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

Feng XU[1], Vicenç PUIG[2], Carlos OCAMPO-MARTINEZ[2],
Sorin OLARU[3] and Silviu-Iulian NICULESCU[4]

[1]Center of Intelligent Control and Telescience,
Graduate School at Shenzhen, Tsinghua University, Shenzhen, P.R.China
[2]Universitat Politècnica de Catalunya (UPC),
Institut de Robòtica i Informàtica Industrial (CSIC-UPC), Barcelona, Spain
[3]E3S (SUPELEC Systems Sciences),
Automatic Control Department, Gif sur Yvette, Paris, France
[4]Laboratoire des Signaux et Systèmes,
CNRS-Centrale Supélec, Gif sur Yvette, Paris, France

Abstract

In this paper, a fault-tolerant control (FTC) scheme is proposed for actuator faults, which is based on tube-based model predictive control (MPC) and set-based fault detection and isolation (FDI). In the class of MPC techniques, tube-based MPC can effectively deal with system constraints and uncertainties with relatively low computational complexity compared with other robust MPC techniques such as min-max MPC. Set-based FDI, generally considering the worst case of uncertainties, can robustly detect and isolate actuator faults. In the proposed FTC scheme, fault detection (FD) is passive by using invariant sets, while fault isolation (FI) is active by means of MPC and tubes. The active FI method proposed in this paper is implemented by making use of the constraint-handling ability of MPC to manipulate the bounds of inputs. Whenever after the system has been detected to become faulty, the input-constraint set of the MPC controller is adjusted to actively excite the system for achieving FI guarantees on-line, where an active FI-oriented input set is designed off-line. In this way, the system can be excited in order to obtain more extra system-operating information for FI than the passive FI approaches. Overall, the objective of this paper is to propose an actuator MPC scheme with FI conservatism and computational complexity as little as possible by combing tube-based MPC and set theory under the framework of MPC, respectively. Finally, a case study is used to show the effectiveness of the proposed FTC scheme.

Keywords: Fault detection, fault isolation, set-theoretic method, fault-tolerant control, model predictive control.

1 Introduction

In general, all technical systems are prone to faults. In a controlled system, if the plant itself is more reliable than the used sensors and actuators, when the closed-loop performance deviates from its normal situation, it is possible to find sensors and/or actuators that have become faulty.

As faults can result in abnormal operation/failure, effectively dealing with faulty situations for technical systems is an important specification to assess the global performance of those systems. The objective of FTC is to maintain satisfactory performance for the controlled system even in the presence of faults. In general, FTC is divided into passive FTC (PFTC) and active FTC (AFTC) [2]. PFTC deals with faults by using controller robustness while AFTC handles faults after obtaining fault information by fault diagnosis techniques. The former is relatively easy to be implemented but only has restrictive fault-tolerant ability. Moreover, the larger the number of faults is, the worse the control performance is. Comparatively, AFTC is more flexible because it contains a fault diagnosis module to obtain the real-time fault information. With the obtained fault information, AFTC can deal with the faults more effectively. The fault diagnosis procedure embedded in an FTC scheme generally includes three steps: fault detection, fault isolation and fault estimation. Although AFTC is the topic of the proposed FTC scheme, this paper focuses more on the FD and FI tasks and assumes that actuator-fault magnitudes are known in advance. However, for FTC based on fault estimation and accommodation, the readers are referred to the works such as [6], [7] and [20]. Additionally, due to relatively low complexity and the ability of dealing with system constraints, MPC is chosen as the control strategy for the proposed scheme [4, 11, 22]. As an optimization-based method, robust MPC itself has a degree of PFTC ability with respect to additive uncertainties [3].

In [13], an actuator FTC scheme using feedback-gain control and invariant sets was proposed, where a bank of controllers were designed to handle faults in different actuators and the FDI task was implemented by using invariant set-based passive FDI methods. However, this scheme does not consider constraints on system variables and needs to wait until the residual has entered into its invariant set to isolate faults. In [19], a fault-tolerant model predictive control (FTMPC) scheme using the Kalman filter was proposed, which focused on the implementation of an FTMPC scheme without addressing in detail the features such as feasibility. In [23], an actuator FTMPC scheme with invariant set-based FDI was presented, which had relatively low complexity because of the use of invariant sets for FDI. However, due to the passive implementation of FDI, the set separation-based FDI condition is more conservative, which implies the loss of potential FDI and FTC performance to some extent. The same authors extend the previous approach to the sensor case using a multisensor scheme [24]. In [16], an FTMPC scheme using set-membership FDI was proposed. This work used an approach that combined passive FD and active FI but used a different implementing method. The active FI method proposed in [16] can reduce FI conservatism but at expenses of high computational complexity due to the requirement of computing fault-separating inputs online. Moreover, the proposed scheme in [16] does not provide guaranteed FI conditions to check whether the considered faults are isolable or not in advance.

Since faults in actuators and sensors generally have different features, the current paper focuses on the actuator faults by exploiting the potential of the proposed scheme. In particular, the objective of this paper is to propose a new scheme of actuator FTMPC to not only obtain less conservative FI and FI guarantees but also implement FTC with relatively low complexity. The proposed FTC scheme can also obtain a balance between FI complexity and conservatism. In the scheme, FD is passively implemented with invariant sets and FI is actively carried out by using MPC and tubes that can isolate faults during the transition induced by faults.

The principle of active FI consists in adjusting the input-constraint set of MPC controller to an off-line designed FI-oriented input set that can guarantee FI. In real time, whenever a fault is detected, the designed input set is used as the temporary input-constraint set of the MPC controller to implement FI during the transition. Moreover, since this input set is constructed off-line, guaranteed FI conditions can be verified off-line by using invariant sets and established on-line by MPC controller for on-line FI guarantees. The proposed FTC scheme is shown in 1,

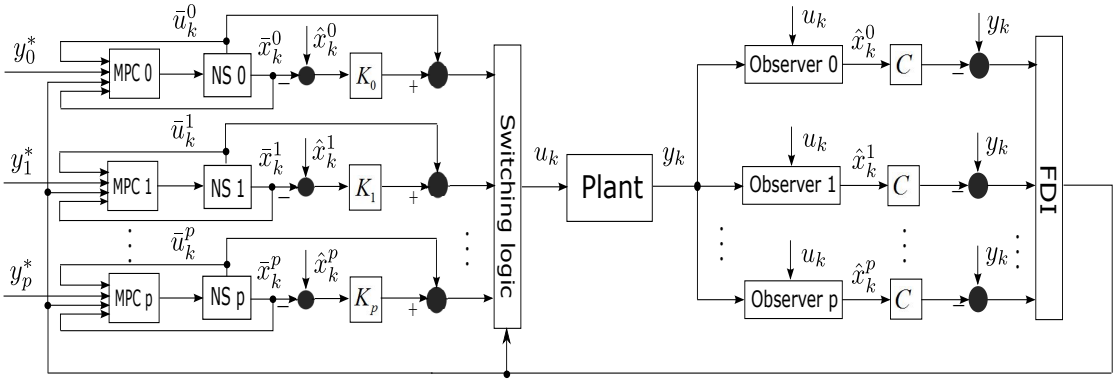


Figure 1: Actuator FTMPC scheme

where *NS* denotes *Nominal System* and the subscript k is only used to show that the discrete-time system is considered in this paper.

The advantages of the proposed scheme are twofold. First, a new actuator FTC scheme integrating MPC with set-based FDI to retain their advantages is proposed. Second, a new active FI strategy based on tube-based MPC to obtain FI guarantees and a balance of FI conservatism and complexity is implemented. The work presented in this paper is inspired by preliminary results by the authors shown in [21].

The remainder of this paper is divided into five sections. Section II, introduces the proposed FTC scheme. Section III presents the FDI strategy based on invariant sets and tubes. Section IV introduces the FTC approach. In Section V, a case study is used to show the effectiveness of the proposed scheme. Finally, Section VI gives some conclusions on the approach.

Note that, in this paper, the inequalities are understood element-wise, O, I and $\text{diag}(\cdot)$ denote the zero, the identity and the diagonal matrices with suitable dimensions, respectively, $|\cdot|$ represents the element-wise absolute value, $\mathbb{B}^r$ is a box composed of r unitary intervals and $\oplus$ and $\ominus$ notate the Minkowski sum and Pontryagin difference, respectively.

2 System Description

2.1 Plant Model

It is assumed that the monitored system is described by a linear discrete time-invariant model including actuator faults, disturbances and noises:

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

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

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 parametric matrices, $x_k \in \mathbb{R}^n$, $u_k \in \mathbb{R}^p$ and $y_k \in \mathbb{R}^q$ are the state, input and output vectors at time instant k, respectively, ω_k and η_k are unknown process disturbances and measurement noise vectors, respectively and F is used to model actuator modes (healthy and faulty) important/critical for system performance/safety.

In (1), matrix F incorporates the considered actuator modes. During real-time operation, a mode switching implies a change of the value of F (i.e. fault occurrence or system recovery to the healthy situation). Moreover, F is assumed to be constant for each mode but time-variant during the whole dynamical behaviors where mode switchings are included.

Assumption 2.1 *Disturbances and noises ω_k and η_k are unknown and bounded by sets*

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

respectively, where ω^c, η^c, $\bar{\omega}$ and $\bar{\eta}$ are assumed to be known and constant vectors. □

Assumption 2.2 *Considered faults Single, abrupt and multiplicative faults are considered and the faults are assumed to be persistent, namely the duration of the faults is longer than the detection and isolation time needed.* □

Under Assumption 2.2, it can be observed that 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 actuator mode while F_i ($i \neq 0$) modeling the i-th actuator-fault mode is denoted as

$$F_i = \text{diag}(1 \ \ldots \ 1 \ \overset{i}{\underset{\downarrow}{f_i}} \ 1 \ \ldots \ 1), \tag{3}$$

where f_i is a scalar inside the interval $[0, 1)$, which models the actuator-fault magnitude of the i-th actuator.

Notice that it is possible to extend the proposed FTMPC scheme to deal with sensor faults, multiple faults and additive faults. For example, if there are more elements rather than a single element different to "1" in the fault-modeling matrix F, the proposed method can be used to handle multiple faults (see [17]).

Assumption 2.3 *Stabilizability and detectability The pairs (A, BF_i) for all $i \in \mathbb{I}$ and (A, C) are stabilizable and detectable, respectively.* □

In this scheme, the input and state constraints are taken into account, which are denoted as

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

respectively, where the vectors x^c, u^c, $\bar{x}$ and $\bar{u}$ are known and constant. W, V, X and U defined in (2) and (4) can be rewritten into zonotopes. Thus, in this paper, all set manipulations are implemented by zonotopes. The notion of zonotopes is given in Definition .1 in Appendex 6.

2.2 Output Setpoints

It is mentioned that $p+1$ actuator modes are considered. Thus, the proposed FTMPC scheme should have $p+1$ different nominal models, each corresponding to one mode. For the i-th mode, the corresponding nominal model is given as

$$\bar{x}^i_{k+1} = A\bar{x}^i_k + BF_i\bar{u}^i_k + \omega^c, \tag{5a}$$
$$\bar{y}^i_k = C\bar{x}^i_k + \eta^c, \tag{5b}$$

where $\bar{u}_k$, $\bar{x}_k$ and $\bar{y}_k$ denote the nominal input, state and output vectors, respectively. For simplicity, it is considered that ω^c and η^c, representing the centers of the sets in (1a) and (1a), are zero vectors.

The control objective under the i-th mode is to regulate the output vector around a given setpoint y_i^*, i.e., in the absence of uncertainties,

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

In this paper, the model in (5) does not consider ω^c and η^c for simplicity of explaination. By using (5), a state-input setpoint pair (x_i^*,u_i^*) corresponding to y_i^* in the i-th mode can be computed by

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

However, without loss of generality, in the case that ω^c and η^c are non-zero, ω^c and η^c can be added into (5a) and (5b), respectively.

