Robust MPC for Actuator-fault Tolerance using Set-based Passive Fault Detection and Active Fault Isolation

Feng Xu, Vicenç Puig, Carlos Ocampo-Martinez, *Senior Member IEEE,* Sorin Olaru, *Senior Member IEEE* and Silviu-Iulian Niculescu

***Abstract*— In this paper, an actuator fault-tolerant control (FTC) scheme is proposed, which is based on tube-based model predictive control (MPC) and set-theoretic fault detection and isolation (FDI). As a robust MPC technique, tube-based MPC, can effectively deal with system constraints and uncertainties with relatively low computational complexity. Set-based FDI can robustly detect and isolate actuator faults. Here, fault detection (FD) is passive by invariant sets, while fault isolation (FI) is active by tubes. Using the constraint-handling ability of MPC controllers, an active FI approach is implemented. A numerical example illustrates the effectiveness of the proposed approach.**

I. Introduction

The objective of FTC is to maintain satisfactory performance for the controlled system even in the presence of faults. Generally, FTC is divided into passive FTC (PFTC) and active FTC (AFTC) [3]. In this paper, AFTC is considered, which is based on MPC. Due to the ability to deal with system constraints, MPC is chosen as the control strategy for this proposed approach. Besides, MPC is implemented by optimizing the cost function on-line, which endows MPC with a degree of inherent fault-tolerant ability. Thus, if MPC can be integrated into the proposed FTC approach, it may have some interesting features [5].

Fault-tolerant model predictive control (FTMPC) has been investigated in the literature. In [12], an FTMPC scheme using the Kalman filter is proposed, which focuses on the implementation of an FTMPC scheme without considering the features such as stability and feasibility. In [1], an FTMPC scheme with invariant set-based FDI is presented, which has relatively less computational complexity. However, the passive implementation of FDI limits the design of reference states and inputs in order to guarantee set separation, which implies the loss of potential system performance to some extent. Besides, in [9], another FTMPC scheme using set-membership FDI is done, whose main advantage consists in using an active FI method to loosen FI conditions. However, due to the requirements for guaranteeing set separation on-line, this approach is at high complexity.

F. Xu, V. Puig and C. Ocampo-Martinez are with the Institut de Robòtica i Informàtica Industrial (CSIC-UPC), Technical University of Catalonia (UPC), Llorens i Artigas, 4-6, 08028 Barcelona, Spain, {fxu, vpuig, cocampo}@iri.upc.edu.

S. Olaru is with the E3S (SUPELEC Systems Sciences), Automatic Control Department, Gif sur Yvette, France, sorin.olaru@supelec.fr.

S. Niculescu is with L2S, UMR CNRS-Supelec, Gif sur Yvette, France, silviu.niculescu@lss.supelec.fr.

This work has been partially supported by the EU project i-Sense (FP7-ICT-2009-6-270428), China Scholarship Council, CNRS-Supélec and Automatic Control Department, Supélec, France.

Comparing with the existing FTMPC schemes, the objective of this paper consists in proposing a new scheme to not only obtain less conservative FI conditions but also implement FTC with relatively low complexity. In this proposed scheme, FD is passively implemented by invariant sets and FI is actively done by tubes that can isolate faults at transient state. Besides, FI conditions can be prechecked off-line by invariant sets but established on-line by MPC controllers.

The advantages of this FTC scheme are threefold. First, it proposes a novel method to integrate MPC with set-based FDI. Second, it proposes a simple active FI strategy to obtain guaranteed FI. Third, it can reduce the complexity of the existing set-based active FI and decrease the conservatism of FI conditions of the set-based passive FI [9], [1].

The remaining of the paper is organized as follows. In Section II, the FTMPC scheme is introduced. In Section III, the FDI approach based on invariant sets and tubes is presented. Section IV proposes the FTC strategy. In Section V, an example is used to show the effectiveness of the proposed scheme. Finally, Section VI draws the main conclusions.

II. Fault-tolerant Control Scheme

The linear discrete time-invariant plant is modelled as

$$x_{k+1} = Ax_k + BFu_k + \omega_k, \tag{1a}$$

$$y_k = Cx_k + \eta_k, \tag{1b}$$

where $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times p}$ and $C \in \mathbb{R}^{q\times n}$ are constant matrices, $x_k \in \mathbb{R}^n$, $u_k \in \mathbb{R}^p$ and $y_k \in \mathbb{R}^q$ are states, inputs and outputs at time instant k, respectively, ω_k and η_k are unknown disturbances and noises, respectively and F is used to model considered actuator modes (healthy and faulty).

Assumption 2.1: ω_k and η_k are bounded by known sets

$$W = \{\omega \in \mathbb{R}^n : |\omega - \omega^c| \leq \bar{\omega}, \omega^c \in \mathbb{R}^n, \bar{\omega} \in \mathbb{R}^n\}, \tag{2a}$$

$$V = \{\eta \in \mathbb{R}^q : |\eta - \eta^c| \leq \bar{\eta}, \eta^c \in \mathbb{R}^q, \bar{\eta} \in \mathbb{R}^q\}, \tag{2b}$$

respectively, where ω^c, η^c, $\bar{\omega}$ and $\bar{\eta}$ are constant vectors. ■

Assumption 2.2: The pairs (A, BF_i) for all considered modes and (A, C) are stabilizable and detectable. ■

Assumption 2.3: Only single and abrupt actuator fault is considered in this paper and the considered faults can persist sufficiently long such that the system has enough responsive time to detect and isolate them. ■

Remark 2.1: Despite only single fault is considered, in principle, the proposed approach can also cope with the multiple faults. ◊

Under Assumption 2.3, F can take $p+1$ different values, i.e., $F = F_i$ ($i \in \mathbb{I} = \{0, 1, 2, \ldots, p\}$). F_0 is the identity matrix denoting the healthy mode and F_i ($i \neq 0$) modelling the i-th actuator-fault mode is denoted as

$$F_i = \text{diag}[1 \ \ldots \ \overset{\overset{i}{\downarrow}}{0} \ \ldots \ 1]. \tag{3}$$

The input and state constraints are denoted as

$$X = \{x \in \mathbb{R}^n : |x - x^c| \leq \bar{x}, x^c \in \mathbb{R}^n, \bar{x} \in \mathbb{R}^n\}, \tag{4a}$$

$$U = \{u \in \mathbb{R}^p : |u - u^c| \leq \bar{u}, u^c \in \mathbb{R}^p, \bar{u} \in \mathbb{R}^p\}, \tag{4b}$$

where x^c, u^c, $\bar{x}$ and $\bar{u}$ are constant vectors.

