Active Fault Detection and Isolation in a Zonotopic Framework

Daniel Ioan, Florin Stoican, Karl Worthmann

Active Fault Detection and Isolation in a Zonotopic Framework

Daniel-Mihail Ioan[1], Florin Stoican
Department of Automatic Control
and Systems Engineering, UPB, Romania
Email: {daniel.ioan@aut, florin.stoican@acse}.pub.ro

Karl Worthmann
Dept. of Ordinary Differential Equations,
TU Ilmenau, Germany
Email: karl.worthmann@tu-ilmenau.de

***Abstract*—We consider a plant affected by multiple faults (modeled through a piecewise affine formalism). Using a bank of finite-window observers and an artificially-induced feedback delay we provide an exact fault detection and isolation (FDI) mechanism, integrated into the overall fault tolerant control scheme. We use zonotopic characterizations for the sets of interest in order to provide explicit conditions for FDI exactness (such that a fault occurrence can be signaled unambiguously) and to alleviate the numerical issues specific to set operations.**

***Keywords*—active FDI, switching dynamics, zonotopes**

I. INTRODUCTION

Fault tolerant control (FTC) is one of today's main topics of interest in the control community [1]. The recent proliferation of large-scale, complex systems has raised the chances of fault occurrences (either at actuator, sensor or plant dynamics level). Thus, a reliable FTC scheme with an exact fault detection and isolation (FDI) together with a robust reconfiguration mechanism is becoming essential.

In what follows, we consider a set-based approach [2], [3]. Having bounding sets for noises, disturbances and model variations it is possible to bound the signals of interest and thus, to characterize explicitly separation conditions which ensure FDI. To this end we use the set-theoretic notions of robust positive invariance and reachability. The former allows offline computations and gives a priori stability guarantees while the later allows to handle the transitional behavior sparked by fault(s) occurrences [4]. There are several issues in the literature which are not usually tackled:

i) The FDI separation condition may not be verified for the current operation conditions.
ii) The FDI mechanism may need a non-zero observation window to asses a fault occurrence. This means that the closed-loop scheme may use faulty information.
iii) The computation of invariant / reachable sets is cumbersome for large dimensions and/or for long intervals [5].

For issue i) the key is to observe that the sets involved are parametrized after variables influenced by the control scheme [6]. Therefore, choosing them such that the condition is always respected avoids the issue of false alarms or missed faults.

To simplify the set computations and help with issue ii) we induce a delay in the feedback generation. Assuming fault persistence and given reference dynamics, 'steady' and transitional sets which bound the tracking error and estimation error dynamics are computed. Residual sets (coming from the output estimation sets) are used to check the FDI condition. Since these sets are parametrized after the reference state and input, we use these variables to guarantee exact FDI.

Lastly, to handle issue iii), we consider zonotopic sets. A sub-class of the polyhedral sets, they are increasingly used due to their resilience to the "dimensionality curse' [7], e.g, for reachability analysis [8], collision detection [9] or guaranteed state estimation [9]. In contrast to polytopes, the operations with zonotopic sets are significantly less computationally demanding, and, also, do not raise numerical instabilities [10], [11]. Toolboxes like CORA [11] handle zonotopic sets representations and operations efficiently.

Combining all these elements we reach an explicit formulation which ensures FDI and involves reference inputs and states. Due to the nonlinear nature of the problem (a bilevel formulation), we consider the mixed integer formalism proposed in [12] but, instead of directly controlling the inputs applied to the control scheme, we control the reference inputs and assume the feedback law already given.

Notation: The Minkowski sum of two sets, A and B is denoted as $A \oplus B = \{x : \; x = a + b, \; a \in A, b \in B\}$. $\mathrm{conv}(S)$ denotes the convex hull of set S.

II. PRELIMINARIES

In the rest of the paper sets will be used to bound various signals with the end goal of detecting and isolating unambiguously a fault occurrence. This implies the use of (robust) invariance, set projection, set addition and all the other tools used in set-theoretic methods.

While there are multiple choices for representing a system (e.g., via polyhedral or ellipsoidal sets [5]), in this paper we consider zonotopes as they provide an excellent compromise between numerical complexity and fidelity of representation:

Definition 1 ([13]): A zonotope is a centrally symmetric polytope, which can be described as a Minkowski sum of line segments. In its *generator representation* a zonotope Z is described by *center* $\mathbf{c} \in \mathbb{R}^n$ and *generators* $\mathbf{g}_1, \ldots, \mathbf{g}_{n_g} \in \mathbb{R}^n$:

$$Z = \{\mathbf{c} + \sum_{i=1}^{n_g} \xi_i \mathbf{g}_i : \|\xi\|_\infty \leq 1\} \tag{1}$$

[1]D. Ioan is currently with the Laboratory of Signals and Systems, Univ. Paris-Sud -CentraleSupelec-CNRS, Université Paris Saclay.

or, compactly with $\mathbf{G} = [\mathbf{g}_1, \dots, \mathbf{g}_{n_g}]$, as

$$Z = \{\mathbf{G}\xi + \mathbf{c} | \xi \in \mathbb{R}^{n_g}, \|\xi\|_\infty \leq 1\} \tag{2}$$

In the next sections, we use notation $\mathscr{Z}(\mathbf{G}, \mathbf{c})$ to denote (1).