Assumption 2.4 *State-input setpoint pair For the i-th mode, the equation* (7) *is solvable for all* $i \in \mathbb{I}$. □

Under Assumption 2.4, a state-input setpoint pair (x_i^*, u_i^*) corresponding to y_i^* can be obtained by solving (7) or degrading the expected performance (i.e., changing the output setpoint) in order to guarantee that (7) is solvable. For a given mode, (7) may have multiple solutions (i.e., the state-input setpoint pair may be not unique) or no solution. Thus, the designer should decide a satisfactory state-input setpoint pair according to particular requirements. Additionally, although the given output can be time-variant (i.e., tracking problem), only the regulation problem is considered in the current paper.

2.3 Observers and Controllers

The tube-based MPC technique used in this scheme is based on [12]. As in [12], for each MPC controller, a state observer is designed. Thus, a bank of observers should be designed to match all modes, each observer matching one mode [1]. Correspondingly, 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 matrix that is selected to stabilize the observer dynamics (8), which is always possible under Assumption 2.3.

In order to control the system under different actuator modes, a bank of tube-based output feedback MPC controllers are used, each corresponding to one mode. The nominal system corresponding to the i-th mode is obtained by neglecting ω_k and η_k in (5).

According to [12], the control law of the i-th tube-based MPC controller is

$$u_k = \bar{u}_k^i + K_i(\hat{x}_k^i - \bar{x}_k^i), \tag{9}$$

where K_i is the corresponding feedback-gain matrix.

[1] This is similar to the idea used in the Multiple Model Adaptive Estimation (MMAE) approach where a bank of parallel Kalman filters, each with a different model, is used. However, in the MMAE approach [5], the hypothesis testing approach is used to determine which is the model with the highest likelihood to explain the input/output data.

3 Fault Detection and Isolation

3.1 System Analysis

In the i-th mode, F takes the value F_i, and the i-th tube-based MPC controller, the i-th state-input setpoint pair and the i-th observer are used in the closed-loop system. Moreover, the state estimation error of the j-th observer is defined as

$$\tilde{x}_k^{i,j,i} = x_k - \hat{x}_k^j. \tag{10}$$

Regarding the superscript notation $\tilde{x}_k^{i,j,i}$, the first index means the i-th system mode, the second index denotes the j-th observer and the third index denotes that the i-th controller is currently selected for closed-loop operation. Thus, $\tilde{x}_k^{i,j,i}$ denotes the state estimation error of the j-th observer when the current closed-loop system is in the i-th mode and with the i-th MPC controller.

If $j \neq i$ in (10), the dynamics of $\tilde{x}_k^{i,j,i}$ can be derived by using (1), (8) and (9) as

$$\begin{aligned}\tilde{x}_{k+1}^{i,j,i} =&(A - L_jC)\tilde{x}_k^{i,j,i} + B(F_i - F_j)\bar{u}_k^i + \omega_k - L_j\eta_k \\ &+ B(F_i - F_j)K_i(\hat{x}_k^i - \bar{x}_k^i),\end{aligned} \tag{11}$$

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

$$\tilde{y}_k^{i,j,i} = y_k - \hat{y}_k^j = C\tilde{x}_k^{i,j,i} + \eta_k. \tag{12}$$

Moreover, in the i-th mode, the term $\hat{x}_k^i - \bar{x}_k^i$ appearing in both (9) and (11) is denoted as

$$e_k^{i,i,i} = \hat{x}_k^i - \bar{x}_k^i, \tag{13}$$

whose dynamics can be derived by using (5) and (8) as

$$e_{k+1}^{i,i,i} = (A + BF_iK_i)e_k^{i,i,i} + L_iC\tilde{x}_k^{i,i,i} + L_i\eta_k, \tag{14}$$

where $\tilde{x}_k^{i,i,i}$ corresponds to the case $j = i$ in (10) and its dynamics can be obtained from (11), i.e.,

$$\tilde{x}_{k+1}^{i,i,i} = (A - L_iC)\tilde{x}_k^{i,i,i} + \begin{bmatrix} I & -L_i \end{bmatrix} \begin{bmatrix} \omega_k \\ \eta_k \end{bmatrix}. \tag{15}$$

Due to $\omega_k \in W$ and $\eta_k \in V$, a *robust positively invariant* (RPI) set of $\tilde{x}_k^{i,i,i}$, denoted as $\tilde{X}^{i,i,i}$, can be constructed. In this paper, the notion of RPI sets and the method to construct the RPI sets are based on [8], [9] and [14], which are given in Appendix 6.

As long as $\tilde{x}_{k^*}^{i,i,i} \in \tilde{X}^{i,i,i}$ holds, $\tilde{x}_k^{i,i,i} \in \tilde{X}^{i,i,i}$ always holds for all $k > k^*$. Similarly, considering $\tilde{x}_k^{i,i,i} \in \tilde{X}^{i,i,i}$ and $\eta_k \in V$, an RPI set of $e_k^{i,i,i}$, denoted as $E^{i,i,i}$, can be constructed by using (14). For the i-th mode, if a fault is detected, an input set $\bar{U}_f^i$ is defined for FI analysis as

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

which should be employed whenever a fault is detected and supposes that

$$\bar{u}_k^i \in \bar{U}_f^i,$$

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

Remark 3.1 *Input-constraint set for FI In this paper, an active FI strategy is proposed. The rationale of the FI strategy is that, after FD, the input-constraint set of the i-th optimization problem corresponding to the i-th MPC controller is adjusted (to $\bar{U}_f^i$) to restrict inputs to values that can excite the plant to enable FI. Besides, $\bar{U}_f^i$ will only be used for FI when the system is in the i-th mode after FD. Moreover, $\bar{U}_f^i$ is different from the input-constraint set U. Likewise, in the proposed FI strategy, after a fault is isolated and simultaneously the system is reconfigured, $\bar{U}_f^i$ will not be used any longer. At this stage, $\bar{U}_f^i$ is introduced in order to help the readers understand the following proposed FI method. However, the detailed introduction of $\bar{U}_f^i$ will be given in Section 4.* □

Similarly, if considering $e_k^{i,i,i} \in E^{i,i,i}$ and $\bar{u}_k^i \in \bar{U}_f^i$ in (11), an RPI set of $\tilde{x}_k^{i,j,i}$, denoted as $\tilde{X}^{i,j,i}$, can be determined. Furthermore, the set of the corresponding output-estimation error is

$$\tilde{Y}^{i,j,i} = C\tilde{X}^{i,j,i} \oplus V. \tag{16}$$

For the particular case $j = i$, the output-estimation-error set $\tilde{Y}^{i,i,i}$ corresponding to $\tilde{X}^{i,i,i}$ can also be determined and used for FDI. Generally, the RPI sets $\tilde{X}^{i,i,i}$, $E^{i,i,i}$ and $\tilde{X}^{i,j,i}$ should be as small as possible, being ideally tight approximations of the minimal RPI set.

3.2 Fault Detection

The FD approach used in this paper is a passive approach based on invariant sets, which can simplify the FD task into only testing whether or not the residual is inside its corresponding invariant set. The advantage of the used FD method consists in its low computational complexity.

Considering (11) and (14), since $\omega_k \in W$ and $\eta_k \in V$, if $\bar{u}_k^i \in \bar{U}_f^i$ always holds, it can be observed that, as long as $e_k^{i,i,i} \in E^{i,i,i}$ holds, $\tilde{x}_k^{i,j,i} \in \tilde{X}^{i,j,i}$ $(j \neq i)$ can always hold. However, if considering (15), it can be seen that $\tilde{X}^{i,i,i}$ is independent of the effect of $e_k^{i,i,i}$ and $\bar{u}_k^i$ while $E^{i,i,i}$ is dependent of $\tilde{X}^{i,i,i}$. Thus, theoretically, the most convenient way to detect faults is to test the inclusion $\tilde{x}_k^{i,i,i} \in \tilde{X}^{i,i,i}$[2]. But, practically, since $\tilde{x}_k^{i,i,i}$ is not obtainable, instead, only the signal $\tilde{y}_k^{i,i,i}$ can be used. Thus, the first criterion for FD is to test whether or not

$$\tilde{y}_k^{i,i,i} \in \tilde{Y}^{i,i,i} \tag{17}$$

is violated in real time. If a violation of (17) is detected, it means that a fault has occurred. Otherwise, it is considered that the system still operates in the i-th mode.

Although (17) can be used for FD, if only (17) is used, the fault sensitivity of the proposed FTC scheme will not be fully exploited. The reason is due to the fact that even though (17) holds, it cannot be guaranteed that the inclusion $\tilde{x}_k^{i,i,i} \in \tilde{X}^{i,i,i}$ holds too, which means that the detection of $\tilde{y}_k^{i,i,i} \in \tilde{Y}^{i,i,i}$ has a different fault sensitivity from that of $\tilde{x}_k^{i,i,i} \in \tilde{X}^{i,i,i}$. In this case, it is necessary to consider the second FD criterion to describe this situation, i.e., to test whether or not

$$e_k^{i,i,i} \in E^{i,i,i} \tag{18}$$

[2]Under the framework of the proposed FTC scheme, the mode switching has several different cases including the situations from the heathy mode to a faulty mode, from a faulty mode to another faulty mode and from a faulty mode to the healthy mode. However, without loss of generality, the terms and/or concepts *fault*, *fault occurrence*, *fault detection* and *fault isolation* are used in this paper for generally denoting *mode*, *mode switching*, *mode-switching detection* and *mode-switching isolation*, respectively.

is violated in real time. If (18) is violated, it also implies that a fault has occurred. Note that, as aforementioned, the FD criterion (18) can indirectly describe the inclusions corresponding to the other observers, i.e.,

$$\tilde{y}_k^{i,j,i} \in \tilde{Y}^{i,j,i}, j \neq i. \tag{19}$$

Thus, the FD strategy of this proposed FTC scheme is to use both (17) and (18). As long as either of them is violated, it implies that the system has become faulty.

Remark 3.2 *Fault detection The simultaneous use of the criteria* (17) *and* (18) *means that the system information captured by all the observers has been used for FD. Additionally, for the proposed FD strategy, even though some faults occur, it is possible that the FD criteria* (17) *and* (18) *are not violated. This means that these faults cannot be detected and will not actively be tolerated under the framework of this proposed active FTC scheme. Instead, they can only be tolerated to some extent by the PFTC ability of the proposed scheme.* □

3.3 Fault Isolation

3.3.1 Behaviors after Faults

In the scheme, the FI task is started up after a fault is detected by the proposed FD strategy. In order to describe the FI strategy, without loss of generality, it is assumed that the l-th ($l \neq i$) fault occurs, i.e., after that, the system mode changes from i to l. Although the mode changes from i to l, before the fault is isolated and the system is reconfigured, the closed-loop system structure will not change yet, which implies that the closed-loop system is still composed of the same controller and observer during the FI phase.

According to (1), (5), (8) and (9), 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

$$\begin{aligned}\tilde{x}_{k+1}^{l,j,i} =&(A - L_jC)\tilde{x}_k^{l,j,i} + B(F_l - F_j)\bar{u}_k^i + \omega_k - L_j\eta_k \\ &+ B(F_l - F_j)K_i e_k^{l,i,i}\end{aligned} \tag{20}$$

and $e_k^{i,i,i}$ in (14) changes to $e_k^{l,i,i}$ with the dynamics

$$e_{k+1}^{l,i,i} = (A + BF_iK_i)e_k^{l,i,i} + L_iC\tilde{x}_k^{l,i,i} + L_i\eta_k. \tag{21}$$

In order to collect all the available system-operating information for fault diagnosis after the l-th fault from the i-th mode, a vector is defined as

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

According to (20) and (21), the dynamics of $\xi_k^{i\to l}$ can be obtained as

$$\xi_{k+1}^{i\to l} = A_{i\to l}\xi_k^{i\to l} + B_{i\to l}\bar{u}_k^i + E_{i\to l}^{\omega}\omega_k + E_{i\to l}^{\eta}\eta_k, \tag{22}$$

where

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

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

Remark 3.3 *Stability Under Assumption 2.3, the observer and feedback gains $L_0, L_1, \ldots, L_p$ and $F_0, F_1, \ldots, F_p$ can be designed to make $A_{i\to l}$ a Schur matrix for all i, $l \in \mathbb{I}$. With (22), the closed-loop system can be stable by designing the observer and feedback gains and the parameters of open-loop optimization problem of the tube-based MPC controller, see [12].* □

Furthermore, if considering $\bar{u}^i_k \in \bar{U}^i_f$, $\omega_k \in W$ and $\eta_k \in V$, an RPI set of $\xi^{i\to l}_k$ 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 $\xi^{i\to l}_k$ can be obtained. For example, an RPI set (denoted as $\tilde{X}^{l,j,i}$) of $\tilde{x}^{l,j,i}_k$ can be obtained by projecting $\Xi^{i\to l}$ to the space of $\tilde{x}^{l,j,i}_k$. Similarly, an RPI set (denoted as $E^{l,i,i}$) of $e^{l,i,i}_k$ can be constructed. This implies that, after the l-th fault, $\tilde{x}^{l,j,i}_k$ and $e^{l,i,i}_k$ will converge into $\tilde{X}^{l,j,i}$ and $E^{l,i,i}$, respectively. Moreover, with (1b), the set of the corresponding output-estimation error can be obtained as

$$\tilde{Y}^{l,j,i} = C\tilde{X}^{l,j,i} \oplus V. \tag{23}$$

In the case that the system mode switches from i to l, all sets of output-estimation errors can be constructed, which are listed in Table 1. Note that, in Table 1, each row excluding the i-th one corresponds to one candidate mode after the mode switching from the i-th one.