Since $p+1$ actuator modes are considered in this paper, the reference system has $p+1$ different reference models, each of which corresponds to one mode. For the i-th mode, the corresponding reference model is given as

$$x_{k+1}^{ref} = Ax_k^{ref} + BF_i u_k^{ref}, \tag{5a}$$

$$y_{k+1}^{ref} = Cx_k^{ref}, \tag{5b}$$

where u_k^{ref}, x_k^{ref} and y_k^{ref} denote the reference inputs, states and outputs, respectively. For brevity, the control objective of the i-th actuator mode[1] is to track an output set-point y_i^*, i.e., in the absence of uncertainties and/or faults

$$\lim_{k\to\infty} (y_k - y_i^*) \to 0. \tag{6}$$

By using (5), a reference state-input pair (x_i^*,u_i^*) in the steady-state operation can be computed by the equation

$$\begin{bmatrix} A - I & B \\ C & O \end{bmatrix} \begin{bmatrix} x_i^* \\ u_i^* \end{bmatrix} = \begin{bmatrix} O \\ y_i^* \end{bmatrix}. \tag{7}$$

Assumption 2.4: The equation (7) corresponding to each mode is solvable to obtain the state-input pairs. ■

Under Assumption 2.4, a state-input pair (x_i^*, u_i^*) corresponding to y_i^* can be obtained by solving (7). Note that, for each mode, the state-input pair may be not unique.

A bank of observers are designed to monitor the behavior of the system, each of which matches one mode. Thus, the observer matching the j-th ($j \in \mathbb{I}$) mode is designed as

$$\hat{x}_{k+1}^j = (A - L_j C)\hat{x}_k^j + BF_j u_k + L_j y_k, \tag{8a}$$

$$\hat{y}_k^j = C\hat{x}_k^j, \tag{8b}$$

where $\hat{x}_k^j$ and $\hat{y}_k^j$ are the estimated states and outputs, respectively, and L_j is the j-th observer gain that can stabilize (8), which is always possible under Assumption 2.2.

A bank of tube-based output feedback MPC controllers are used to tolerate actuator faults, each of which is for one actuator mode. The nominal system corresponding to the i-th mode is obtained from (1) by neglecting the uncertainties ω_k and η_k, which is given as

$$\bar{x}_{k+1}^i = A\bar{x}_k^i + BF_i\bar{u}_k^i, \tag{9a}$$

$$\bar{y}_k^i = C\bar{x}_k^i. \tag{9b}$$

[1]For simplicity, only the set-point tracking problem is considered here. However, the proposed approach can be extended to track a time-varying reference output using the same principle.

According to [7], the control law of the i-th tube-based MPC controller has the following form:

$$u_k = \bar{u}_k^i + K_i(\hat{x}_k^i - \bar{x}_k^i), \tag{10}$$

where K_i is the corresponding feedback gain.

III. Fault Detection and Isolation

A. System Analysis

In the steady-state operation of the i-th mode, F in (1) takes the value F_i, and the i-th tube-based MPC controller, the i-th state-input pair and the i-th observer should be used in the closed-loop system. Moreover, in the i-th mode, the state estimation error of the j-th observer is defined as

$$\tilde{x}_k^{i,j,i} = x_k - \hat{x}_k^j. \tag{11}$$

Remark 3.1: In the superscript of $\tilde{x}_k^{i,j,i}$, the first index denotes that the plant is in the i-th mode, the second index denotes that the j-th observer and the third index denotes that the i-th MPC controller is active in the system. ◊

If $j \neq i$ in (11), using (1), (8) and (10), the dynamics of $\tilde{x}_k^{i,j,i}$ can be derived as

$$\begin{aligned}\tilde{x}_{k+1}^{i,j,i} =& (A - L_j C)\tilde{x}_k^{i,j,i} + B(F_i - F_j)\bar{u}_k^i + \omega_k - L_j\eta_k \\ &+ B(F_i - F_j)K_i(\hat{x}_k^i - \bar{x}_k^i)\end{aligned} \tag{12}$$

and the corresponding output estimation error of the j-th observer can also be derived as

$$\tilde{y}_k^{i,j,i} = y_k - \hat{y}_k^j = C\tilde{x}_k^{i,j,i} + \eta_k. \tag{13}$$

Besides, in the steady-state operation of the i-th mode, the term $\hat{x}_k^i - \bar{x}_k^i$ appearing in (10) and (12) is denoted by

$$e_k^{i,i,i} = \hat{x}_k^i - \bar{x}_k^i, \tag{14}$$

whose dynamics can be derived by using (8) and (9) as

$$e_{k+1}^{i,i,i} = (A + BF_iK_i)e_k^{i,i,i} + L_iC\tilde{x}_k^{i,i,i} + L_i\eta_k, \tag{15}$$

where $\tilde{x}_k^{i,i,i}$ corresponds to the case of $j = i$ in (11) and its dynamics can be obtained from (12), i.e.,

$$\tilde{x}_{k+1}^{i,i,i} = (A - L_iC)\tilde{x}_k^{i,i,i} + [I \ \ -L_i] \begin{bmatrix} \omega_k \\ \eta_k \end{bmatrix}. \tag{16}$$