Let us consider two zonotopes: $Z_1 = \mathscr{Z}(\mathbf{G}_1, \mathbf{c}_1) \subset \mathbb{R}^n$, $Z_1 = \mathscr{Z}(\mathbf{G}_2, \mathbf{c}_2) \subset \mathbb{R}^n$ and a matrix $\mathbf{R} \in \mathbb{R}^{m \times n}$. Then the following propeties hold [14]:

i) is closed under linear transformation:

$$\mathbf{R}\mathscr{Z}(\mathbf{G}_1, \mathbf{c}_1) = \mathscr{Z}(\mathbf{R}\mathbf{G}_1, \mathbf{R}\mathbf{c}_1); \tag{3}$$

ii) is closed under Minkowski sum:

$$\mathscr{Z}(\mathbf{G}_1, \mathbf{c}_1) \oplus \mathscr{Z}(\mathbf{G}_2, \mathbf{c}_2) = \mathscr{Z}(\begin{bmatrix}\mathbf{G}_1 & \mathbf{G}_2\end{bmatrix}, \mathbf{c}_1 + \mathbf{c}_2); \tag{4}$$

iii) is symmetric, up to its center:

$$-Z_1 = -\mathscr{Z}\{\mathbf{G}_1, \mathbf{c}_1\} = \mathscr{Z}\{\mathbf{G}_1, -\mathbf{c}_1\}. \tag{5}$$

In particular, the Minkowski addition and projection operations greatly simplify for zonotopic sets with respect to their polyhedral counterparts and make large-scale computations feasible and numerically robust [8].

For further use, we define the notion of *robust positive invariance (RPI)*.

Definition 2: For LTI dynamics $x_{k+1} = Ax_k + \delta_k$ with $\delta_k \in \Delta$, the set Ω is called RPI iff the set inclusion

$$A\Omega \oplus \Delta \subseteq \lambda\Omega, \tag{6}$$

holds for $0 < \lambda \leq 1$.

When $0 < \lambda < 1$ we call Ω contractive and convergence inside it in a finite time is guaranteed. ♦

It is well-known [15] that the minimal RPI (mRPI) set Ω_∞ can be obtained through the set recurrence:

$$\Omega_0 = \{0\},\ \Omega_{k+1} = A\Omega_k \oplus \Delta. \tag{7}$$

In general, the limit set of (7) cannot be obtained explicitly. Instead, various methods exist for computing arbitrarily close approximations [16]. The repeated additions in (7) are manageable for zonotopic sets. In fact, due to (3) and (4), and assuming that $\Delta = \mathscr{Z}(G, c)$ we have that

$$\Omega_k = \mathscr{Z}(\begin{bmatrix}\mathbf{G} & \dots & A^{k-1}\mathbf{G}\end{bmatrix}, \mathbf{c} + \dots A^{k-1}\mathbf{c}) \tag{8}$$

Using (8) for $k \mapsto k+1$ and introducing it in (6) we have that, for a desired λ, the minimal value of k for which (6) holds is

$$k^* = \arg\min_k A^k \mathscr{Z}(\mathbf{G}, \mathbf{c}) \subseteq \lambda \mathscr{Z}(\mathbf{G}, \mathbf{c}). \tag{9}$$

III. PROBLEM DESCRIPTION

Let us consider the dynamics

$$\mathbf{x}_{k+1} = \mathbf{A}(i_k)\mathbf{x}_k + \mathbf{B}(i_k)\mathbf{u}_k + \mathbf{r}(i_k) + \mathbf{B}_w(i_k)\mathbf{w}_k \tag{10a}$$
$$\mathbf{y}_k = \mathbf{C}(i_k)\mathbf{x}_k + \mathbf{s}(i_k) + \mathbf{D}_v(i_k)\mathbf{v}_k \tag{10b}$$

where $\mathbf{x}_k, \mathbf{x}_{k+1} \in \mathbb{R}^n$ denote the current and successor states, $\mathbf{u}_k \in \mathbb{R}^m$ the input, $\mathbf{y}_k \in \mathbb{R}^p$ the output, $\mathbf{w}_k \in \mathbf{W} \subset \mathbb{R}^{m_w}$ the process noise and $\mathbf{v}_k \in \mathbf{V} \subset \mathbb{R}^{m_v}$ the measurement noise. Matrices $\mathbf{A}$, $\mathbf{B}$, $\mathbf{B}_w$, $\mathbf{C}$, $\mathbf{D}_v$ and bias terms $\mathbf{r} \in \mathbb{R}^n$, $\mathbf{s} \in \mathbb{R}^p$ are of appropriate dimension and take values from pre-defined collections of cardinality N, as indexed by i_k (e.g., $\mathbf{A}(i_k)$ takes values from $\{\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_N\}$).

Formulation (10) is both general enough to handle realistic dynamics (subject to model variation, noises, faults, etc.) and restrictive enough to provide, coupled with the tools from Section II, numerically manageable constructions. In particular, we use (10) to model dynamics which alternate between a healthy mode (by convention, $i_k = 0$) and various pre-defined[1] faulty modes ($i_k \neq 0$). What remains to be assessed is the fault occurrence (via a FDI mechanism).

