Choose \( t_1^n \) such that

\[
|x(t^n_{1+s}) - \nu_i, f_i(t^n_{1+s})| \leq \frac{M^* - 1}{\sqrt{2}} |x(t^n_0) - \nu_i, f_i(t^n_0)|
\]  

(24)

If \( |x(t^n_{1+s}) - \nu_i, f_i(t^n_{1+s})| \leq B_i \varepsilon - a_i(t^n - t^n_0)
|x(t^n_0) - \nu_i, f_i(t^n_0)| \)

then apply the controller \( u_{\sigma(t^n)}(t) \) \( \forall t \geq t^n_{1+s} \); Stop the switching.

else, go to 3.

3. Let \( M^* = M^* - \{ \sigma(t^n) \} \); Set \( \sigma(t^n_{1+s}) = i^* \) where

\[
i^* = \arg \min_{i \in M^*} \left( y(t^n_{1+s}) - y_r(\pi_i(\hat{f}_i(t^n_{1+s}))) \right)
\]  

(25)

Apply the controller \( u_{\sigma(t^n)}(t) \) at \( t = t^n_{1+s} \); Let \( s = s + 1 \); Go to 2.

We shall prove that Algorithm 1 solves the FTRP. The switching sequence obtained from (23) and (25) is non-repeated, since at each switching instant, the next controller is selected from the set \( M^* \) where the incorrect controller activated before has been removed (Step 3). Thus at most \( M - 1 \) switchings occur before the controller \( u_i(t) \) is applied. We consider the worst situation that \( \sigma(t^n_{M-1}) = i \). The results in other situations are obtained straitly.

Because the function \( \hat{S}_i(\cdot) = S(\cdot) \), the initial \( \hat{f}_i(t^n_0) = f_{(in)i} \), and the fault detection delay is not considered, there must be one fictitious fault signals \( \hat{f}_i \) which is the same as the real fault signal \( f_i \). Note that \( \beta > 1 \) and control mode \( \sigma(t^n_0) \) is faulty, according to Assumption 3, we can choose \( t^n_0 > t^n_0 \) such that \( \beta \rightarrow 2 \) with \( s = 0 \).

Since \( \sigma(t^n_{M-2}) = i \), it holds that \( \hat{f}_i \sigma(t^n_{M-2}) = f_{(M-2)i} \). By induction, we can obtain for \( t \geq t^n_{M-1} \)

\[
|x(t^n_{M-1}) - \pi_i(\sigma(t^n_{M-2}))f_i(t^n_{M-2})| \\
\leq \beta B e^{-a(t^n_{M-2}) |x(t^n_0) - \nu_i, f_i(t^n_0)|} \\
\sum_{j=1}^{M-1} \left( \beta |\pi_{i,j}| - \pi_j(\sigma(t^n_{M-2}))f_i(t^n_{M-2}) \right)(t^n_{M-2}) \\
+ \pi_i(\sigma(t^n_{M-2}))f_i(t^n_{M-2}) \\
\right)
\]  

(26)

Inequality (26) means that \( x - \pi_i(\sigma(t^n_{M-2}))f_i(t^n_{M-2}) \) converges to zero \( \forall t \geq t_f \). It follows that \( \lim_{t \rightarrow 0} e(t) = 0 \).

The following theorem applies the results of Theorems 2, 3 to solve the OFTRP in the successional faulty case.

**Theorem 4:** Consider a system (4) and (7)-(9) satisfying assumptions 2, 3. Each time when a fault occurs, Algorithm 1 is applied. The OFTRP is solvable if \( C1 \) and either \( C2 \) or \( C3 \) in Theorem 2 hold, and \( t_k - t_{k-1} \geq t^n_{M-1} - t^n_0 \), for \( k = 1, 2, ... \).

**Proof:** The proof follows the results of theorems 2 and 3.

For each fault, Algorithm 1 takes the time of \( t^n_{M-1} - t^n_0 \) to solve the FTRP. If \( t_k - t_{k-1} \geq t^n_{M-1} - t^n_0 \), then the FTRP for the current fault mode \( \rho(t_{k-1}) \) can be solved in \( [t_{k-1}, t_k] \) before the next fault occurs as illustrated in Fig. 4.

![Fig. 4. the switching time scales of controllers and fault modes](image)

There always exist \( B^* > 0 \) and \( a^* > 0 \) such that (26) can be rewritten as

\[
|x(t^n_{M-1}) - \pi_i(\sigma(t^n_{M-1}))f_i(t^n_{M-1})| \\
\leq B e^{-a^*(t^n_{M-1}) |x(t^n_{M-1}) - \pi_i(\sigma(t^n_{M-1}))f_i(t^n_{M-1})|} \\
\forall t \in [t^n_{M-1}, t_k].
\]  

The rest of the proof goes along the same line as that of Theorem 2.