Due to $\omega_k \in W$ and $\eta_k \in V$, a *robust positively invariant* (RPI) set denoted as $\tilde{X}^{i,i,i}$ of $\tilde{x}_k^{i,i,i}$ can be constructed (see [10], [8], [11] for RPI sets). According to the notion of invariant sets, as long as $\tilde{x}_{k^*}^{i,i,i} \in \tilde{X}^{i,i,i}$, $\tilde{x}_k^{i,i,i} \in \tilde{X}^{i,i,i}$ always holds for all $k > k^*$. Similarly, considering $\tilde{x}_k^{i,i,i} \in \tilde{X}^{i,i,i}$, an RPI set (denoted as $E^{i,i,i}$) of $e_k^{i,i,i}$ can be obtained by using (15).

In the i-th mode, if a fault is detected, for FI point of view, one defines an input set $\bar{U}_f^i$ for FI analysis (i.e., $\bar{u}_k^i \in \bar{U}_f^i$)

$$\bar{U}_f^i = \{\bar{u}^i \in \mathbb{R}^p : \left|\bar{u}^i - \bar{u}_f^{i,c}\right| \leq \bar{u}_f^i, \bar{u}_f^{i,c} \in \mathbb{R}^p, \bar{u}_f^i \in \mathbb{R}^p\},$$

where both $\bar{u}_f^{i,c}$ and $\bar{u}_f^i$ are constant vectors.

Similarly, considering $e_k^{i,i,i} \in E^{i,i,i}$ and $\bar{u}_k^i \in \bar{U}_f^i$ in (12), an RPI set (denoted as $\tilde{X}^{i,j,i}$) of $\tilde{x}_k^{i,j,i}$ can be obtained[2]. The corresponding set of output estimation errors is

$$\tilde{Y}^{i,j,i} = C\tilde{X}^{i,j,i} \oplus V, \tag{17}$$

where, in the case of $j = i$, the output estimation error set $\tilde{Y}^{i,i,i}$ corresponding to $\tilde{X}^{i,i,i}$ can be obtained as well.

Remark 3.2: From FDI point of vew, all the RPI sets $\tilde{X}^{i,i,i}$, $E^{i,i,i}$ and $\tilde{X}^{i,j,i}$ should be as small as possible. $\Diamond$

Since $\tilde{y}_k^{i,j,i}$ is available while $\tilde{x}_k^{i,j,i}$ is unavailable, $\tilde{y}_k^{i,j,i}$ is defined as the residual signal of the proposed FTC approach.

B. Fault Detection

The FD approach used here is a passive approach, which is based on invariant sets. Thus, the FD task can be simplified into only testing whether or not the residual is inside its corresponding invariant set, whose advantage consists in less computational complexity. As analyzed in Section III-A, for each mode $i \in \mathbb{I}$, only the sets $\tilde{X}^{i,i,i}$ and $\tilde{Y}^{i,i,i}$ are independent of $\bar{u}_k^i$, while $\tilde{X}^{i,j,i}$ and $\tilde{Y}^{i,j,i}$ ($j \neq i$) depend on $\bar{u}_k^i$. Thus, in order to assure that FD is not affected by $\bar{u}_k^i$, in the i-th mode, only the set $\tilde{Y}^{i,i,i}$ is used for the FD task, i.e., testing whether or not

$$\tilde{y}_k^{i,i,i} \in \tilde{Y}^{i,i,i} \tag{18}$$

is violated in real time. If a violation of (18) is detected, it means that a fault has occurred in the system. Otherwise, it is considered that the system still operates in the i-th mode.

For some faults, even they occur, perhaps (18) is still respected. This means that these faults can not be detected, then actively tolerated. Instead, they can only be tolerated to some extent by the PFTC ability of this proposed scheme.

C. Fault Isolation

1) After-fault Behaviors : The FI task is started when a fault is detected. Without loss of generality, it is assumed that the l-th ($l \neq i$) fault occurs at time instant k_d, i.e., after k_d, the system mode changes from i to l. Although the mode changes from i to l, before the fault is isolated, the system structure does not change yet, which implies that the closed-loop system is still composed of the same components.

According to (1), (8), (9) and (10), when the l-th fault occurs, the state estimation error of the j-th observer changes from $\tilde{x}_k^{i,j,i}$ to $\tilde{x}_k^{l,j,i}$ with the dynamics

$$\begin{aligned}\tilde{x}_{k+1}^{l,j,i} =&(A - L_jC)\tilde{x}_k^{l,j,i} + B(F_l - F_j)\bar{u}_k^i + \omega_k - L_j\eta_k \\ &+ B(F_l - F_j)K_i e_k^{l,i,i},\end{aligned} \tag{19}$$

and $e_k^{i,i,i}$ in (15) changes to $e_k^{l,i,i}$ in (19) with the dynamics

$$e_{k+1}^{l,i,i} = (A + BF_iK_i)e_k^{l,i,i} + L_iC\tilde{x}_k^{l,i,i} + L_i\eta_k. \tag{20}$$

To collect the whole process information after the l-th fault from the i-th mode, one defines an augmented vector

$$\xi_k^{i\to l} = \begin{bmatrix}\tilde{x}_k^{l,0,i} & \cdots & \tilde{x}_k^{l,i,i} & \cdots & \tilde{x}_k^{l,p,i} & e_k^{l,i,i}\end{bmatrix}^T.$$

[2] $\bar{U}_f^i$ different from the constraint set U is only used for active FI.