A. State estimation

Let us assume a bank of observers, one per mode of functioning. That is, we define the j-th observer as a finite-window Luenberger observer whose internal model is given by the the j-th mode of dynamics (10):

$$\hat{\mathbf{x}}^j_{k-\tau+1} = \bar{\mathbf{x}}_{k-\tau+1} \tag{11a}$$
$$\hat{\mathbf{x}}^j_{\ell+1} = \mathbf{A}(j)\hat{\mathbf{x}}^j_\ell + \mathbf{B}(j)\mathbf{u}_\ell + \mathbf{r}(j) + \mathbf{L^j}(\mathbf{y}_\ell - \hat{\mathbf{y}}^j_\ell) \tag{11b}$$
$$\hat{\mathbf{y}}^j_\ell = \mathbf{C}(j)\hat{\mathbf{x}}^j_\ell + \mathbf{s}(j), \tag{11c}$$

for $\ell = k - \tau + 1, \dots, k$ and $\bar{\mathbf{x}}_{k-\tau+1}$, the state reference at time instant $k - \tau + 1$, to be defined later.

Dynamics (11) can be interpreted as follows: at the current moment 'k', all the available information of the last τ instants of time ($\mathbf{u}_{k-\tau+1}, \dots, \mathbf{u}_k, \mathbf{y}_{k-\tau+1}, \dots, \mathbf{y}_k$), together with initialization $\hat{\mathbf{x}}^j_{k-\tau+1} = \bar{\mathbf{x}}_{k-\tau+1}$ provide a state estimation $\hat{\mathbf{x}}^j_k$ and output estimation $\hat{\mathbf{y}}^j_k$. While arguably this construction discards some information (i.e., older information from the estimation), it will prove to be useful for the FDI mechanism.

Combining (10) and (11) we get the state and output estimation error, $\tilde{\mathbf{x}}^j_k \triangleq \mathbf{x}_k - \hat{\mathbf{x}}^j_k$ and $\tilde{\mathbf{y}}^j_k \triangleq \mathbf{y}_k - \hat{\mathbf{y}}^j_k$, respectively, associated to the j-th observer:

$$\tilde{\mathbf{x}}^j_{k-\tau+1} = \mathbf{z}_{k-\tau+1} \tag{12a}$$
$$\begin{aligned}\tilde{\mathbf{x}}^j_{\ell+1} = &\left[\mathbf{A}(j) - \mathbf{L}^j\mathbf{C}(j)\right]\tilde{\mathbf{x}}^j_\ell \\ &+ \left[(\mathbf{A}(i_\ell) - \mathbf{A}(j)) - \mathbf{L}^j\left(\mathbf{C}(i_\ell) - \mathbf{C}(j)\right)\right]\mathbf{x}_\ell \\ &+ \left[\mathbf{B}(i_\ell) - \mathbf{B}(j)\right]\mathbf{u}_\ell + \mathbf{r}(i_\ell) - \mathbf{r}(j) + \mathbf{B}_w(i_\ell)\mathbf{w}_\ell \\ &- \mathbf{L}^j\left[\mathbf{s}(i_\ell) - \mathbf{s}(j)\right] - \mathbf{L}^j\mathbf{D}_v(i_\ell)\mathbf{v}_\ell,\end{aligned} \tag{12b}$$
$$\tilde{\mathbf{y}}^j_\ell = \mathbf{C}(j)\tilde{\mathbf{x}}^j_\ell + \left[\mathbf{C}(i_\ell) - \mathbf{C}(j)\right]\mathbf{x}_\ell + \mathbf{s}(i_\ell) - \mathbf{s}(j) + \mathbf{D}_v\mathbf{v}_\ell, \tag{12c}$$

for $\ell = k - \tau + 1, \dots, k$ and $\mathbf{z}_{k-\tau+1}$, the tracking error at time instant $k - \tau + 1$, to be defined later.

Matrix $\mathbf{L}^j$ is taken such that the closed-loop state-matrix $\mathbf{A}_{L^j} = \mathbf{A}(j) - \mathbf{L}^j\mathbf{C}(j)$ is stable (always possible if the pair $(\mathbf{A}(j), \mathbf{C}(j))$ is observable).

Note that when the model used in the observer and the active dynamics coincide (i.e., $i_k = j$), (12) reduces to:

$$\tilde{\mathbf{x}}^j_{k-\tau+1} = \mathbf{z}_{k-\tau+1} \tag{13a}$$
$$\tilde{\mathbf{x}}^j_{\ell+1} = \mathbf{A}_{L^j}\tilde{\mathbf{x}}^j_\ell + \mathbf{B}_w(j)\mathbf{w}_\ell - \mathbf{L}^j\mathbf{D}_v(j)\mathbf{v}_\ell, \tag{13b}$$
$$\tilde{\mathbf{y}}^j_\ell = \mathbf{C}(j)\tilde{\mathbf{x}}^j_\ell + \mathbf{D}_v(j)\mathbf{v}_\ell. \tag{13c}$$

[1]Note that we assume both the fault models and their magnitudes known.

for $\ell = k-\tau+1,\ldots,k$ and $\mathbf{z}_{k-\tau+1}$, the tracking error at time instant $k-\tau+1$, to be defined later.