Table 1: Sets of output-estimation errors

	Observer 0	$\cdots$	Observer i	$\cdots$	Observer p
Mode 0	$\tilde{Y}^{0,0,i}$	$\cdots$	$\tilde{Y}^{0,i,i}$	$\cdots$	$\tilde{Y}^{0,p,i}$
$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$	$\vdots$
Mode i	$\tilde{Y}^{i,0,i}$	$\cdots$	$\tilde{Y}^{i,i,i}$	$\cdots$	$\tilde{Y}^{i,p,i}$
$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$	$\vdots$
Mode p	$\tilde{Y}^{p,0,i}$	$\cdots$	$\tilde{Y}^{p,i,i}$	$\cdots$	$\tilde{Y}^{p,p,i}$

3.3.2 Residual Tubes

Generally, the residual is defined as a signal sensitive to faults and with a manageable magnitude. In this FTC scheme, the output-estimation errors are defined as the residual signals. The dynamics of $\tilde{x}^{l,l,i}$ extracted from (22) are used for the FI implementation, which has the form

$$\tilde{x}^{l,l,i}_{k+1} = (A - L_lC)\tilde{x}^{l,l,i}_k + \omega_k - L_l\eta_k, \tag{24}$$

while $\tilde{x}^{l,j,i}$ ($j \neq l$) will not be used for the direct FI implementation but for the establishment of guaranteed FI conditions. By using W and V to replace ω_k and η_k, the set-based description of $\tilde{x}_k^{l,l,i}$ and $\tilde{y}_k^{l,l,i}$ can be obtained as

$$\tilde{X}_{k+1}^{l,l,i} = (A - L_l C)\tilde{X}_k^{l,l,i} \oplus W \oplus (-L_l V), \tag{25a}$$

$$\tilde{Y}_k^{l,l,i} = C\tilde{X}_k^{l,l,i} \oplus V. \tag{25b}$$

Proposition 3.1 *Estimation-error tubes Given that the l-th ($l \neq i$) fault occurs when the system is 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 (25) 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 $k \geq k*$.*

Proof : Since (25a) considers the worst case of the uncertain factors ω_k and η_k in (24), if at time instant $k*$, $\tilde{x}_{k*}^{l,l,i} \in \tilde{X}_{k*}^{l,l,i}$ holds, it implies that $\tilde{x}_k^{l,l,i} \in \tilde{X}_k^{l,l,i}$ and $\tilde{y}_k^{l,l,i} \in \tilde{Y}_k^{l,l,i}$ will always hold for all $k \geq k*$. □

It is assumed that the l-th fault is detected at time instant k_d when the system is in the i-th mode. If an initial set is used to initialize (25a) at time instant k_d, the tubes corresponding to the state and output estimation errors generated by (25) can be denoted as

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

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

That initial set is used to initialize the dynamics (25) to generate tubes for FI and introduced here for the discussion of the FI method. The detailed constructing method for set initialization will be presented in Section 3.3.4.

When the system is in the i-th mode, a violation of (17) or (18) implies that a mode changing from i to another unknown mode has occurred (this unknown mode is denoted as $f \in \mathbb{I} \setminus \{i\}$), i.e., there are p mode candidates except for the i-th one. Thus, for FI, all the p output-estimation error tubes $\tilde{\mathbb{T}}_{k_d}^{y,l,l,i}$ ($l \in \mathbb{I} \setminus \{i\}$) have to be obtained. At time instant k_d, the proposed FI algorithm generates p output-estimation-error tubes $\tilde{\mathbb{T}}_{k_d}^{y,l,l,i}$ ($l \in \mathbb{I} \setminus \{i\}$), each corresponding to a candidate mode. Moreover, for the p corresponding observers, as long as

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

are guaranteed at the FD time such that

$$\tilde{y}_{k_d}^{f,l,i} \subseteq \tilde{Y}_{k_d}^{l,l,i}. \tag{28}$$

Therefore, this implies that, among the p generated output-estimation-error tubes after FD, there exists at least one tube (here it is assumed that this tube corresponds to the m-th actuator mode) that can always satisfy

$$\tilde{y}_k^{f,m,i} \subseteq \tilde{Y}_k^{m,m,i},\ \ k \geq k_d,\ m \in \mathbb{I} \setminus \{i\}. \tag{29}$$

If the fault is indexed by l (i.e., $f = l$) and (27) is satisfied, for all $k \geq k_d$, $\tilde{\mathbb{T}}_{k_d}^{y,l,l,i}$ can always satisfy $\tilde{y}_k^{f,l,i} \subseteq \tilde{Y}_k^{l,l,i}$. This implies that the fault will be indicated by one of the p tubes that can always satisfy (29).

3.3.3 Fault Isolation Approach

In order to isolate a fault, it has to guarantee that one and only one tube can always satisfy its corresponding inclusion (29) after FD and then the fault can be indicated by the index of this tube. Based on this idea, guaranteed FI conditions are established in Proposition 3.2.

Proposition 3.2 *Guaranteed FI conditions When the system is in the i-th mode, for any observer out of the $p+1$ observers (assume that it is indexed by j), if all the $p+1$ output-estimation-error sets corresponding to this observer (i.e., the $p+1$ sets in the j-th column of Table 1) can satisfy*

$$\tilde{Y}^{j,j,i} \cap \bigcup_{l=0}^{p} \tilde{Y}^{l,j,i} = \varnothing, \quad l \neq j,\ i,\ j,\ l \in \mathbb{I}, \tag{30}$$

once a mode changing from the i-th mode to another considered mode is detected at time instant k_d, this mode can be isolated during the transition induced by the mode changing by searching the output-estimation-error tube that satisfies (29) *for all $k \geq k_d$.*

Proof : As concluded, $\tilde{\mathbb{T}}_{k_d}^{y,j,j,i}$ will converge into $\tilde{Y}^{j,j,i}$. If (30) holds, $\tilde{\mathbb{T}}_{k_d}^{y,j,j,i}$ is able to confine the output-estimation error $\tilde{y}_k^{l,j,i}$ only under the condition $l = j$. If $l \neq j$, at the first several steps, $\tilde{\mathbb{T}}_{k_d}^{y,j,j,i}$ is able to confine $\tilde{y}_k^{l,j,i}$ due to the initialization condition (27). But, as $\tilde{\mathbb{T}}_{k_d}^{y,j,j,i}$ approaches $\tilde{Y}^{j,j,i}$, $\tilde{y}_k^{l,j,i}$ diverges from $\tilde{\mathbb{T}}_{k_d}^{y,j,j,i}$. This implies that, under the condition (30), by searching the tube that is always able to confine $\tilde{y}_k^{l,j,i}$ after FD, the fault can be isolated. □

3.3.4 Construction of Initial Sets

As mentioned in (26), one of the key points of the proposed FI strategy consists in constructing the initial sets of state-estimation errors, which satisfy (27) at time instant k_d to initialize (25) in order to generate the output-estimation-error tubes. For the j-th observer, according to (12), it can obtain

$$C\tilde{x}_{k_d}^{i,j,i} \in \{\tilde{y}_{k_d}^{i,j,i}\} \oplus (-V). \tag{31}$$

In (31), since $\tilde{y}_{k_d}^{i,j,i}$ can be obtained in real time, it is always possible to construct a zonotopic set containing $\tilde{x}_{k_d}^{i,j,i}$ at the FD time. In [1], a method computing a zonotope containing the intersection of a strip and a zonotope is given in Property .4. Based on this method, a zonotope containing $\tilde{x}_{k_d}^{i,j,i}$ can be constructed by considering (31) composed of q inequalities (i.e., strips). Besides, the method proposed in [10] can also be used to construct a zonotopic set containing $\tilde{x}_{k_d}^{i,j,i}$. This method can compute a zonotopic approximation of the intersection of a zonotope and a polytope. With this method, (31) is considered as a whole that describes a polytope to construct an initial zonotope, which can be seen in Property .5.

Remark 3.4 *Construction of initial sets If C is invertible, a set bounding $\tilde{x}_{k_d}^{i,j,i}$ can be directly obtained by* (31) *with the inverse of C. If C is not invertible, an initial zonotope to bound $\tilde{x}_{k_d}^{i,j,i}$ can be obtained by the method in Propositions .4 or .5. In the second case, it may need to give a zonotopic starting set for the methods in Propositions .4 and .5 and this set can be designed according to the physical constraints of the system.* □

According to (31), it can be observed that, for the j-th observer, the expression of (31) is independent of system mode changing. This means that (31) can always be used to construct a set to bound the state estimation error of the j-th observer in any mode. Since X, U, W and V can be rewritten as zonotopes, from the computational point of view, all tubes are generated by using zonotopes.

4 Fault-tolerant Control

4.1 Steady-state Behaviors

In the proposed FTC scheme, the system operation is divided into the transient-state and steady-state phases. The steady-state operation corresponds to the situation that all relevant system signals corresponding to a system mode are inside their corresponding bounding sets, respectively. Comparatively, the transient-state operation describes the operating process between fault occurrence and the steady-state operation of the mode corresponding to this fault. In this paper, these two operations will be discussed, separately. This subsection focuses on the system behaviors during the steady-state operation.

At steady state of the i-th mode, the tube-based MPC technique proposed in [12] is adopted to implement FTC and the control law of the i-th one is given in (9). For the tube-based MPC controller (9), the key part $\bar{u}_k^i$ is the open-loop optimization problem based on the i-th nominal system as in (5).

X and U are the hard system constraints that imply the indirect constraints on the nominal system-based open-loop optimization problem. In the i-th mode, the indirect input constraint is computed via (9), i.e.,

$$u_k = \bar{u}_k^i + K_i e_k^{i,i,i}.$$

As per Section 3.1, at steady state of the i-th mode,

$$e_k^{i,i,i} \in E^{i,i,i}$$

should hold. Thus, the input-constraint set of the open-loop optimization problem can be obtained as

$$\bar{u}_k^i \in \bar{U}^i = U \ominus K_i E^{i,i,i}. \tag{32}$$

Additionally, taking

$$x_k = \bar{x}_k^i + e_k^{i,i,i} + \tilde{x}_k^{i,i,i}$$

into account, the hard state-constraint set for the steady-state functioning can be described as

$$\bar{x}_k^i \in \bar{X}^i = X \ominus (E^{i,i,i} \oplus \tilde{X}^{i,i,i}). \tag{33}$$

Assumption 4.1 *Indirect constraint sets In the i-th mode, $\bar{X}^i$ and $\bar{U}^i$ are non-empty for all $i \in \mathbb{I}$.* □

The non-emptiness of $\bar{X}^i$ and $\bar{U}^i$ is the precondition for using the tube-based MPC technique. Assumption 4.1 is a well-known and accepted condition in the field. Under Assumption 4.1, the open-loop optimization problem of the i-th tube-based MPC controller, based on the i-th nominal system (5), has the following form

$$\begin{aligned} J_k = \min_{\bar{\mathbf{u}}^i} & \sum_{j=0}^{N-1} \|(\bar{x}_{k+j|k}^i - x_i^*)\|_{Q_i}^2 + \|(\bar{u}_{k+j|k}^i - u_i^*)\|_{R_i}^2 \\ & + \|(\bar{x}_{k+N|k}^i - x_i^*)\|_{P_i}^2 \\ \text{subject to} \quad & \bar{x}_{k+j|k}^i \in \bar{X}^i, \\ & \bar{u}_{k+j|k}^i \in \bar{U}^i, \\ & \bar{x}_{k+N|k}^i \in \bar{X}_T^i, \\ & \bar{x}_{k|k}^i = \bar{x}_k^i, \end{aligned} \tag{34}$$

where $\bar{\mathbf{u}}^{\mathbf{i}} = [\bar{u}^i_{k|k}, \bar{u}^i_{k+1|k}, \cdots, \bar{u}^i_{k+N-1|k}]$ is the optimized control sequence over the horizon N, Q_i R_i and P_i are positive-definite matrices and $\bar{X}^i_T$ is the corresponding terminal state constraint set. The purpose of adding the terminal constraint in (34) is for feasibility and stability. In (34), $\bar{X}^i_T$ is defined as the *maximal control invariant* (MCI) set of the i-th nominal system corresponding to the nominal constraint sets $\bar{X}^i$ and $\bar{U}^i$ such that the i-th tube-based MPC controller is feasible (see Definition .6 in Appendex for the MCI sets). As mentioned in Remark 3.3, the tube-based MPC controller can be designed to make the closed-loop system stable, see [3] and [12] for the details of tube-based MPC.