As per (19) and (20), the dynamics of $\xi_k^{i\to l}$ is obtained as

$$\xi_{k+1}^{i\to l} = A_{i\to l}\xi_k^{i\to l} + B_{i\to l}\bar{u}_k^i + E_{i\to l}^{\omega}\omega_k + E_{i\to l}^{\eta}\eta_k, \tag{21}$$

where

$$A_{i\to l} = \begin{bmatrix} A-L_0C & O & \cdots & O & B(F_l-F_0)K_i \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ O & A-L_iC & \cdots & O & B(F_l-F_i)K_i \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ O & O & \cdots & A-L_pC & B(F_l-F_p)K_i \\ O & L_iC & \cdots & O & A+BF_iK_i \end{bmatrix},$$

$$B_{i\to l} = \begin{bmatrix} B(F_l-F_0) \\ \vdots \\ B(F_l-F_i) \\ \vdots \\ B(F_l-F_p) \\ O \end{bmatrix},\ E_{i\to l}^{\omega} = \begin{bmatrix} I \\ \vdots \\ I \\ \vdots \\ I \\ O \end{bmatrix},\ E_{i\to l}^{\eta} = \begin{bmatrix} -L_0 \\ \vdots \\ -L_i \\ \vdots \\ -L_p \\ L_i \end{bmatrix}.$$

Assumption 3.1: The designed observer and feedback gains $L_0, L_1, \ldots, L_p$ and $F_0, F_1, \ldots, F_p$ always assure that the matrix $A_{i\to l}$ is a Schur matrix. ■

Similarly, since $\bar{u}_k^i \in \bar{U}_f^i$, $\omega_k \in W$ and $\eta_k \in V$, an RPI set of $\xi_k^{i\to l}$ can be constructed, which is denoted as $\Xi^{i\to l}$. By projecting $\Xi^{i\to l}$ towards the component space, an RPI set of each component of $\xi_k^{i\to l}$ can be obtained. For example, an RPI set (denoted as $\tilde{X}^{l,j,i}$) of $\tilde{x}_k^{l,j,i}$ can be obtained by projecting $\Xi^{i\to l}$ to the space of $\tilde{x}_k^{l,j,i}$. Similarly, an RPI set (denoted as $E^{l,i,i}$) of $e_k^{l,i,i}$ can be computed by projection. This implies, after the l-th fault, $\tilde{x}_k^{l,j,i}$ and $e_k^{l,i,i}$ finally enter into $\tilde{X}^{l,j,i}$ and $E^{l,i,i}$, respectively. Moreover, using (1b), the set of output estimation errors corresponding to $\tilde{X}^{l,j,i}$ is

$$\tilde{Y}^{l,j,i} = C\tilde{X}^{l,j,i} \oplus V. \tag{22}$$

2) Residual Tubes: The dynamics of $\tilde{x}^{l,l,i}$ extracted from (21) are used for FI, which has the form

$$\tilde{x}_{k+1}^{l,l,i} =(A - L_lC)\tilde{x}_k^{l,l,i} + \omega_k - L_l\eta_k. \tag{23}$$

Substituting W and V into (23), the set-based description of $\tilde{x}_k^{l,l,i}$ and $\tilde{y}_k^{l,l,i}$ can be obtained as

$$\tilde{X}_{k+1}^{l,l,i} =(A - L_lC)\tilde{X}_k^{l,l,i} \oplus W \oplus (-L_lV), \tag{24a}$$

$$\tilde{Y}_k^{l,l,i} =C\tilde{X}_k^{l,l,i} \oplus V. \tag{24b}$$

Similarly, a set-based description of (19) is obtained as

$$\begin{aligned}\tilde{X}_{k+1}^{l,j,i} =&(A - L_jC)\tilde{X}_k^{l,j,i} \oplus B(F_l - F_j)\bar{U}_f \oplus W \oplus (-L_jV) \\ &\oplus B(F_l - F_j)K_iE^{l,i,i}.\end{aligned} \tag{25}$$

As k tends to infinity, $\tilde{X}_{k+1}^{l,j,i}$ and $\tilde{X}_{k+1}^{l,l,i}$ will converge to the *minimal robust positively invariant* (mRPI) sets of (19) and (23), i.e., they finally enter into RPI sets $\tilde{X}^{l,j,i}$ and $\tilde{X}^{l,l,i}$ and stay inside, respectively. Besides, the output estimation error set sequence corresponding to $\tilde{X}_k^{l,j,i}$ is obtained as $\tilde{Y}_k^{l,j,i} = C\tilde{X}_k^{l,j,i} \oplus V$.

Proposition 3.1: Given that the l-th ($l \neq i$) fault occurs in the i-th mode and the state estimation error $\tilde{x}_{k*}^{l,l,i}$ of the l-th observer is bounded by a set $\tilde{X}_{k*}^{l,l,i}$ at time instant $k*$, if $\tilde{X}_{k*}^{l,l,i}$ is used to initialize (24) to generate tubes, $\tilde{x}_k^{l,l,i} \in \tilde{X}_k^{l,l,i}$ and $\tilde{y}_k^{l,l,i} \in \tilde{Y}_k^{l,l,i}$ will hold for all $k \geq k*$. □

In the i-th mode, it is assumed that the l-th fault is detected at time instant k_d. If an initial set is used to initialize (24a) at time instant k_d, the tubes of state and output estimation errors generated by (24) are denoted as

$$\tilde{\mathbb{T}}^{x,l,l,i}_{k_d} = \{\tilde{X}^{l,l,i}_{k_d}, \tilde{X}^{l,l,i}_{k_d+1}, \tilde{X}^{l,l,i}_{k_d+2}, \dots\}, \tag{26a}$$

$$\tilde{\mathbb{T}}^{y,l,l,i}_{k_d} = \{\tilde{Y}^{l,l,i}_{k_d}, \tilde{Y}^{l,l,i}_{k_d+1}, \tilde{Y}^{l,l,i}_{k_d+2}, \dots\}. \tag{26b}$$