B. Tracking error

Let us assume the reference dynamics (with $\bar{\mathbf{u}}_k^j$ persistent references a priori given):

$$\bar{\mathbf{x}}_{k+1}^j = \mathbf{A}(j)\bar{\mathbf{x}}_k^j + \mathbf{B}(j)\bar{\mathbf{u}}_k^j + \mathbf{r}(j), \tag{14a}$$
$$\bar{\mathbf{y}}_k^j = \mathbf{C}(j)\bar{\mathbf{x}}_k^j + \mathbf{s}(j). \tag{14b}$$

Remark 1: The reference models (14) are in fact the nominal models (with noises $\mathbf{w}_k$ and $\mathbf{v}_k$ discarded) from (10). ♦
To close the loop we take

$$\mathbf{u}_k = \bar{\mathbf{u}}_k^{i'_k} + \mathbf{K}^{i'_k}(\hat{\mathbf{x}}_{k-\tau+1}^{i'_k} - \bar{\mathbf{x}}_{k-\tau+1}^{i'_k}) \tag{15}$$

where the selection of feedback matrix, state estimation and reference values $(\mathbf{K}^{i'_k}, \hat{\mathbf{x}}_{k-\tau+1}^{i'_k}, \bar{\mathbf{u}}_k^{i'_k}, \bar{\mathbf{x}}_k^{i'_k})$ will be done by the fault tolerant scheme described in Section IV-B. Note that the use of an artificially delayed information (the state estimation $\hat{\mathbf{x}}_{k-\tau+1}^{i'_k}$) is required by the FDI construction).

A typical measure of performance and stability is the analysis and bounding of the state and output tracking errors $\mathbf{z}_k^j \triangleq \mathbf{x}_k - \bar{\mathbf{x}}_k^j$ and $\boldsymbol{\xi}_k^j \triangleq \mathbf{y}_k - \bar{\mathbf{y}}_k^j$ respectively. Gathering (10), (14) and (15) we have:

$$\begin{aligned}\mathbf{z}_{k+1} = {} & \mathbf{A}(i_k)\mathbf{z}_k + \mathbf{B}(i_k)\mathbf{K}^{i'_k}\mathbf{z}_{k-\tau+1} + [\mathbf{r}(i_k) - \mathbf{r}(i'_k)] \\ & + [\mathbf{A}(i_k) - \mathbf{A}(i'_k)]\,\bar{\mathbf{x}}_k^{i'_k} + [\mathbf{B}(i_k) - \mathbf{B}(i'_k)]\,\bar{\mathbf{u}}_k^{i'_k} \\ & - \mathbf{B}(i_k)\mathbf{K}^{i'_k}\tilde{\mathbf{x}}_{k-\tau+1}^{i'_k} + \mathbf{B}_w(i_k)w_k \end{aligned} \tag{16a}$$
$$\begin{aligned}\boldsymbol{\xi}_k = {} & \mathbf{C}(i_k)z_k + [\mathbf{C}(i_k) - \mathbf{C}(i'_k)]\,\bar{\mathbf{x}}_k^{i'_k} \\ & + \mathbf{D}_v(i_k)\mathbf{v}_k + [\mathbf{s}(i_k) - \mathbf{s}(i'_k)]\,. \end{aligned} \tag{16b}$$

Matrices $\mathbf{K}^{i'_k}$ are taken such that the closed-loop dynamics are stable [17]. Assuming that the active dynamics (10) and the selected gain and state estimation coincide (i.e., $i_k = i'_k = j$), the tracking error dynamics (16) become

$$\begin{aligned}\mathbf{z}_{k+1} = {} & \mathbf{A}(j)z_k + \mathbf{B}(j)\mathbf{K}^j\mathbf{z}_{k-\tau+1} \\ & - \mathbf{B}(j)\mathbf{K}^j\tilde{\mathbf{x}}_{k-\tau+1}^j + \mathbf{B}_w(j)\mathbf{w}_k \end{aligned} \tag{17a}$$
$$\boldsymbol{\xi}_k = \mathbf{C}(j)\mathbf{z}_k + \mathbf{D}_v(j)\mathbf{v}_k. \tag{17b}$$

With (15) we revisit (12) and highlight the reference state and input:

$$\tilde{\mathbf{x}}_{k-\tau+1}^j = \mathbf{z}_{k-\tau+1} \tag{18a}$$
$$\begin{aligned}\tilde{\mathbf{x}}_{\ell+1}^j = {} & \mathbf{A}_{L^j}\tilde{\mathbf{x}}_\ell^j \\ & + [(\ \mathbf{A}(i'_\ell) - \mathbf{A}(j)) - \mathbf{L}^j\,(\mathbf{C}(i'_\ell) - \mathbf{C}(j))]\,(\bar{\mathbf{x}}_\ell^{i'_\ell} + \mathbf{z}_\ell) \\ & + [\mathbf{B}(i'_\ell) - \mathbf{B}(j)]\,(\bar{\mathbf{u}}_\ell + \mathbf{K}^{i'_\ell}(\mathbf{z}_{\ell-\tau+1} - \tilde{\mathbf{x}}_{\ell-\tau+1}^{i'_\ell})) \\ & + \mathbf{r}(i'_\ell) - \mathbf{r}(j) + \mathbf{B}_w(i'_\ell)\mathbf{w}_\ell \\ & - \mathbf{L}^j\,[\mathbf{s}(i'_\ell) - \mathbf{s}(j)] - \mathbf{L}^j\mathbf{D}_v(i'_\ell)\mathbf{v}_\ell, \end{aligned} \tag{18b}$$
$$\begin{aligned}\tilde{\mathbf{y}}_\ell^j = {} & \mathbf{C}(j)\tilde{\mathbf{x}}_\ell^j + [\mathbf{C}(i'_\ell) - \mathbf{C}(j)]\,(\bar{\mathbf{x}}_\ell^{i'_\ell} + \mathbf{z}_\ell) \\ & + \mathbf{s}(i'_\ell) - \mathbf{s}(j) + \mathbf{D}_v(i'_\ell)\mathbf{v}_\ell, \end{aligned} \tag{18c}$$

for $\ell = k-\tau+1,\ldots,k$. We use index i'_ℓ when rewriting $\mathbf{u}_\ell$: for now we make no assumption on the selected index in (15).

C. Set characterizations

For further use we require the sets which characterize the state estimation error (12) and tracking error (16) dynamics.

Recall that by construction, observers (11) have a finite window (i.e., the k-th state and output estimations are derived only from the information available in the interval $k-\tau+1,\ldots,k$). Hence, whatever happens outside of this interval has no influence in the estimations and, implicitly, on the sets which bound them.

First, several assumptions are necessary:

A1) any two consecutive switches are separated by at least $\tau + \tau_c$ instants of time;

A2) (15) uses correct information (the indices of the state estimation and of the dynamics are matched, $i_k = i'_k = j$);

Assuming that dynamics (10) have been under the j-th mode for at least τ consecutive time instants (Assumption A1)), the estimation error of the j-th observer follows (13), thus allowing to compute the corresponding bounding sets:

$$\tilde{\mathscr{X}}_{k-\tau+1}^{j,j} = \{\mathbf{z}_{k-\tau+1}\}, \tag{19a}$$
$$\tilde{\mathscr{X}}_{\ell+1}^{j,j} = \mathbf{A}_{L^j}\tilde{\mathscr{X}}_\ell^{j,j} \oplus \mathbf{B}_w(j)\mathbf{W} \oplus \{-\mathbf{L}^j\mathbf{D}_v(j)\mathbf{V}\}, \tag{19b}$$
$$\tilde{\mathscr{Y}}_\ell^{j,j} = \mathbf{C}(j)\tilde{\mathscr{X}}_\ell^{j,j} \oplus \mathbf{D}_v(j)\mathbf{V}. \tag{19c}$$

for $\ell = k-\tau+1,\ldots,k$. Consequently, we have inclusions $\tilde{\mathbf{x}}_{\ell+1}^j \in \tilde{\mathscr{X}}_{\ell+1}^{j,j}$ and $\tilde{\mathbf{y}}_\ell^j \in \tilde{\mathscr{Y}}_\ell^{j,j}$.

Assuming that the correct estimation is used in (15) – Assumption A2) the tracking error follows (17). Further assuming that $\tilde{\mathbf{x}}_{k-\tau+1}^j \in \tilde{X}^{j,j}$, $\mathbf{w}_k \in \mathbf{W}$ hold, an invariant set $\mathscr{Z}^{j,j}$ is computed as follows: using the extended tracking error state $\boldsymbol{\varkappa}_k = \begin{bmatrix}\mathbf{z}_k^\top & \mathbf{z}_{k-1}^\top & \ldots\mathbf{z}_{k-\tau}^\top\end{bmatrix}^\top$, we obtain an invariant set which guarantees $\boldsymbol{\varkappa}_k \in \mathbf{Z}^j$. Projecting along the subspace associated with $\mathbf{z}_k$ we obtain the set which bounds $\boldsymbol{\varkappa}_k$ while under the selected index j:

$$\mathbf{z}_k \in \mathscr{Z}^{j,j}. \tag{20}$$

Up to now we have shown the sets bounding the 'steady' estimation and tracking error (when the observer and plant model coincide). For further use, we have to consider the case of model mismatch as well.