4.2 Transient-state Behaviors before FD

As aforementioned, after fault occurrence, the system leaves from the steady-state operation and enters into the transient-state operation. Different from the steady-state operation of the i-th mode, the fault occurrence implies that the system mode changes from the i-th one to another one that will be denoted by an index l ($l \neq i$).

In order to analyze the transient-state behaviors induced by a fault, the transient-state operation is divided into three different phases. The first phase starts from the occurrence till detection of the fault, the second phase starts from the detection to isolation of the fault and the third one begins from system reconfiguration to the steady-state operation of the l-th mode. Considering that the second and third phases of the transition correspond to the FI task, this subsection only focuses on the first-phase transition and the other two transient-state phases will be discussed in the next subsection.

Remark 4.1 *After-fault behaviors When the system is in the i-th mode at the beginning, after the l-th fault, $\tilde{y}^{i,i,i}_k$ and $e^{i,i,i}_k$ will change into $\tilde{y}^{l,i,i}_k$ and $e^{l,i,i}_k$, respectively.* □

During the first phase of the transition, even though the l-th fault has occurred, the FD criteria (17) and (18) still hold, i.e.,

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

and

$$e^{l,i,i}_k \in E^{i,i,i}.$$

Although the FD criteria (17) and (18) still hold during the first phase of the transition, it cannot be guaranteed that

$$\tilde{x}^{l,i,i}_k \in \tilde{X}^{i,i,i} \tag{35}$$

can still hold, which can be observed from (20) and (21). This problem is is inevitable. Because the satisfaction of (35) cannot be guaranteed, during this transient-state phase, the state constraint

$$x_k = \bar{x}^i_k + e^{l,i,i}_k + \tilde{x}^{l,i,i}_k \in X$$

may be violated. However, notice that, during the first phase of the transition, the input constraint

$$u_k = \bar{u}^i_k + K_i e^{l,i,i}_k \in U$$

always holds under the satisfaction of Assumption 4.1 and $e^{l,i,i}_k \in E^{i,i,i}$. As mentioned, since the problem indicated in (35) is inevitable, the satisfaction of the state constraint has to be assumed during this phase.

Assumption 4.2 *First-phase transition During the first-phase transition, the inclusion $x_k = \bar{x}^i_k + e^{l,i,i}_k + \tilde{x}^{l,i,i}_k \in X$ always holds.* □

Considering that the open-loop optimization problem in (34) is not affected by the real system, then its feasibility can always be preserved during the first phase of the transition. Moreover, during this phase, the closed-loop system is still composed of the same elements with the i-th *fault-free* mode. Although the l-th fault has occurred, the process considers that the system still operates in the i-th mode as long as both state and input constraints are satisfied.

4.3 Transient-state Behaviors during FI

The active FI task corresponds to the second phase of the transition. During this phase, it is already known that a fault has occurred in the system. Thus, the most important objective is to isolate the fault. The basic FI principle here is to directly change the input-constraint set of the i-th open-loop optimization problem on the i-th nominal system to indirectly change the input set of the plant to force the satisfaction of the proposed FI conditions by means of the constraint-handling ability of the open-loop MPC optimization problem behind the MPC controller. In this way, the plant input vector can be confined into a predefined set U_f^i to excite the system and to obtain more system-operating information for FI implementation. Note that U_f^i for active FI has already been briefly introduced in Remark 3.1.

As observed from (22) and (23), when the system mode changes from i to l, the sets of the state and output estimation errors are determined by the sets of $\bar{u}_k^i$, ω_k and η_k and the fault magnitudes if it is considered that the observer and feedback gains have already been designed. Without explicitly considering the observer and feedback gains, a function is used to describe the sets of the output-estimation errors to help the readers understand the proposed FI approach, i.e.,

$$\tilde{Y}^{l,j,i} = f^{i\to l}(\bar{U}_f^i, W, V),\ j \neq l, \tag{36}$$

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

Assumption 4.3 *Input-constraint set In the i-th mode, for all $i \in \mathbb{I}$, there exists an input set $\bar{U}_f^i$ such that the FI conditions proposed in Proposition 3.2 are satisfied.* □

Thus, under Assumption 4.3, at the time instant when a switching from the mode i to l is detected, if $\bar{u}_k^i$ can always be confined inside the FI input set $\bar{U}_f^i$ by the open-loop optimisation problem of the i-th MPC controller, the FI conditions in Proposition 3.2 can be forced to hold on-line by $\bar{U}_f^i$ and then the FI approach proposed in Section 3.3 can be used to isolate the fault. Thus, when the system is in the i-th mode, the tube-based MPC controller has two objectives:

- steady-state operation (including the first-phase transition): no fault is detected and the main task is to achieve system performance. Thus, in order to make full use of the potential performance of the system, the input-constraint set $\bar{U}^i$ is used for the i-th open-loop optimization problem.

- transient-state operation (only the second phase): a fault is detected and the main task is to isolate the fault and reconfigure the system to obtain satisfactory performance even in the presence of the fault. During this stage, the proposed FI approach actively adjusts the input-constraint set of the i-th open-loop optimization problem from $\bar{U}^i$ to $\bar{U}_f^i$ at the FD time k_d to establish the FI conditions on-line, which is the proposed active FI strategy.

During the second phase of the transition (i.e., the FI process), in addition to guarantee the satisfaction of the FI conditions, the feasibility, stability and constraint satisfaction of the

controller and system should also be considered. The optimization problem (34) is updated by directly using the nominal state from the nominal prediction model. The nominal states are generated by the nominal prediction model free from the effect of the real system. Thus, as long as the i-th open-loop optimization problem can be designed to be feasible, the feasibility feature of the optimization can be preserved during the whole FI process if the constraints X and U are not considered. Since the set of the nominal input vector of the i-th nominal system is adjusted for FI, the feasibility of the i-th optimization problem should be preserved by using a new pair of constraint sets.

Thus, during the FI process, except that the input constraint of (34) is switched from $\bar{U}^i$ to $\bar{U}_f^i$ to establish the FI conditions on-line, the state and terminal constraints are accordingly switched from $\bar{X}^i$ to $\bar{X}_f^i$ and $\bar{X}_T^i$ to $\bar{X}_{fT}^{\ i}$, respectively. The set $\bar{X}_f^i$ is the state constraint set of (34) for the FI process and $\bar{X}_{fT}^{\ i}$ is a *control invariant* (CI) set of the i-th nominal system corresponding to $\bar{u}_k^i \in \bar{U}_f^i$ and $\bar{x}_k^i \in \bar{X}_f^i$. The sets $\bar{U}_f^i$ and $\bar{X}_f^i$ are a pair of designing parameters used to guarantee FI and constraint satisfaction in this FTC scheme.

Remark 4.2 *Transient constraint satisfaction During the FI process, from the mode i to l, $\bar{U}_f^i \oplus K_i e_k^{l,i,i} \in U$ and $\bar{X}_f^i \oplus e_k^{l,i,i} \oplus \tilde{x}_k^{l,i,i} \in X$ should hold such that the hard input and state constraints are not violated, which is the precondition of the proposed FTC scheme and is used to ensure the availability of the tube-based MPC technique. The satisfaction of this condition can be affected by system dynamics, faults, $\bar{U}_f^i$ and $\bar{X}_f^i$. This means that a proper pair of $\bar{U}_f^i$ and $\bar{X}_f^i$ should be designed to guarantee the effectiveness of the proposed FI strategy.* □

Based on the explanation of Remark 4.2, in order to ensure the availability of the proposed FTC scheme, Assumption 4.4 is further made.

Assumption 4.4 *Transient constraint sets There exists a pair of $\bar{U}_f^i$ and $\bar{X}_f^i$ such that the constraints $u_k \in U$ and $x_k \in X$ are not violated during the whole FI phase.* □

Notice that the selection of the pair ($u_k \in U$ and $x_k \in X$) plays an important role in the proposed FTC scheme. Since the methodological procedure of selecting that pair is out of the scope of this paper, $\bar{U}_f^i$ and $\bar{X}_f^i$ have been selected by trial and error towards the suitable operation of the proposed approach. During the FI task, in addition to the constraint satisfaction, the feasibility and stability of the i-th open-loop optimization problem with a new pair of constraint sets should be guaranteed as well. Based on the optimization (34), to guarantee its feasibility, the nominal states generated from the nominal system internal model inside its terminal state constraints should always be confined in the MCI set. Thus, at the FD time k_d, when switching the constraints of the i-th open-loop optimization problem for active FI, the nominal state $\bar{x}_{k_d}^i$ should be considered for the sake of feasibility.

Proposition 4.1 *Transient-state feasibility During FI, if $\bar{x}_k^i \in \bar{X}_{fT}^{\ i}$ holds at time instant k,* (34) *will be always feasible at the next time instants.*

Proof : Since $\bar{X}_{fT}^{\ i}$ is a CI set of the i-th nominal system under the constraint sets $\bar{U}_f^i$ and $\bar{X}_f^i$ and the i-th optimisation problem is open-loop, $\bar{x}_k^i \in \bar{X}_{fT}^{\ i}$ implies the feasibility of the optimization problem at all the next time instants according to the definition of the CI sets. □

For the proposed FI strategy, the constraint sets of the i-th open-loop optimization should be adjusted for FI implementation at the FD time k_d. Thus, based on Proposition 4.1, the following strategy is proposed to guarantee the feasibility of the MPC controller during FI:

- if $\bar{x}_{k_d}^i \in \bar{X}_{fT}^{\ i}$, (34) is always feasible during the FI process according to Proposition 4.1.

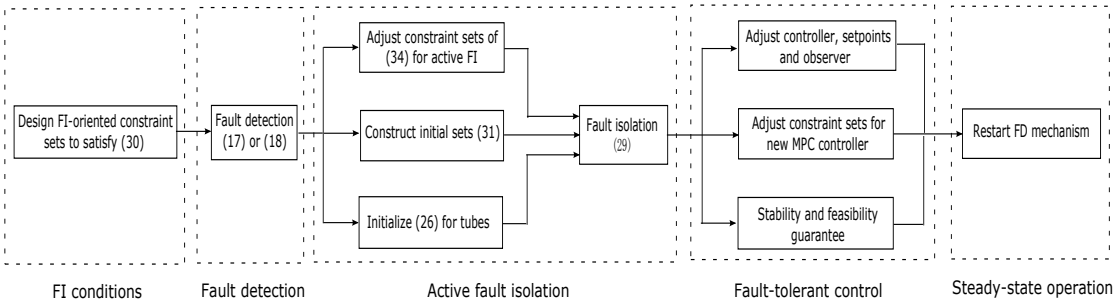


Figure 2: Flow chart of FTC

- if $\bar{x}^i_{k_d} \notin \bar{X_f}^i_T$, the centre of $\bar{X_f}^i_T$ is used to update (34) to guarantee feasibility at time instant k_d. For $k > k_d$, at one time instant $k*$, if $\bar{x}^i_{k^*} \in \bar{X_f}^i_T$, the feasibility of (34) can always be guaranteed for all $k > k^*$. Otherwise, the centre of $\bar{X_f}^i_T$ is still used to update (34) till the inclusion $\bar{x}^i_k \in \bar{X_f}^i_T$ is satisfied at one time instant $k > k_d$.