Remark 3.3: Generally, when the system is in the i-th mode, the detection of a violation of (18) implies that a mode switching from i to another unknown mode denoted as f ($f \in \mathbb{I}\setminus\{i\}$) occurred, i.e., there are p mode candidates (healthy or faulty). Thus, for FI, one has to obtain all the p output estimation error tubes $\tilde{\mathbb{T}}^{y,l,l,i}_{k_d}$ ($l \in \mathbb{I}\setminus\{i\}$). ◊

Thus, at time instant k_d, the proposed FI algorithm generates p output-estimation-error tubes $\tilde{\mathbb{T}}^{y,l,l,i}_{k_d}$ ($l \in \mathbb{I}\setminus\{i\}$), each of which corresponds to a candidate mode. Moreover, for the p corresponding observers, as long as

$$\tilde{x}^{f,l,i}_{k_d} \subseteq \tilde{X}^{l,l,i}_{k_d},\ f,\ l \in \mathbb{I}\setminus\{i\} \tag{27}$$

is guaranteed at time instant k_d such that $\tilde{y}^{f,l,i}_{k_d} \subseteq \tilde{Y}^{l,l,i}_{k_d}$, which implies that, among the p output-estimation-error tubes $\tilde{\mathbb{T}}^{y,l,l,i}_{k_d}$ ($l \in \mathbb{I}\setminus\{i\}$), there exists at least one tube (indexed by m) that can always satisfy

$$\tilde{y}^{f,m,i}_{k} \subseteq \tilde{Y}^{m,m,i}_{k},\ k \geq k_d,\ m \in \mathbb{I}\setminus\{i\}. \tag{28}$$

Remark 3.4: If the fault is indexed by l (i.e., $f = l$) and (27) holds, for all $k \geq k_d$, $\tilde{\mathbb{T}}^{y,l,l,i}_{k_d}$ can always satisfy $\tilde{y}^{f,l,i}_{k} \subseteq \tilde{Y}^{l,l,i}_{k}$. This implies that the fault will be indicated by one of the p tubes that can always satisfy (28). ◊

3) Fault Isolation Algorithm: To isolate a fault, one has to guarantee that one and only one tube can always satisfy (28) after FD and the index of this tube indicates the fault.

Proposition 3.2: In the i-th mode, for any observer (indexed by j), if all the corresponding $p+1$ output-estimation-error sets satisfy

$$\tilde{Y}^{j,j,i} \cap \bigcup_{l=0}^{p} \tilde{Y}^{l,j,i} = \emptyset,\ l \neq j,\ i,\ j,\ l \in \mathbb{I}, \tag{29}$$

once a mode switching from the i-th mode has occurred, the mode can be isolated by searching the output-estimation-error tube that always satisfies (28).

Proof : As previously concluded, the tube $\tilde{\mathbb{T}}^{y,j,j,i}_{k_d}$ will finally enter into $\tilde{Y}^{j,j,i}$. Thus, if (29) holds, the tube $\tilde{\mathbb{T}}^{y,j,j,i}_{k_d}$ will only be able to confine the output estimation error $\tilde{y}^{l,j,i}_{k}$ under the condition $l = j$. If $l \neq j$, at the first several steps, $\tilde{\mathbb{T}}^{y,j,j,i}_{k_d}$ may be able to confine $\tilde{y}^{l,j,i}_{k}$ because of the initialization condition (27). But, as $\tilde{\mathbb{T}}^{y,j,j,i}_{k_d}$ approaches $\tilde{Y}^{j,j,i}$, $\tilde{y}^{l,j,i}_{k}$ must diverge from $\tilde{\mathbb{T}}^{y,j,j,i}_{k_d}$. This implies that, under the condition (29), by searching the tube that is always able to confine $\tilde{y}^{l,j,i}_{k}$, the fault can be isolated. □

4) Construction of Initial Sets: The key of the FI approach is to construct initial sets satisfying (27) at time instant k_d to generate the output-estimation-error tubes. For example, for the j-th observer, one can obtain

$$C\tilde{x}^{i,j,i}_{k_d} \in \{\tilde{y}^{i,j,i}_{k_d}\} \oplus (-V). \tag{30}$$

Using (30), a set to bound $\tilde{x}^{i,j,i}_{k_d}$ can always be constructed, which is used to initialize (24a) to generate the output-estimation-error tubes. Moreover, for the j-th observer, the expression of (30) is independent of modes. This means that (30) can always be used to construct a set to bound the state estimation error of the j-th observer in any mode.

Remark 3.5: If C is not invertible, a set to bound $\tilde{x}^{i,j,i}_{k_d}$ can still be obtained by intersecting all strips (each strip corresponds to an elementwise inequality of (30)) or all strips of (30) with the physical constraint set of $\tilde{x}^{i,j,i}_{k}$ in the case that C has zero columns. ◊

Remark 3.6: Since X, U, W and V can be rewritten as zonotopes, from the computational point of view, all the tubes are generated by using zonotopes in this paper. Thus, the initial sets should be constructed as zonotopes (see [2], [6] for the relevant properties of zonotopes). ◊

IV. Fault-tolerant Control

A. Steady-state Behaviors

The tube-based MPC technique proposed in [7] is adopted to implement FTC in this scheme and the control law of the i-th one is given in (10). It is assumed that the system is at steady state of the i-th mode. The key part of the MPC control law is the open-loop optimization problem behind the tube-based MPC controller, which is based on the i-th nominal system, i.e., $\bar{u}^i_k$ in (10).