Assuming that dynamics (10) have been under the j'-th mode for at least τ consecutive time instants (Assumption A1)), the estimation error of the j-th observer follows (18) with the additions $i_\ell = i'_\ell = j'$ and $\tilde{\mathbf{x}}_{\ell-\tau}^{j'} \in \tilde{\mathscr{X}}^{j',j'}$. This leads to bounding sets for the state/output estimation parametrized after the tracking error and state/input references:

$$\tilde{\mathscr{X}}_{k-\tau+1}^{j,j'} = \{\mathbf{z}_{k-\tau+1}\} \tag{21a}$$
$$\begin{aligned}\tilde{\mathscr{X}}_{\ell+1}^{j,j'} = {} & \mathbf{A}_{L^j}\tilde{\mathscr{X}}_\ell^{j,j'} \\ & \oplus\{[(\ \mathbf{A}\ (j') - \mathbf{A}(j)) - \mathbf{L}^j\,(\mathbf{C}(j') - \mathbf{C}(j))]\,(\bar{\mathbf{x}}_\ell^{j'} + \mathbf{z}_\ell)\} \\ & \oplus[\ \mathbf{B}(j'\ ) - \mathbf{B}(j)]\,(\{\bar{\mathbf{u}}_\ell^{j'}\} \oplus \mathbf{K}^{j'}(\{\mathbf{z}_{\ell-\tau}\} \oplus \{-\tilde{\mathscr{X}}^{j',j'}\})) \\ & \oplus\{\mathbf{r}(j') - \mathbf{r}(j)\} \oplus \mathbf{B}_w(j')\mathbf{W} \\ & \oplus\{-\mathbf{L}^j\,[\mathbf{s}(j') - \mathbf{s}(j)]\} \oplus \{-\mathbf{L}^j\mathbf{D}_v(j')\mathbf{V}\}, \end{aligned} \tag{21b}$$
$$\begin{aligned}\tilde{Y}_\ell^{j,j'} = {} & \mathbf{C}(j)\tilde{\mathscr{X}}_\ell^{j,j'} \oplus \{[\mathbf{C}(j') - \mathbf{C}(j)]\,(\bar{\mathbf{x}}_\ell^{j'} + \mathbf{z}_\ell)\} \\ & \oplus\{\mathbf{s}(j') - \mathbf{s}(j)\} \oplus \mathbf{D}_v(j')\mathbf{V}, \end{aligned} \tag{21c}$$

for $\ell = k-\tau+1,\dots,k$. As expected, (21) reduces to (19) when $j = j'$. Lastly, we evaluate the behavior of the tracking error in the interval after a fault and while the correct observer is not yet correctly selected. Using (16) and with the notations $i_k \mapsto j, i'_k \mapsto j'$ and assuming that the switch $j \to j'$ happens at k and that $\tilde{\mathbf{x}}^{j'}_{\ell-\tau} \in \tilde{\mathscr{X}}^{j'j'}$ we have the set recurrence:

$$\mathscr{Z}^{j,j'}_k = \{\mathbf{z}_k\} \tag{22a}$$

$$\begin{aligned}\mathscr{Z}^{j,j'}_{\ell+1} &= \mathbf{A}(j)\mathscr{Z}^{j,j'}_\ell \oplus \{\mathbf{B}(j)\mathbf{K}^{j'}\mathbf{z}_{\ell-\tau+1}\} \\ &\oplus \{-\mathbf{B}(j)\mathbf{K}^{j'}\tilde{\mathscr{X}}^{j'j'}\} \oplus \mathbf{B}_w(j)\mathbf{W} \\ &\oplus \{[\mathbf{A}(j)-\mathbf{A}(j')]\,\bar{\mathbf{x}}^{j'}_{\ell-\tau+1}\} \oplus \{[\mathbf{B}(j)-\mathbf{B}(j')]\,\bar{\mathbf{u}}^{j'}_k\}.\end{aligned} \tag{22b}$$

for $\ell = k+1,\dots,k+\tau$.

Remark 2: The sets defined here are parametrized after the tracking error and after the reference state and input values[2]. The tracking errors appearing in (19a), (21a)–(21b) and (22a) will be replaced with bounding sets as resulted from the FTC scheme. The reference state and input appearing in (21b)–(21c) and (22b) will be used as decision variables to ensure FDI. ♦

IV. FAULT TOLERANT CONTROL SCHEME

The use of bounding sets allows an exact FDI implementation (without missed faults and false alarms) but it requires that the set inclusions assumed in the construction of (19), (21), (20) and (22) hold at all times.

First we discuss the set inclusions and their convergence to ‘steady’ values and second we show how to explicitly choose the reference states and inputs such that FDI is guaranteed.

A. Fault tolerant control scheme implementation

As a first step we revisit the sets obtained earlier and show the stability of the closed-loop scheme. To better clarify these issues, let us consider the following fault scenario, also illustrated in Fig. 1 where, at $k = k_1+1$ the plant switches from functioning mode j to mode j'':

I) For $k \leq k_1$ the plant dynamics are in the j-th mode for a sufficiently long time and the plant/control models are matched ($i_k = i'_k = j$). Therefore, the tracking error and the estimation errors are in their respective sets ($\mathbf{z}_k \in \mathscr{Z}^{j,j}, \tilde{\mathbf{x}}^j_k \in \tilde{\mathscr{X}}^{j,j}(\mathscr{Z}^{j,j})$, $\tilde{\mathbf{x}}^{j'}_k \in \tilde{\mathscr{X}}^{j',j}(\mathscr{Z}^{j,j})$.

II) From $k = k_1+1$ onwards the dynamics switch to mode $i_k = j'$ (i.e., a (different) fault occurs). Hence, the tracking error is no longer guaranteed to use a matched reference model ($i'_k \neq j'$) and thus $\mathbf{z}_k$ is given by dynamics (16) and its bounding set enlarges ($\mathbf{z}_k \in \mathscr{Z}^{j',j}_k$). The estimation errors are indefinite since they are based on mixed information (the observation window contains data from both the j and j' modes of functioning).