The aforementioned strategy to guarantee the feasibility is from a practical viewpoint. Moreover, since the set operation and representation are based on zonotopes, $\bar{X_f}^i_T$ should also be a zonotope and its center can always be obtained to update the open-loop optimization problem as a remedial measure.

During the second phase of the transition, the feasibility of both the open-loop optimization and constraint satisfaction problems can be guaranteed by using the aforementioned method. However, another important aspect of the proposed FTC scheme is the stability of the closed-loop scheme. Generally, to guarantee this feature, two points should be considered: the stability of the closed-loop dynamics, which can be guaranteed by Remark 3.3, and the feasibility and stability of the open-loop optimization problem (34), which can be guaranteed by using the terminal-state constraint and selecting suitable control parameters as shown in (34). Particularly, this paper follows the procedure presented in [12] in order to design a stabilizing tube-based MPC controller.

4.4 Transient-state Behaviors after FI

In the FTC scheme, when a fault is isolated at time instant k_i, at the same time the system should be reconfigured with a different tube-based MPC controller that corresponds to this new mode. After the controller adjusting, the FTC scheme will face the same feasibility problem as that during the second phase of the transition: it is assumed that the l-th actuator mode is isolated. Thus, the l-th tube-based MPC controller with the corresponding input and state constraints should be used, the l-th observer is used to obtain the state estimation and the l-th nominal system is used to generate the nominal states for the l-th open-loop optimization problem.

In order to guarantee the feasibility after system reconfiguration, two methods are proposed. The first one is similar with the second-phase transition, which uses the center of $\bar{X}^l_T$ to update the l-th open-loop optimization problem till at one time instant when

$$\bar{x}^l_k \in \bar{X}^l_T$$

holds. The second method is to use a state value $\bar{x}^l_{k_i} \in \bar{X}^l_T$ to initialize the l-th nominal system and open-loop optimization at the FI time instant k_i. With either of the two methods, according

to Proposition 4.1, the feasibility of the l-th open-loop optimization problem can always be preserved after reconfiguration. Additionally, the system can also keep stable during this phase.

During this third-phase transition, except for the feasibility, stability and constraint satisfaction, it still needs to guarantee the right restart of the FD mechanism. After system reconfiguration, the closed-loop system is operating in the l-th mode. Thus, the restarting of the FD mechanism should be considered to monitor the mode-switching behaviors in this new mode. However, since in the FTC scheme, the implementation of FD is based on invariant sets, if the FD mechanism is simultaneously restarted when the system is reconfigured, it is possible that the FD strategy creates false FD alarms. This situation will appear if the signals $\tilde{y}_k^{l,l,l}$ and $e_k^{l,l,l}$ do not enter into their respective sets $\tilde{Y}^{l,l,l}$ and $E^{l,l,l}$. This implies that for the sake of right restarting, it should be guaranteed that all signals $\tilde{y}_k^{l,l,l}$ and $e_k^{l,l,l}$ have already entered into their respective sets.

In this paper, there are also two methods to avoid the false FD alarms. The first one is to set a waiting time and as long as this waiting time is sufficiently long, after the waiting time, the signals can enter into their sets and the restarting of the FD mechanism can be done in the right way. The second one is that, after reconfiguration,

$$\tilde{y}_k^{l,l,l} \in \tilde{Y}^{l,l,l} \text{ and } e_k^{l,l,l} \in E^{l,l,l}$$

are tested until at a time instant both inclusions hold. Then, at this time instant, the FD mechanism is restarted in the new operating mode to avoid false FD alarms.

Remark 4.3 *Waiting time The waiting time can be arbitrarily defined as long as it can assure the right restarting of the FD mechanism such that the aforementioned false FD alarms can be avoided. However, it is better to define the waiting time with proper length based on the settling time of the system.* □

4.5 Fault-tolerant Control Procedure

In previous sections, the FDI and FTC approaches have been introduced in detail. In this subsection, the key point is to make a brief summary for the proposed FTC scheme, which is presented as follows:

- it is assumed that the system is at steady state of the i-th mode. The FD task consists in real-time testing whether (17) or (18) is violated or not. If no violation is detected, It is considered that the system is still in the i-th mode. Otherwise, it implies that a fault has occurred in the system.

- once a fault is detected at time instant k_d, the active FI approach will be started up to isolate the fault by adjusting the constraints of (34) from $\bar{X}^i$, $\bar{U}^i$ and $\bar{X}_T^i$ to $\bar{X}_f^i$, $\bar{U}_f^i$ and $\bar{X}_{fT}^{\ i}$, respectively, to satisfy the FI conditions on-line. Notice that the corresponding methods to guarantee the feasibility should be used during this phase.

- simultaneously, at $k = k_d$, p output-estimation-error tubes (26) are initialized by using initial sets constructed by (31). For each tube, (29) is tested in real time. Whenever a tube violates (29), the index of this tube is removed from the fault candidates until there is one and only one tube left, which implies that the fault is isolated and that the index of this only left tube indicates the fault.

- once the fault is isolated (it is assumed that the fault is indexed by l), the l-th observer, the l-th tube-based MPC controller and the l-th state-input pair are selected to reconfigure the

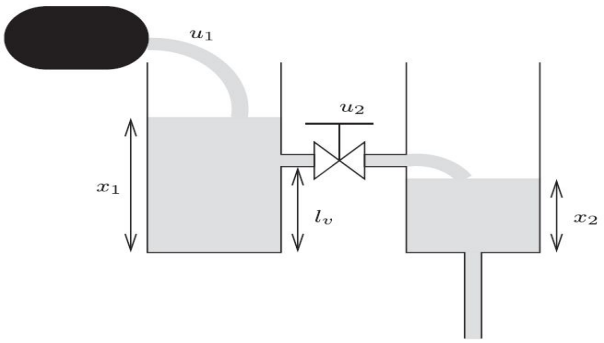


Figure 3: Two-tank system

system (now the constraint sets should be $\bar{X}_f^l$, $\bar{U}_f^l$ and $\bar{X}_{fT}^{\ l}$ for the new MPC controller, respectively). Notice that the corresponding methods to guarantee the feasibility of the l-th open-loop optimization and the right restarting of the FD mechanism should be used.

- after the system enters into the steady state of the l-th mode, the whole working procedure of the proposed scheme will be revisited to monitor this new mode and the control objective is to regulate the system around the corresponding setpoint.

To further help the readers understand the the approach proposed in this paper, a flow chart describing the FTC procedure is presented in Figure 2, where the whole procedure is divided into five steps: *FI conditions, fault detection, fctive fault isolation, Fault-tolerant control* and *steady-state operation.*

5 Illustrative Example

A two-tank system taken from [18], shown in Figure 3, is used as the example to illustrate the proposed FTC scheme. The mathematical model of this two-tank system can be found in [15]. With a sampling time of 0.01s, the dynamics of the system can be represented in discrete-time form as

$$x_{k+1} = A_d x_k + B_d F_i u_k + E_d \omega_k, \tag{37a}$$

$$y_k = C_d x_k + \eta_k, \tag{37b}$$

with

$$A_d = \begin{bmatrix} 0.975 & 0 \\ 0.025 & 0.975 \end{bmatrix}, \; C_d = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$
$$B_d = \begin{bmatrix} 0.1 & -0.05 \\ 0 & 0.05 \end{bmatrix}, \; E_d = \begin{bmatrix} 0.1 & 0 \\ 0 & 0.1 \end{bmatrix},$$

where F_i is used to model the actuator statuses (healthy or faulty), respectively, and it is further assumed that $|\omega| \leq \begin{bmatrix} 0.001 & 0.001 \end{bmatrix}^T$ and $|\eta| \leq \begin{bmatrix} 0.001 & 0.001 \end{bmatrix}^T$.

In this case study, faults in actuators are considered. In total, there are three actuator modes considered, i.e., F_0 (healthy mode), F_1 (a fault the first actuator) and F_2 (a fault the second actuator):

$$F_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \; F_1 = \begin{bmatrix} 0.5 & 0 \\ 0 & 1 \end{bmatrix}, \; F_2 = \begin{bmatrix} 1 & 0 \\ 0 & 0.5 \end{bmatrix}.$$

The water levels of the two tanks should vary within a range because of the phylical limitations. Moreover, actuators also have a limited range of operation. Thus, the system state and input constraints describing the limits of water levels and valves are set as

$$U = \left\{ u : \begin{bmatrix} -1 \\ -1 \end{bmatrix} \leq u \leq \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\},$$
$$X = \left\{ x : \begin{bmatrix} -1 \\ -1 \end{bmatrix} \leq x \leq \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}.$$

Based on (37), three observers with the form (8) are designed, each matching one actuator mode. Without loss of generality, the same poles are defined for the three observers for simplicity, i.e., $p = [0.2,\ 0.1]^T$. Thus, the three designed observer gains are

$$L_0 = L_1 = L_2 = \begin{bmatrix} 0.775 & 0 \\ 0.025 & 0.875 \end{bmatrix}.$$

Correspondingly, three tube-based MPC controllers corresponding to the three modes are designed to control the system, whose feedback gains are designed as

$$K_0 = \begin{bmatrix} -0.7913 & -0.3189 \\ 0.2199 & -0.4766 \end{bmatrix},$$
$$K_1 = \begin{bmatrix} -0.6727 & -0.3012 \\ 0.3532 & -0.4109 \end{bmatrix},$$
$$K_2 = \begin{bmatrix} -0.8097 & -0.3052 \\ 0.1161 & -0.3142 \end{bmatrix}.$$

In this example, the output setpoints for the three actuator modes are given as

$$y_0^* = y_1^* = y_2^* = \begin{bmatrix} 0.1 \\ 0.05 \end{bmatrix}.$$

Associated with these output setpoints, the state and input setpoint pairs are

$$x_0^* = \begin{bmatrix} 0.1 \\ 0.05 \end{bmatrix}, u_0^* = \begin{bmatrix} 0.0125 \\ -0.025 \end{bmatrix},$$
$$x_1^* = \begin{bmatrix} 0.1 \\ 0.05 \end{bmatrix},\ u_1^* = \begin{bmatrix} 0.025 \\ -0.025 \end{bmatrix},$$
$$x_2^* = \begin{bmatrix} 0.1 \\ 0.05 \end{bmatrix},\ u_2^* = \begin{bmatrix} 0.0125 \\ -0.05 \end{bmatrix}.$$

In this example, two fault scenarios are considered, each one corresponding to one actuator fault:

- Scenario 1: from time instants 1 to 75, the system is healthy and from 76 to 150, the first actuator fault occurs.
- Scenario 2: from time instants 1 to 75, the system is healthy and from 76 to 150, the second actuator fault occurs.

For these two scenarios, after the the fault occurrence, a pair of active FI input and state sets needs to be designed for the nominal MPC optimization problem of the healthy tube-based MPC controller, which are presented as

$$\bar{U}_f^0 = \left\{ u : \begin{bmatrix} 0.2 \\ 0.2 \end{bmatrix} \leq u \leq \begin{bmatrix} 0.4 \\ 0.4 \end{bmatrix} \right\},$$
$$\bar{X}_f^0 = \left\{ x : \begin{bmatrix} -0.973 \\ -0.9306 \end{bmatrix} \leq x \leq \begin{bmatrix} 0.973 \\ 0.9306 \end{bmatrix} \right\}.$$

Remark 5.1 *State-input sets for active FI The set pair $\bar{U}_f^0$ and $\bar{X}_f^0$ is not unique. If only the implementation of FI is considered, any set pair that satisfies the proposed FI conditions can be used for active FI.* □

Without loss of generality, only scenarios from heathy to faulty are considered to illustrate this FTC scheme. Thus, corresponding to $\bar{U}_f^0$, the after-fault sets of output-estimation errors of the two actuator-fault modes switched from the healthy mode can be constructed, which are shown in Figure 4. Figure 4 shows that the active FI set $\bar{U}_f^0$ can satisfy the guaranteed FI conditions in Proposition 3.2. This implies that, after detection of either of the two faults, it is guaranteed that the fault can be isolated by using the proposed FI approach.