**IV. A DC MOTOR EXAMPLE**

A DC motor investigated in [13] is employed to illustrate a potential application field of our approach. \( x = [\theta_m, \omega_m]^T \) is the state, where \( \theta_m, \omega_m \) denote the angular position and velocity of the motor. The system model is:

\[
\dot{\theta}_m = \omega_m \\
\dot{\omega}_m = -\kappa_e \sin(\theta_m) - \frac{b}{J_m} \omega_m + \frac{c}{J_m} u \\
y = \theta_m + f_1 \\
e = y - y_r = y - 2\theta_m = -\theta_m + f_1
\]  

(27)

where \( J_m \) denotes the inertia of the motor. \( \kappa_e > 0 \) is the elasticity constant. \( u \) is the voltage. \( b \) and \( c \) are the viscous friction and the amplifier gain. \( f_1 \) is the sensor fault.

In the fault-free case, design the controller \( u = K(x) = \frac{J_m}{J_m} \sin(\theta_m) + \frac{1}{J_m} \omega_m + K_1 \theta_m + K_2 \omega_m \) such that the matrix \( \begin{bmatrix} K_1 & K_2 \end{bmatrix} \) is Hurwitz. This leads to the asymptotical stability of the origin \( x = 0 \).

Denote \( (i)_{(i)} \) as the parameter of mode \( i \). Three sensor faults are considered:

\[
f(1): \quad y = \theta_m + f_1 \\
f(2): \quad y = \theta_m + 2f_1 \\
f(3): \quad y = \theta_m + 4f_1
\]  

(28) (29) (30)

where \( f_1 \) is generated by the following exosystem

\[
\begin{cases}
  \hat{f}_1 = f_2 \\
  \hat{f}_2 = -f_1
\end{cases}
\]  

(31)
Choosing a mapping $x = \pi^{(1)}(f) = \begin{bmatrix} \pi^{(1)}_1(f) \\ \pi^{(1)}_2(f) \end{bmatrix}$ leads to
\[
\frac{\partial \pi^{(1)}_1(f)}{\partial t} = \pi^{(1)}_2(f) \\
\frac{\partial \pi^{(1)}_2(f)}{\partial t} = -\kappa_e \sin(\pi^{(1)}_1(f)) - \frac{b}{J_m} \pi^{(1)}_2(f) + \frac{c}{J_m} C(f) \\
0 = y(\pi^{(1)}_1(f)) - y_r(\pi^{(1)}_1(f))
\] (32)
where $C(f) = \frac{J_m}{c} \left( \frac{\kappa_e}{J_m} \sin(\pi^{(1)}_1(f)) + \frac{b}{J_m} \pi^{(1)}_2(f) - \pi^{(1)}_1(f) \right)$. We can design the fault tolerant regulation law for fault mode 1 as
\[
u^{(1)}_1 = \alpha^{(1)}_1(x, f) = C^{(1)}(f) + K(x) - K(\pi^{(1)}_1(f)) \quad (33)
\] It is clear that controller (33) satisfies conditions (5)-(6) in Theorem 1, thus the FTRP is solvable.

Similarly, we choose two mappings $\pi^{(2)}(f) = \begin{bmatrix} 2f_1 \\ 2f_2 \end{bmatrix}$, $\pi^{(3)}(f) = \begin{bmatrix} 4f_1 \\ 4f_2 \end{bmatrix}$, and design $C^{(2)}(f) = \frac{J_m}{c} \left( \frac{\kappa_e}{J_m} \sin(\pi^{(2)}_1(f)) + \frac{b}{J_m} \pi^{(2)}_2(f) - \pi^{(2)}_1(f) \right)$, $C^{(3)}(f) = \frac{J_m}{c} \left( \frac{\kappa_e}{J_m} \sin(\pi^{(3)}_1(f)) + \frac{b}{J_m} \pi^{(3)}_2(f) - \pi^{(3)}_1(f) \right)$. The FTC law can be provided as
\[
u^{(2)} = \alpha^{(2)}_2(x, f) = C^{(2)}(f) + K(x) - K(\pi^{(2)}_1(f)) \quad (34) \\
u^{(3)} = \alpha^{(3)}_3(x, f) = C^{(3)}(f) + K(x) - K(\pi^{(3)}_1(f)) \quad (35)
\] Controllers (34) and (35) solve the FTRP for fault modes 2 and 3, respectively.

In the simulation, the parameters are $J_m = 0.935 \text{ kgm}^2$, $\kappa_e = 0.311 \text{ Nm/rad}$, $b = 1.17 \text{ Nms/rad}$, $c = 20.196 \text{ Nm/V}$. Suppose that $f^{(1)}_1$ occurs at $t = 3s$, and $f^{(2)}_2$ occurs at $t = 8s$. Fig. 5 shows that the fault $f^{(1)}_1$ is detected at nearly $t = 3s$ using threshold (11). Once $f^{(1)}_1$ is detected, Algorithm 1 is applied. We choose $\beta = 1.5$. The non-repeated switching sequence obtained from (23) and (25) is $u^{(1)}_2 \rightarrow u^{(1)}_1$. The dwell period of $u^{(1)}_1$ is 0.245s; Once the fault is detected at $t = 3s$, $u^{(2)}_2$ is applied, then switch to $u^{(1)}_1$ at $t = 3.245s$. $f^{(2)}_2$ is still assumed to occur at $t = 8s$. Fig. 6 shows that the OFTRP is solved with the fault isolation delay.

V. CONCLUSION

This paper researches the successional fault case of non-linear systems from the hybrid system point of view. A novel FDI/FRTC scheme based on supervisory switching control has been proposed.

REFERENCES