III) From $k = k_1+\tau+1$ and until $k = k_1+\tau+\tau_c$ the j'-th observer retrieves the correct estimation and the closed-loop is guaranteed to use the correct information ($i_k = i'_k = j'$). The tracking error is not yet in its invariant set ($\mathscr{Z}^{j',j'}$) but converges towards it (in τ_c time instants, computed a priori). The estimation error for the mismatched observers (for any $j \neq j'$) is computed iteratively via (21) but is cumbersome due to the terms $\mathbf{z}_{k_1+\tau+1}\dots\mathbf{z}_{k_1+\tau+\tau_c}$ which are bounded by transitional sets. At $k = k_1+\tau+\tau_c$ we have inclusion $\mathbf{z}_k \in \mathscr{Z}^{j',j'}$ and hence the estimation errors (and associated output errors) are again within their ‘steady’ sets.

[2]To keep the notation simple we ignored this aspect but whenever necessary, we will employ the full form. For example, $\tilde{\mathscr{Y}}_k^{j,j'}$ from (21) may be written as $\tilde{\mathscr{Y}}_k^{j,j'}(\mathbf{z}_{k-2\tau+1}\dots\mathbf{z}_k, \bar{\mathbf{u}}_{k-\tau+1}\dots\bar{\mathbf{u}}_k, \bar{\mathbf{x}}_{k-\tau+1}\dots\bar{\mathbf{x}}_k)$.

Recalling Remark 2, note that in step I) we use $\tilde{\mathscr{X}}^{j,j}(\mathscr{Z}^{j,j})$, $\tilde{\mathscr{X}}^{j',j}(\mathscr{Z}^{j,j})$. By this, we mean that in (13) and (21) we replace $\mathbf{z}_{k-\tau+1}$ and, $\mathbf{z}_{k-2\tau+1}\dots\mathbf{z}_k$, respectively, with $\mathscr{Z}^{j,j}$.

B. Active fault detection and isolation

Recall that within our framework, the plant is called “underfault” whenever the active index in (10) is $i_k \neq 0$. Thus, we require so-called residual signals which are sensible to specific faults occurrences and whose behavior can unambiguously state whether the system is under fault (detection) and, if so, which is the active fault (isolation). In here we take the observer outputs (11) as the residuals.

From (19) and (21) we have that the output (12b) can stay in one of N possible output sets (in $\tilde{\mathscr{Y}}^{j,j}$ whenever the plant and observer models coincide and in one of the remaining N-1 sets, $\tilde{\mathscr{Y}}^{j,j'}$ when $j \neq j'$). Hence, a sufficient condition to unambiguously decide whether the plant is in the j-th mode of functioning is to have

$$\tilde{\mathscr{Y}}^{j,j}(\mathscr{Z}^{j,j}) \cap \tilde{\mathscr{Y}}^{j,j'}(\mathscr{Z}^{j,j}) = \emptyset, \quad \forall j \neq j', \tag{23}$$

Then, the set inclusion $\tilde{\mathbf{y}}^j_k \in \tilde{\mathscr{Y}}^{j,j}$ is unambiguous (in the sense that $\tilde{\mathbf{y}}^j_k \in \tilde{\mathscr{Y}}^{j,j}$ implies $\tilde{\mathbf{y}}^j_k \notin \tilde{\mathscr{Y}}^{j,j'}$, $\forall j' \neq j$). Repeating (23) for each of the observers allows to uniquely identify the fault (out of the N observers just the one where the internal model and the dynamics model coincide will respect $\tilde{\mathbf{y}}^j_k \in \tilde{\mathscr{Y}}^{j,j}$):

$$i'_k = \arg \min_{j:\, \tilde{\mathbf{y}}^j_k \in \tilde{\mathscr{Y}}^{j,j}} ||\tilde{\mathbf{y}}^j_k||_2. \tag{24}$$

Using the index from (24) into (15) closes the loop and guarantees that the tracking error dynamic remains in a predefined domain. Several remarks are in order.

Remark 3: Any fault could be isolated from a single observer as long as $j' \neq j'' \leftrightarrow \tilde{\mathscr{Y}}^{j,j'} \cap \tilde{\mathscr{Y}}^{j,j''} = \emptyset$. However, in general this is hard to check and since we already have a bank of observers at our disposal, we prefer to check (23). ♦

Remark 4: Usually the problem of “closing the loop” is ignored when devising the FDI mechanism, i.e., the effects of the fault are ignored when analyzing the residuals. As it can be clearly seen in (18) and (16) these effects cannot be ignored since τ cannot be chosen arbitrarily large. ♦

Remark 5: Relation (23) assumes that $\mathbf{z}_k \in \mathscr{Z}^{j,j}$ holds. This corresponds to step I) from Fig. 1. Consequently, we avoid checking the FDI condition during steps II) and III). Instead, having detected the jump $j \to j'$ at $k = k_1+1$ we know (via Assumption A1)) that no other switch will happen in this interval. Hence, we let the estimation error and tracking error