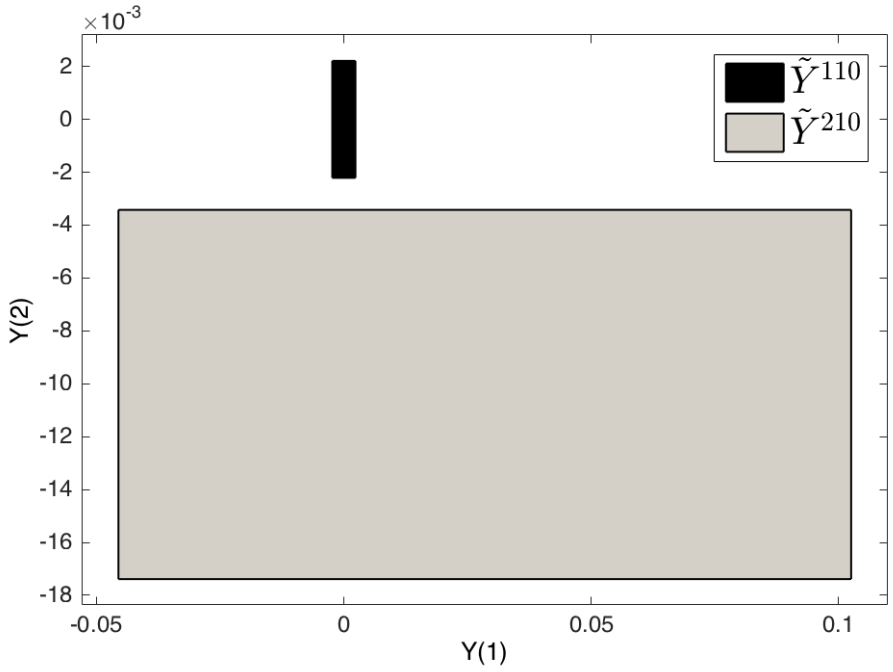
For comparison, Figure 5 shows the after-fault sets without active FI. In this case, the after-fault output-estimation-error sets from the healthy mode should be constructed by using the input set $\bar{U}^0$ that can be computed by (32) (see Figure 5). In Figure 5, the sets $\tilde{Y}^{110n}$ and $\tilde{Y}^{220n}$ are relatively small and shows that if the proposed active FI strategy is not used, it cannot be guaranteed to isolate the faults after FD.

Note that, in Figures 4 and 5, the sets $\tilde{Y}^{110}$, $\tilde{Y}^{210}$, $\tilde{Y}^{220}$, $\tilde{Y}^{110n}$, $\tilde{Y}^{210n}$ and $\tilde{Y}^{220n}$ are outer-bounding interval hulls of the corresponding invariant sets for simplicity of computation, which do not affect the checking of the proposed FI conditions.

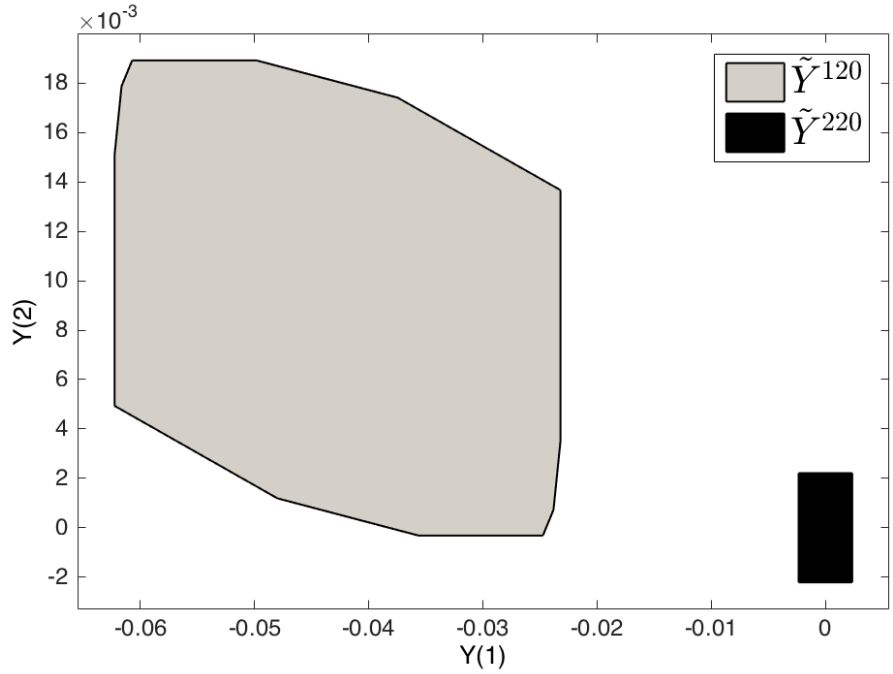
Remark 5.2 *Notations In the Figures 6, 7, 8, 9, 10 and 11, the notations $E^{000}(l)$, $e_k^{i00}(l)$, $\tilde{Y}^{000}(l)$, $\tilde{y}_k^{i00}(l)$, $\tilde{Y}_k^{111}(l)$, $\tilde{Y}_k^{222}(l)$, $\tilde{y}_k^{i10}(l)$, $\tilde{y}_k^{i20}(l)$ and $y(l)$, $u(l)$ denote the l-th components of $E^{0,0,0}$, $e_k^{i,0,0}$, $\tilde{Y}^{0,0,0}$, $\tilde{y}_k^{i,0,0}$, $\tilde{Y}_k^{1,1,1}$, $\tilde{Y}_k^{2,2,2}$, $\tilde{y}_k^{i,1,0}$, $\tilde{y}_k^{i,2,0}$, y and u, respectively. Since the output matrix is the identity matrix, the figure of system states is omitted here for simplicity.*

For the first fault scenario, the FD results are shown in Figure 6, where $\tilde{y}_{86}^{i00}(1) \notin \tilde{Y}^{000}(1)$ indicates that a fault is detected at this time instant. Thus, the proposed active FI process is activated at the time instant $k = 86$. Furthermore, it is obtained that $\tilde{y}_{87}^{i10} \in \tilde{Y}_{87}^{111}$ and $\tilde{y}_{87}^{i20} \notin \tilde{Y}_{87}^{222}$ hold, which implies that the fault in the first actuator has occurred. Then, the whole system is reconfigured to tolerate the fault. Accordingly, the inputs and outputs of Scenario 1 are presented in Figures 8, which show that the proposed FTC scheme can tolerate this fault with satisfactory performance. Moreover, all the constraints can be well satisfied during the whole process.

For the second scenario, the simulation results are shown in Figures 9, 10 and 11. In Figure 9, it is shown that an actuator fault is detected at time instant $k = 80$ because $\tilde{y}_{80}^{i00}(1) \notin \tilde{Y}^{000}(1)$ is detected. Thus, at the FD time $k = 80$, the active FI process is started as seen in Figure 10. Similarly, in Figure 10, $\tilde{y}_k^{i10}$ and $\tilde{y}_k^{i20}$ correspond to the first and second observers, respectively. It can be observed that $\tilde{y}_{81}^{i10} \notin \tilde{Y}_{81}^{111}$ and $\tilde{y}_{81}^{i20} \in \tilde{Y}_{81}^{222}$ hold, which implies that the second actuator fault is isolated at time instant $k = 81$. Once the second fault is isolated, the system is reconfigured by the corresponding MPC controller and state-input setpoint pair. The results in Figures 11 show that, although the output performance has a slight degradation, the AFTC strategy can generally obtain the satisfactory performance and the constraints are always well satisfied.

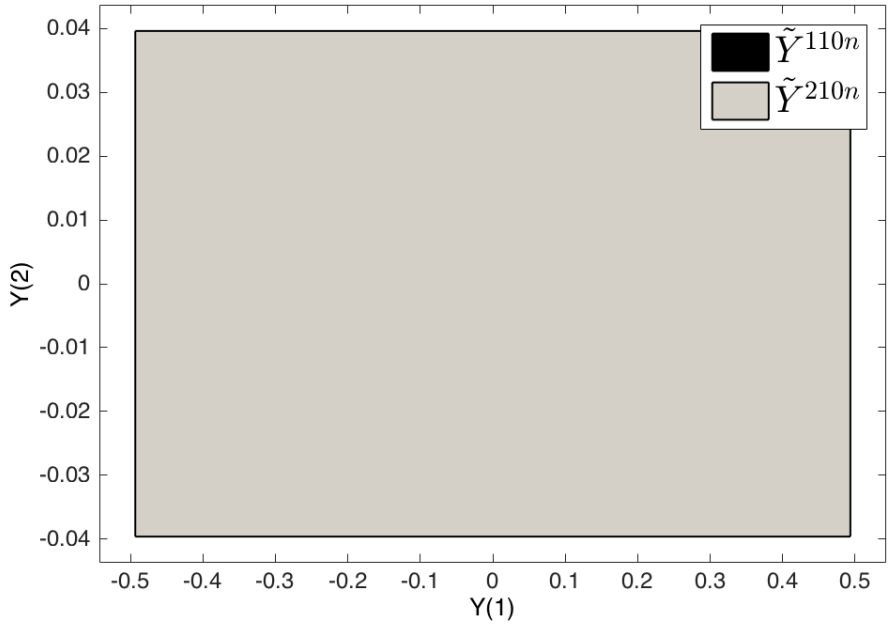


(a)

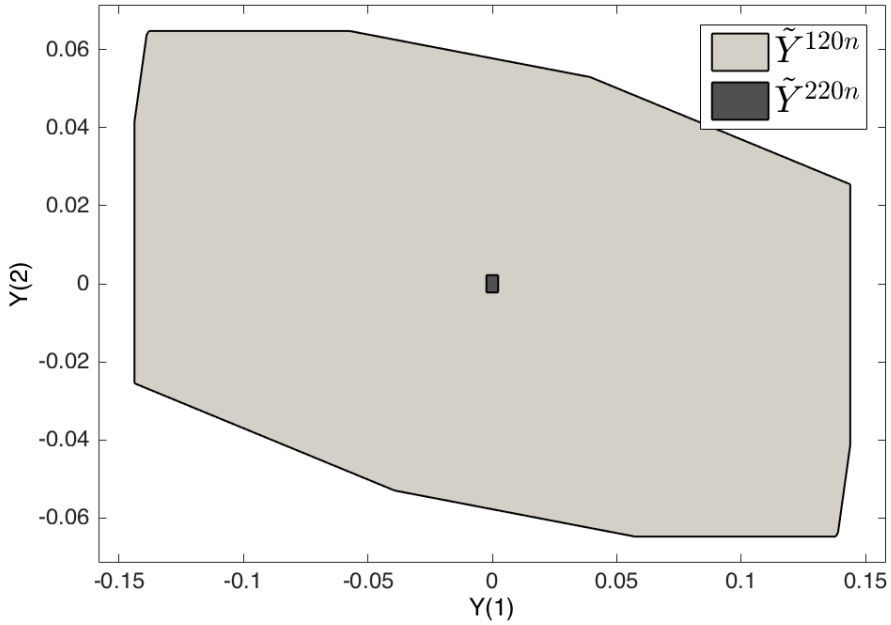


(b)

Figure 4: After-fault sets with active FI



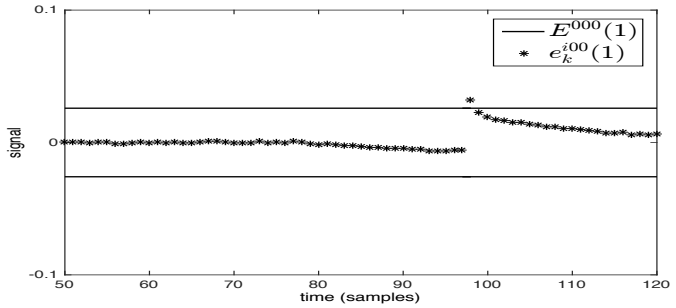
(a)