In reality, it is known that X and U in (4) are the hard system constraints. Those hard constraints implies the indirect hard constraints on the nominal system-based open-loop optimization problem. In the case of the i-th mode, the indirect input hard constraint is via (10), i.e., $u_k = \bar{u}^i_k + K_i e^{i,i,i}_k$. As per Section III-A, at steady state of the i-th mode, $e^{i,i,i}_k \in E^{i,i,i}$ holds, Thus, the hard input constraints of the nominal system-based open-loop optimization problem can be obtained as $\bar{u}^i_k \in \bar{U}^i = U \ominus K_i E^{i,i,i}$. Considering $x_k = \bar{x}^i_k + e^{i,i,i}_k + \tilde{x}^{i,i,i}_k$, the hard state constraints can be further obtained as

$$\bar{x}^i_k \in \bar{X}^i = X \ominus (E^{i,i,i} \oplus \tilde{X}^{i,i,i}). \tag{31}$$

Assumption 4.1: $\bar{X}^i$ and $\bar{U}^i$ ($i \in \mathbb{I}$) are nonempty. ■

Thus, the open-loop optimization problem of the i-th tube-based MPC controller, based on the i-th nominal system (9), has the following form:

$$\begin{aligned} J_k = \min_{\bar{\mathbf{u}}^i} \sum_{j=0}^{N-1} &\|(\bar{x}^i_{k+j|k} - x^*_i)\|^2_{Q_i} + \|(\bar{u}^i_{k+j|k} - u^*_i)\|^2_{R_i} \\ &+ \|(\bar{x}^i_{k+N|k} - x^*_i)\|^2_{P_i} \\ \text{subject to}\quad & \bar{x}^i_{k+j|k} \in \bar{X}^i,\quad \bar{u}^i_{k+j|k} \in \bar{U}^i, \\ & \bar{x}^i_{k+N|k} \in \bar{X}^i_T,\quad \bar{x}^i_{k|k} = \bar{x}^i_k, \end{aligned} \tag{32}$$

where $\bar{\mathbf{u}}^{\mathbf{i}} = [\bar{u}^i_{k|k}, \bar{u}^i_{k+1|k}, \cdots, \bar{u}^i_{k+N-1|k}]$, N is the prediction horizon, Q_i R_i and P_i are positive-definite matrices and $\bar{X}^i_T$ is the corresponding terminal constraint set.

If $\bar{X}^i_T$ is the *maximal control invariant* (MCI) set of the i-th nominal system, the i-th tube-based MPC controller can be designed to be feasible. In this paper, the implementation of the tube-based MPC controller follows [4] and [7].

B. Transient-state Behaviors

Different from the steady-state operation of the i-th mode, once a fault (denoted by l) has occurred, it implies that the mode changes from i to l ($l \neq i$). To analyze the transient-state behavior induced by the fault, the transient-state process is split into two phases. The former starts from the occurrence till the detection of the fault and the latter starts from the detection to the isolation of the fault. Since the latter is related here to active FI, it will be separately discussed.

In the first phase, despite the l-th fault has occurred, the FD criterion in (18), i.e., $\tilde{x}_k^{l,i,i} \in \tilde{X}^{i,i,i}$, still holds. Thus, as per (20), $e_k^{l,i,i} \in E^{i,i,i}$ also holds. Thus, before FI, the closed-loop system is still composed of the same components with the i-th "fault-free" mode. Therefore, although the l-th fault has occurred, one can "think" the system still operates in the i-th mode since $\tilde{x}_k^{l,i,i} \in \tilde{X}^{i,i,i}$, $e_k^{l,i,i} \in E^{i,i,i}$, $\bar{u}_k^i \in \bar{U}^i$, and $\bar{x}_k^i \in \bar{X}^i$, which implies that the feasibility and hard constraints of the system are still respected in this phase.

C. Active Fault Isolation

1) Fault Isolation Principle: Without considering the effect of the observer and feedback gains and considered faults, as per (21) and (22), when the system mode changes from i to l ($l \neq i$), the sets of output estimation errors are decided by the sets of the uncertainties and nominal inputs, i.e.,

$$\tilde{Y}^{l,j,i} = f^{i \to l}(\bar{U}_f^i, W, V), \;\; j \neq l, \tag{33}$$

which implies whether the FI conditions in Proposition 3.2 hold or not depends on the set of nominal inputs $\bar{u}_k^i$. Note that $Y^{l,l,i}$ is decided by W and V and free from the effect of $\bar{U}_f^i$, which is the reason why only $Y^{i,i,i}$ is used for FD.

Assumption 4.2: There exists a set $\bar{U}_f^i$ satisfying $\bar{U}_f^i \subseteq \bar{U}^i$ such that the FI conditions in Proposition 3.2 hold. ■

Assumption 4.2 means, when a switching from the mode i to l ($l \neq i$) is detected, if $\bar{u}_k^i$ is always confined inside $\bar{U}_f^i$, the FI conditions in Proposition 3.2 can be established online by the i-th MPC controller and the proposed FI approach can isolate the mode. Thus, in the i-th mode, the i-th MPC controller has two different objectives:

- Steady-state operation (including the first-phase transition): No fault is detected and the main task is to implement system performance. Thus, the input constraint of (32) is $\bar{U}^i$.
- Transient-state operation (only considering the second-phase transition): A fault is detected and the main task is to isolate the fault and reconfigure the system. During this stage, the proposed FI approach actively switches the input constraint of (32) from $\bar{U}^i$ to $\bar{U}_f^i$ at the FD time k_d to establish the FI conditions (i.e., active FI).

2) Transient-state Feasibility and Stability: As per (9) and (32), (32) is updated by directly using the nominal state from the i-th nominal system. Since the nominal states are free from the effect of the real system, fault occurrence does not affect the feasibility and stability of (32) provided that all the constraints of (32) are always respected.

However, during the FI process, since the input constraint of (32) is switched from $\bar{U}^i$ to $\bar{U}_f^i$ to establish the FI conditions, to guarantee the feasibility of (32), one has to switch the terminal constraint from $\bar{X}_T^i$ to $\bar{X}_{f_T}^{\;i}$ ($\bar{X}_{f_T}^{\;i}$ is a *control invariant* (CI) set[3] of the i-th nominal system corresponding to $\bar{u}_k^i \in \bar{U}_f^i$, which satisfies the constraints.

Remark 4.1: During FI, this proposed approach uses $\bar{X}_{f_T}^{\;i}$ as both the state and terminal constraints of (32). ◊

Assumption 4.3: During FI, from the modes i to l, $\bar{U}_f^i \oplus K_i e_k^{l,i,i} \in U$ and $\bar{X}_{f_T}^{\;i} \oplus e_k^{l,i,i} \oplus \tilde{x}_k^{l,i,i} \in X$ always hold, i.e., the hard constraints are not violated. ■

Remark 4.2: Since $\bar{U}_f^i \subseteq U^i$, it implies that, comparing with the steady-state operation, the admissible regions of $e_k^{l,i,i}$, $e_k^{l,i,i}$ and $\tilde{x}_k^{l,i,i}$ during active FI relatively increase. By selecting smaller $\bar{U}_f^i$, one can give $e_k^{l,i,i}$ and $\tilde{x}_k^{l,i,i}$ larger admissible regions to satisfy Assumption 4.3. ◊

To guarantee the feasibility of (32), one has to consider the nominal state $\bar{x}_{k_d}^i$ of the i-th nominal system at k_d.

Proposition 4.1: At the FD time k_d, if $\bar{x}_{k_d}^i \in \bar{X}_{f_T}^{\;i}$ holds, (32) will be always feasible during the whole FI process.

Proof : Since $\bar{X}_{f_T}^{\;i}$ is a CI set, $\bar{x}_{k_d}^i \in \bar{X}_{f_T}^{\;i}$ implies $\bar{x}_{k_d+1}^i \in \bar{X}_{f_T}^{\;i}$. Thus, there always exist control sequences that satisfy the input and control constraints during FI. □

Summarizing, the following strategy to guarantee the feasibility of the MPC controller during FI is proposed: If $\bar{x}_{k_d}^i \in \bar{X}_{f_T}^{\;i}$, (32) is always feasible. Otherwise, the center of $\bar{X}_{f_T}^{\;i}$ is used to update (32) to guarantee feasibility. Then, if $\bar{x}_{k_d+1}^i \in \bar{X}_{f_T}^{\;i}$, the feasibility at the next steps can always be guaranteed. Otherwise, still use the center of $\bar{X}_{f_T}^{\;i}$ to update (32). Once a fault is isolated, the similar strategy is used to guarantee the feasibility of the MPC controller corresponding to a new MPC controller during the initial phase after system reconfiguration. After the system enters into steady state, the MPC controller is feasible under Assumption 4.1.

V. Illustrative Numerical Example

In this example, two actuator faults F_1 and F_2 are considered, three observers are designed and three tube-based MPC controllers are used to control the modes. Only results of the second fault are presented due to space limitation. The parameters are given as follows:

- Parameter matrices:
  $A = \begin{bmatrix} 0.6 & 0.05 \\ 0.1 & 0.7 \end{bmatrix}, B = \begin{bmatrix} 0.5 & 0.1 \\ 0.2 & -0.3 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$
- Disturbances: $\bar{w} = \begin{bmatrix} 0.05 & 0.05 \end{bmatrix}^T, w^c = \begin{bmatrix} 0 & 0 \end{bmatrix}^T.$
- Noises: $\bar{\eta} = \begin{bmatrix} 0.05 & 0.05 \end{bmatrix}^T, \eta^c = \begin{bmatrix} 0 & 0 \end{bmatrix}^T.$
- Observer gains: $L_0 = L_1 = L_2 = \begin{bmatrix} 1 & 0.05 \\ 0.1 & 0.2 \end{bmatrix}.$
- Feedback gains:
  $K_0 = \begin{bmatrix} 0.1288 & 0.0644 \\ 0.1559 & 0.0780 \end{bmatrix}, K_1 = \begin{bmatrix} 0 & 0.3220 \\ 0 & 0.3898 \end{bmatrix},$

[3] $\bar{X}_{f_T}^{\;i}$ can be an RPI set of the i-th nominal system with $u_k^i \in \bar{U}_f^i$.

$$K_2 = \begin{bmatrix} 0.1610 & 0 \\ 0.1949 & 0 \end{bmatrix}.$$

- Fault magnitudes: $F_1 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, F_2 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$.
- Output set-point: $y_2^* = \begin{bmatrix} 1.5 & 1 \end{bmatrix}^T$.
- State-input set-point pairs:
  $u_0^* = \begin{bmatrix} 1.0588 & 0.2059 \end{bmatrix}^T, x_0^* = \begin{bmatrix} 1.5 & 1 \end{bmatrix}^T,$
  $u_2^* = \begin{bmatrix} 1.0453 & 0 \end{bmatrix}^T, x_2^* = \begin{bmatrix} 1.4863 & 1.0168 \end{bmatrix}^T.$
- Initial conditions:
  $x_0 = \begin{bmatrix} 0 & 0 \end{bmatrix}^T, \hat{x}_0^0 = \hat{x}_0^1 = \hat{x}_0^2 = \begin{bmatrix} 0 & 0 \end{bmatrix}^T.$
- System constraints:
  $U = \{u : \begin{bmatrix} -10 & -10 \end{bmatrix}^T \leq u \leq \begin{bmatrix} 10 & 10 \end{bmatrix}\}^T,$
  $X = \{x : \begin{bmatrix} -30 & -30 \end{bmatrix}^T \leq x \leq \begin{bmatrix} 30 & 30 \end{bmatrix}\}^T.$
- Input sets for active FI:
  $\bar{U}_f^0 = \{u : \begin{bmatrix} 7.5 & 7.5 \end{bmatrix} \leq u \leq \begin{bmatrix} 8.5 & 8.5 \end{bmatrix}\}^T.$
- Prediction horizon: $N = 10$.
- Parameters of MPC controllers :
  $Q = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, R = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, P = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$
- Sampling time: $T = 0.1$s.