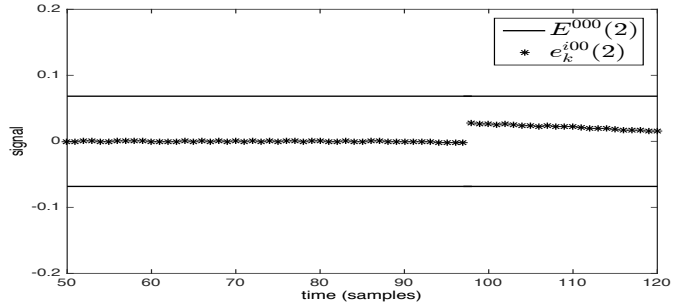
(b)

Figure 5: After-fault sets without active FI

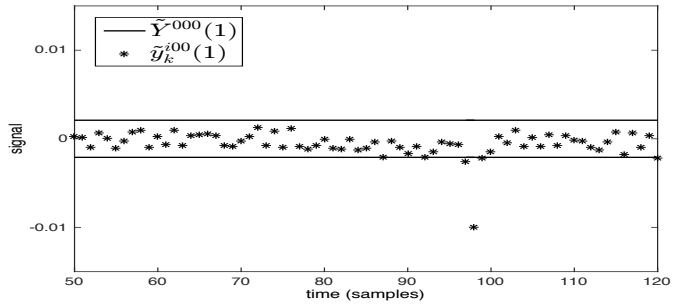
Remark 5.3 *Restarting of FD mechanism In order to avoid false fault alarms, whenever the system is reconfigured, a waiting time of* 20 *sampling times is set. During the waiting time, the FD mechanism is frozen till this period elapses. Then, the FD mechanism is restarted again to*



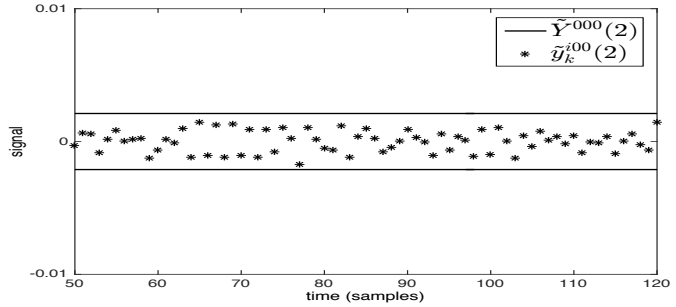
(a)



(b)

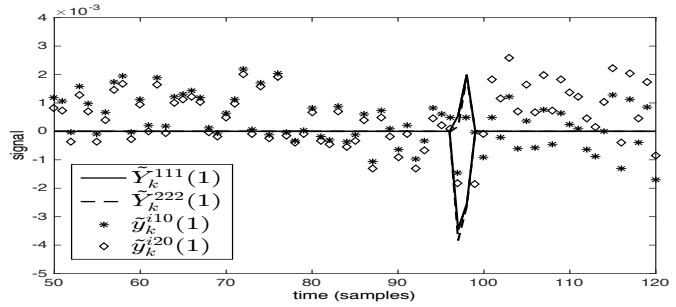


(c)

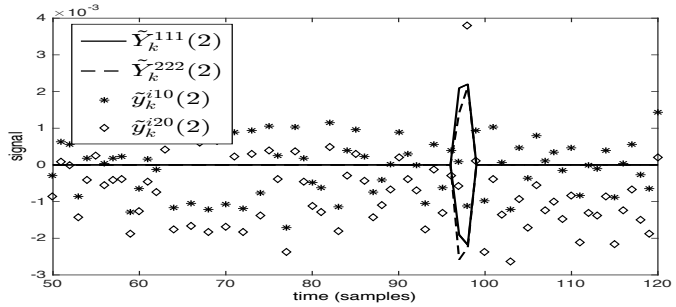


(d)

Figure 6: FD of fault 1

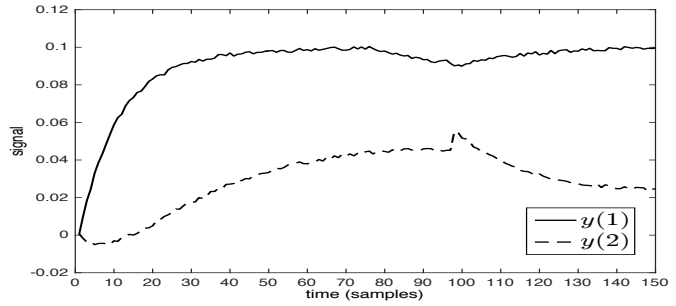


(a)

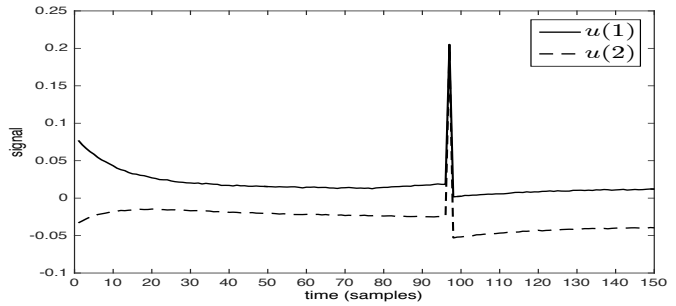


(b)

Figure 7: FI of fault 1

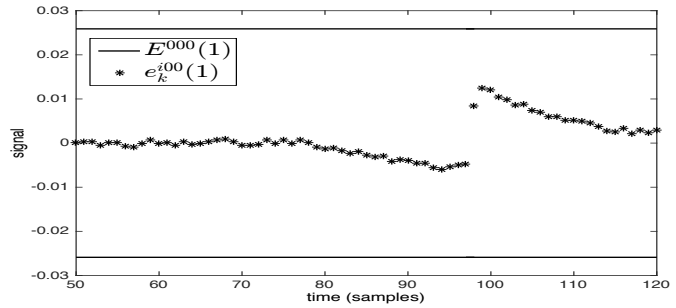


(a)

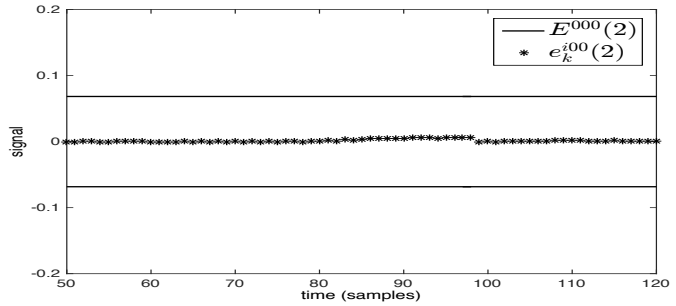


(b)

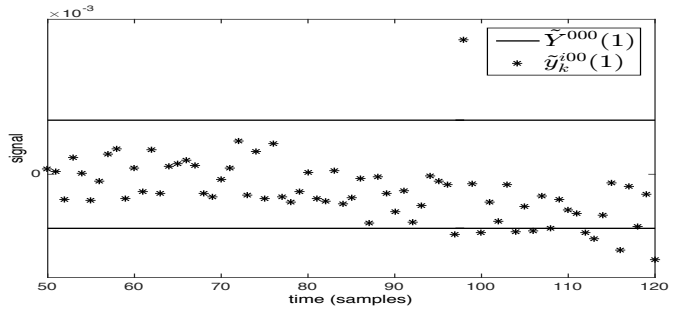
Figure 8: System outputs and inputs of scenario 1



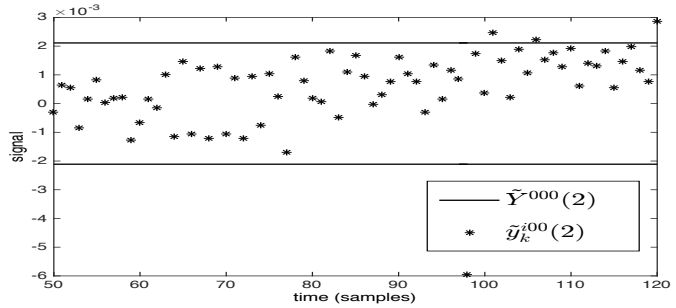
(a)



(b)

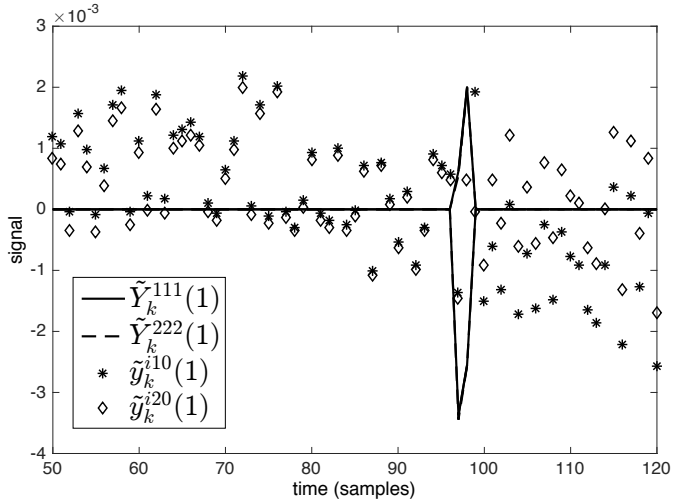


(c)

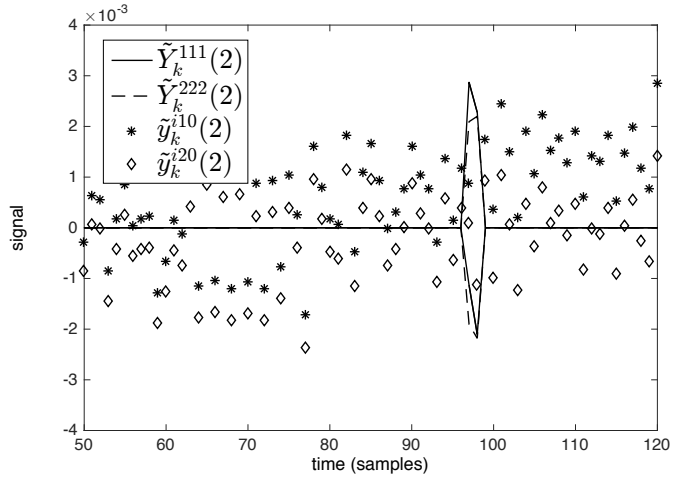


(d)

Figure 9: FD of fault 2



(a)



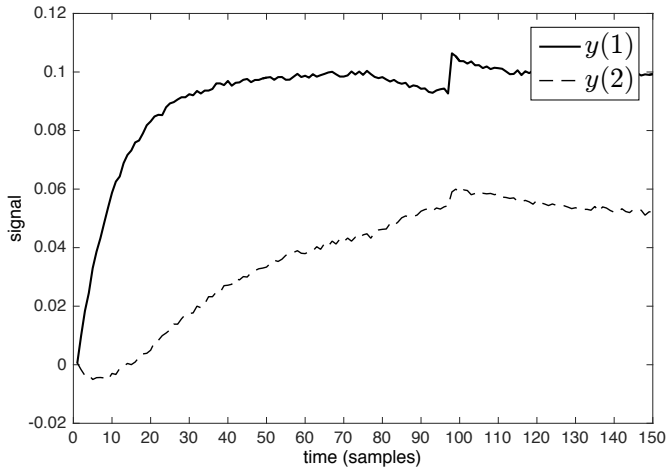
(b)

Figure 10: FI of fault 2

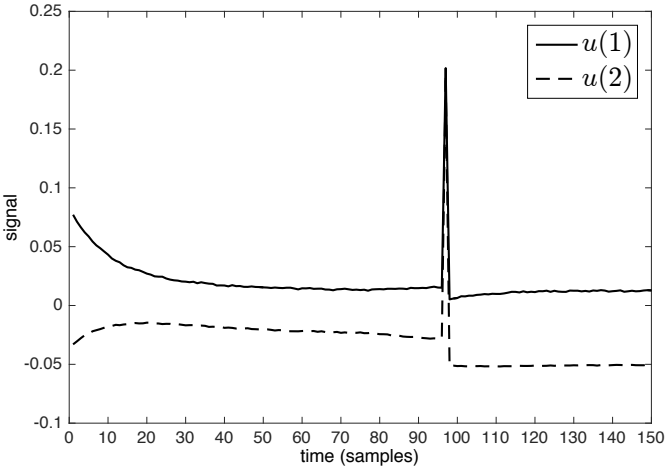
monitor a new mode.