Based on $\bar{U}_f^0$, the corresponding sets of output estimation errors for active FI can be computed. By off-line testing, those sets can satisfy Proposition 3.2 (the details are omitted here). Furthermore, corresponding to the constraints X and U of the system, the state and input constraints $\bar{X}^0$ and $\bar{U}^0$, $\bar{X}^1$ and $\bar{U}^1$, and $\bar{X}^2$ and $\bar{U}^2$ of the nominal MPC controllers can be obtained (the details are omitted here).

The simulation scenario for FDI and FTC of the second actuator fault is defined as: from time instants 0 to 50, the system is healthy, then from time instants 51 to 100, the second actuator fault occurs. When the system is healthy, only the set $\tilde{Y}^{0,0,0}$ is used for FD. The FDI and FTC results of the second actuator fault are shown in Figure 1, 2 and 3. In Figure 1 and 2, it can be observed that the fault is detected and isolated at time instants 61 and 62, respectively. This means that the active FI mechanism is started at time instant 61 and is terminated at time instant 62, and the system is reconfigured at time instant 62 to tolerate the fault. Similarly, according to Figure 3, it can be observed that the state and input constraints are respected all the time. Besides, in Figure 3, even though the system is in the faulty mode, after reconfiguration, the output set-point is still well tracked.

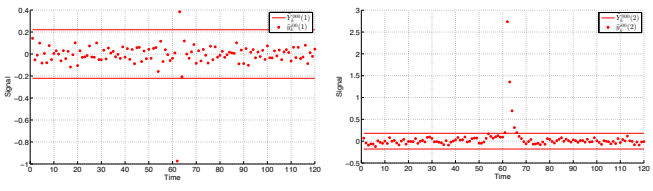

Fig. 1. FD of the second actuator fault

Remark 5.1: To avoid false alarms of faults, after the system is reconfigured, a waiting time is set and the FD mechanism is frozen till the waiting time elapses. Then, the FD mechanism is restarted again to monitor a new mode. In this example, a waiting time is 10 steps. ◊

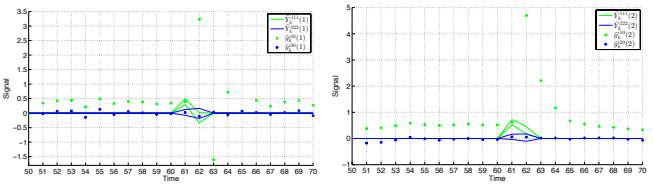

Fig. 2. FI of the second actuator fault

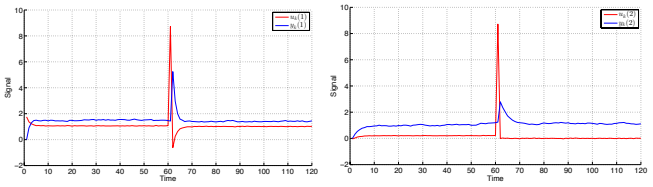

Fig. 3. FTC of the second actuator fault

VI. Conclusions

In this paper, an actuator FTMPC scheme is proposed, where tube-based MPC and set-theoretic FDI are used. In this scheme, FD is passive by invariant sets and FI is active by MPC controllers and tubes. The proposed FTMPC scheme has robust FDI performance, relatively less computational complexity and conservative FI conditions. Besides, for undetectable faults, the PFTC ability of the scheme can still tolerate them to some extent in spite of a degree of performance degradation.

References

[1] J. A. De Doná A. Yetendje, M. M. Seron. Robust MPC multicontroller design for actuator fault tolerance of constrained systems. In *Proceedings of the 18th IFAC World Congress*, Milano, Italy, 2011.

[2] T. Alamo, J.M. Bravo, and E.F. Camacho. Guaranteed state estimation by zonotopes. In *Proceedings of the 42nd IEEE Conference on Decision and Control*, Maui, Hawaii, USA, December 2003.

[3] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki. *Diagnosis and Fault-Tolerant Control*. Springer-Verlag, Berlin, Germany, 2006.

[4] F. Borrelli, A. Bemporad, and M. Morari. *Predictive Control for Linear and Hybrid Systems*. UC-Berkeley, USA, 2013.

[5] J.D. Boskovic and R.K. Mehra. Fault accommodation using model predictive methods. In *Proceedings of the 2002 American Control Conference*, volume 6, pages 5104–5109, 2002.

[6] C. Combastel. A state bounding observer based on zonotopes. In *Proc. of the European Control Conference*, Cambridge, UK, 2003.

[7] D.Q. Mayne, S.V. Raković, R. Findeisen, and F. Allgower. Robust output feedback model predictive control of constrained linear systems. *Automatica*, 42(7):1217 – 1222, 2006.

[8] S. Olaru, J.A. De Doná, M.M. Seron, and F. Stoican. Positive invariant sets for fault tolerant multisensor control schemes. *International Journal of Control*, 83(12):2622–2640, 2010.

[9] D. M. Raimondo, G. R. Marseglia, R. D. Braatz, and J. K. Scott. Fault-tolerant model predictive control with active fault isolation. In *Proceeding s of SysTol*, Nice, France, 2013.

[10] S.V. Rakovic, E.C. Kerrigan, K.I. Kouramas, and D.Q. Mayne. Invariant approximations of the minimal robust positively invariant set. *Automatic Control, IEEE Transactions on*, 50(3):406 – 410, 2005.

[11] F. Stoican and S. Olaru. *Set-theoretic Fault-tolerant Control in Multisensor Systems*. John Wiley & Sons, Inc., 2013.

[12] S. Sun, L. Dong, L. Li, and S. Gu. Fault-tolerant control for constrained linear systems based on MPC and FDI. *International Journal of Information and Systems Sciences*, 4(4):512 –23, 2008.