6 Conclusions

In this paper, an actuator FTC scheme combining tube-based MPC and set-theoretic FDI are proposed. In the scheme, FD is passive by using invariant sets and FI is active by relying on MPC and tubes, which is the most important contribution of this paper. The use of tube-based MPC and set-theoretic FDI is interesting because their relatively low computational complexity, FDI robustness and their proper combination to implement the proposed active FI strategy. Thus, the proposed FTMPC scheme owns robust FDI performance, low computational complexity and less conservative FI conditions. The key of this FTC scheme consists in designing the input



(a)



(b)

Figure 11: System outputs and inputs of scenario 2

and state sets for active FI. In this paper, these sets are chosen by off-line trial and error as a pragmatic method, which can be improved if a systematic designing method can be proposed for the input and state FI sets in the future. It should be emphasized that the proposed FTC scheme cannot detect all faults. Thus, for undetectable faults, the PFTC ability of this scheme can still tolerate them to some extent despite a possible degree of performance degradation may appear. Due to tube-based MPC, the advantages of the proposed FTC scheme consist in its relatively simple structure and less conservative active FI. In the future, the authors will focus on designing state-input constraint sets to further improve this FTC scheme.

acknowledgment

This work was supported by the DGR of Generalitat de Catalunya [SAC group Ref.2014/SGR/0375], the Spanish projects ECOCIS (Ref.DPI2013-48243-C2-1-R) and HARCRICS (Ref.DPI2014-58104-R), China Scholarship Council (CSC), the Automatic Control Department of Supélec and CNRS-Supélec, France.

References

[1] T. Alamo, J.M. Bravo, and E.F. Camacho. Guaranteed state estimation by zonotopes. *Automatica*, 41(6):1035–1043, 2005.

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

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

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

[5] P.D. Hanlon and P.S. Maybeck. Multiple-model adaptive estimation using a residual correlation kalman filter bank. *Aerospace and Electronic Systems, IEEE Transactions on*, 36(2):393–406, Apr 2000.

[6] B. Jiang and F.N. Chowdhury. Fault estimation and accommodation for linear MIMO discrete-time systems. *IEEE Transactions on Control Systems Technology*, 13(3):493–499, 2005.

[7] B. Jiang, M. Staroswiecki, and V. Cocquempot. Fault accommodation for nonlinear dynamic systems. *IEEE Transactions on Automatic Control*, 51(9):1578–1583, 2006.

[8] E. Kofman, H. Haimovich, and M.M. Seron. A systematic method to obtain ultimate bounds for perturbed systems. *International Journal of Control*, 80(2):167–178, 2007.

[9] I. Kolmanovsky and E. Gilbert. Theory and computation of disturbance invariant sets for discrete-time linear systems. *Mathematical Problems in Engineering*, 4:317–367, 1998.

[10] V.T.H. Le, C.N. Stoica, T. Alamo, E.F. Camacho, and D. Dumur. Zonotope-based set-membership estimation for multi-output uncertain systems. In *Proceedings of 2013 IEEE international Symposium on Intelligent Control (ISIC), Part of 2013 IEEE Multi-Conference on Systems and Control*, Hyderabad, India, August 2013.

[11] J.M. Maciejowski. Fault-tolerant aspects of MPC. In *IEE Two-Day Workshop on Model Predictive Control: Techniques and Applications*, pages 1/1–1/4, London, The UK, 1999.

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

[13] C. Ocampo-Martinez, J.A. De Doná, and M.M Seron. Actuator fault-tolerant control based on set separation. *International Journal of Adaptive Control and Signal Processing*, 24(12):1070–1090, 2010.

[14] 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.

[15] E.N. Osella, H. Haimovich, and M.M Seron. Integration of invariant-set-based FDI with varying sampling rate virtual actuator and controller. *International Journal of Adaptive Control and Signal Processing*, 2015.

[16] D.M. Raimondo, G.R. Marseglia, R.D. Braatz, and J.K. Scott. Fault-tolerant model predictive control with active fault isolation. In *Proceedings of 2013 Conference on Control and Fault-Tolerant Systems (SysTol)*, pages 6567–6572, Nice, France, October 9-11 2013.

[17] Vasso Reppa, Sorin Olaru, and Marios M Polycarpou. Structural detectability analysis of a distributed sensor fault diagnosis scheme for a class of nonlinear systems. *9th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes (SAFEPROCESS 2015)*, 48(21):1485–1490, 2015.

[18] T. Steffen. *Control Reconfiguration of Dynamical Systems*. Springer, Germany, 2005.

[19] 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):512–523, 2008.

[20] D. Xu, B. Jiang, and P. Shi. Nonlinear actuator fault estimation observer: An inverse system approach via a T-S fuzzy model. *International Journal of Applied Mathematics and Computer Science*, 22(1):183–196, 2012.

[21] F. Xu, V. Puig, C. Ocampo-Martinez, S. Olaru, and S. Nicolescu. Robust MPC for actuator-fault tolerance using set-based passive fault detection and active fault isolation. In *Proceedings of the IEEE Conference on Decision and Control*, Los Angeles, USA, Decembre 2014.

[22] X. Yang and J. M. Maciejowski. Fault tolerant control using gaussian processes and model predictive control. *International Journal of Applied Mathematics and Computer Science*, 25(1):133–148, 2015.

[23] A. Yetendje, M. M. Seron, and J. A. De Doná. Robust MPC multicontroller design for actuator fault tolerance of constrained systems. In *Proceedings of the 18th IFAC World Congress*, Milano, Italy, August 28-September 2 2011.

[24] A. Yetendje, M. M. Seron, and J. A. De Doná. Robust multisensor fault tolerant model-following mpc design for constrained systems. *International Journal of Applied Mathematics and Computer Science*, 22(1):211–223, 2012.

Definition .1 *Zonotopes An r-order zonotope Z is defined as $Z = g \oplus H\mathbb{B}^r$, where g and H are its center and segment matrix (or generator matrix), respectively.*

Definition .2 *Interval hull The interval hull $\square Z$ of a zonotope $Z = g \oplus H\mathbb{B}^r \subset \mathbb{R}^n$ is the smallest box containing Z, i.e.,*

$$\square Z = \{x : |x_i - g_i| \leq \| H_i \|_1\},$$

where H_i is the i-th row of H, x_i and g_i are the i-th components of x and g, respectively.

Property .1 *Minkowski sum of zonotopes Given two zonotopes $Z_1 = g_1 \oplus H_1\mathbb{B}^{r_1} \subset \mathbb{R}^n$ and $Z_2 = g_2 \oplus H_2\mathbb{B}^{r_2} \subset \mathbb{R}^n$, $Z_1 \oplus Z_2 = (g_1 + g_2) \oplus [H_1 \quad H_2]\mathbb{B}^{r_1+r_2}$.*

Property .2 *Multiplication of zonotopes Given a zonotope $Z = g \oplus H\mathbb{B}^r \subset \mathbb{R}^n$ and a suitable matrix K, $KZ = Kg \oplus KH\mathbb{B}^r$.*

Property .3 *Reordering of zonotopes Given a zonotope $Z = g \oplus H\mathbb{B}^r \subset \mathbb{R}^n$ and an integer s (with $n < s < r$), denote by $\hat{H}$ the matrix resulting from the reordering of the columns of the matrix H in decreasing Euclidean norm. $Z \subseteq g \oplus [\hat{H}_T \quad Q]\mathbb{B}^s$ where $\hat{H}_T$ is obtained from the first $s-n$ columns of the matrix $\hat{H}$ and $Q \in \mathbb{R}^{n\times n}$ is a diagonal matrix whose elements satisfy $Q_{ii} = \sum_{j=s-n+1}^{r} \mid \hat{H}_{ij} \mid$, $i = 1, \ldots, n$.*

Property .4 *Intersection of a zonotope and a strip Given a zonotope $Z = g \oplus H\mathbb{B}^r \subset \mathbb{R}^n$, a strip $S = \{x \in \mathbb{R}^n \mid |cx - d| \leq \sigma\}$ and a vector $\lambda \in \mathbb{R}^n$, then $Z \cap S \subseteq \hat{Z}(\lambda) = \hat{g}(\lambda) \oplus \hat{H}(\lambda)\mathbb{B}^{r+1}$ holds, where $\hat{g}(\lambda) = g + \lambda(d - cg)$ and $\hat{H}(\lambda) = [(I - \lambda c)H \quad \sigma\lambda]$.*

Property .5 *Intersection of a zonotope and a polytope Given a matrix $\Lambda \in \mathbb{R}^{n\times m}$, a zonotope $Z = g \oplus H\mathbb{B}^r$, and an H-polytope $P = \{x \in \mathbb{R}^n : |Cx - d| \leq [\phi_1, \phi_2, ..., \phi_m]^T\}$, with $C \in \mathbb{R}^{m\times n}$, $d \in \mathbb{R}^m$, $\phi_i \in \mathbb{R}_+$ $(i = 1, 2, ..., m)$, define a vector $\hat{g}(\Lambda) = g + \Lambda(d - Cg)$ and a matrix $\hat{H}(\Lambda) = [(I - \Lambda C)H \quad \Lambda\Phi]$, with a diagonal matrix $\Phi = diag(\phi_1, \phi_2, ..., \phi_m)$. Then a family of zonotopes (parameterized by the matrix Λ) that contains the intersection of the zonotope Z and the polytope P is obtained as $Z \cap P \subseteq \hat{Z}(\Lambda) = \hat{g} \oplus \hat{H}\mathbb{B}^{r+m}$.*

Definition .3 *RPI set A set $\mathcal{X}$ is an RPI set of the dynamics $x_{k+1} = Ax_k + \omega_k$ if for $x_k \in \mathcal{X}$ and $\omega_k \in W$, $x_{k+1} \in A\mathcal{X} + W \subseteq \lambda\mathcal{X}$ $(0 < \lambda \leq 1)$ always holds.*

Definition .4 *Minimal RPI set The minimal RPI (mRPI) set of the dynamics $x_{k+1} = Ax_k + \omega_k$ is defined as an RPI set contained in any closed RPI set and the mRPI set is unique and compact.*

Theorem .1 *Construction of invariant sets Considering the dynamics $x_{k+1} = Ax_k + B\delta_k$ where A and B are constant matrices and A is a Schur matrix, δ_k belongs to $\Delta = \{\delta : |\delta - \delta^\circ| \leq \bar{\delta}\}$ with δ° and $\bar{\delta}$ constant, and letting $A = V\Lambda V^{-1}$ be the Jordan decomposition, the set*

$$\begin{aligned}\Phi(\theta) =& \{x \in \mathbb{R}^n : \left|V^{-1}x\right| \leq (I - |\Lambda|)^{-1}\left|V^{-1}B\right|\bar{\delta} + \theta\} \\ & \oplus \xi^\circ,\end{aligned} \tag{38}$$

is RPI and attractive for the state trajectories, with θ any (arbitrarily small) vector with positive components, where $\xi^\circ = (I - A)^{-1}B\delta^\circ$:

1. *For any θ, the set $\Phi(\theta)$ is (positively) invariant, that is, if $x_0 \in \Phi(\theta)$, then $x_k \in \Phi(\theta)$ for all $k \geq 0$.*
2. *Given $\theta \in \mathbb{R}^n, \theta > 0$, and $x_0 \in \mathbb{R}^n$, there exists $k^* \geq 0$ such that $x_k \in \Phi(\theta)$ for all $k \geq k^*$.*

Definition .5 *CI set A set $\mathcal{X} \subseteq X$ is a CI set of the dynamics $x_{k+1} = Ax_k + Bu_k$ if for any $x_k \in \mathcal{X}$, there always exists $u_k \in U$ such that $x_{k+1} \in \mathcal{X}$ for all $k \geq 0$.*

Definition .6 *MCI set A set $\mathcal{X}_\mathcal{M} \subseteq X$ is said to be the MCI set of the dynamics $x_{k+1} = Ax_k + Bu_k$, if it is CI and contains all CI sets inside X.*