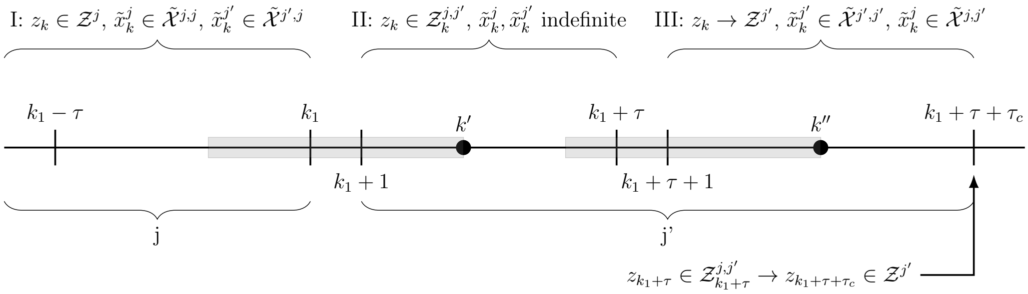


Fig. 1: Timeline for a fault scenario with set inclusion illustration.

sets to settle and re-activate the FDI mechanism only after the lapsing of $\tau + \tau_c$ instants. Thus, we avoid the cumbersome calculations of the interconnected transitional estimation and tracking error sets resulting from (21) and (22). ♦

Up to now, we have only stated the constraints which ensure FDI. The more interesting question is whether it is possible (and if so, how) to force the validation of the FDI condition (23). The key is to notice that $\tilde{\mathscr{Y}}^{j,j'}$ is parametrized after reference variables[3] $\bar{\mathbf{x}}^j_{k-\tau+1}, \bar{\mathbf{u}}^j_{k-\tau+1} \dots \bar{\mathbf{u}}^j_k$.

What remains is to extract the 'variable' part out of $\tilde{\mathscr{Y}}^{j,j'}$. To this end, let us define the following operators:

$$\mathbb{A}_A^N = \begin{bmatrix} A \\ A^2 \\ \vdots \\ A^N \end{bmatrix}, \ \mathbb{B}_{A,B}^N = \begin{bmatrix} B & \dots & 0 \\ AB & \dots & 0 \\ \vdots & \ddots & \vdots \\ A^{N-1}B & \dots & B \end{bmatrix} \tag{25a}$$

$$\mathbb{C}^N_{C,A,B} = \begin{bmatrix} CA^{N-1}B & \dots & CB \end{bmatrix}. \tag{25b}$$

Further denoting $\bar{\boldsymbol{x}}^j_k = \begin{bmatrix} \bar{\mathbf{x}}^{j,\perp}_{k-\tau+1} & \dots \bar{\mathbf{x}}^{j,\perp}_k \end{bmatrix}^\perp$, $\bar{\boldsymbol{u}}^j_k = \begin{bmatrix} \bar{\mathbf{u}}^{j,\perp}_{k-\tau+1} & \dots \bar{\mathbf{u}}^{j,\perp}_k \end{bmatrix}^\perp$ and $\mathbf{X}(j',j) = \mathbf{X}(j') - \mathbf{X}(j)$ we have that the variable part in $\tilde{\mathscr{Y}}^{j,j'}$ is given by

$$\mathbb{C}^\tau_{\mathbf{C}(j),\mathbf{A}_{L^j},\mathbf{B}(j',j)} \bar{\boldsymbol{u}}^j_k + \mathbb{C}^\tau_{\mathbf{C}(j),\mathbf{A}_{L^j},\mathbf{A}_{L^{j,j'}}} \bar{\boldsymbol{x}}^j_k + \mathbf{C}(j',j)\bar{\mathbf{x}}^j_k \tag{26}$$

with $\mathbf{A}_{L^{j,j'}} = \mathbf{A}(j',j) - \mathbf{L}^j\mathbf{C}(j',j)$.

Using (14) we have that

$$\bar{\mathfrak{r}}^j_k = \mathbb{A}^\tau_{\mathbf{A}(j)} \mathbf{x}^j_{k-\tau+1} + \mathbb{B}^\tau_{\mathbf{A}(j),\mathbf{B}(j)} \bar{\boldsymbol{u}}^j_k + \mathbb{B}^\tau_{\mathbf{A}(j),\mathbf{I}} \bar{\mathbf{r}}^j \tag{27a}$$

$$\bar{\mathbf{x}}^j_k = \mathbf{A}^\tau(j)\mathbf{x}^j_{k-\tau+1} + \mathbb{C}^\tau_{\mathbf{I},\mathbf{A}(j),\mathbf{B}(j)} \bar{\boldsymbol{u}}^j_k \tag{27b}$$

Introducing (27) in (26) we have

$$\begin{aligned} &\left[\mathbb{C}^\tau_{\mathbf{C}(j),\mathbf{A}_{L^j},\mathbf{A}_{L^{j,j'}}} \mathbb{A}^\tau_{\mathbf{A}(j)} + \mathbf{C}(j',j)\mathbf{A}^\tau(j)\right] \bar{\mathbf{x}}^j_{k-\tau+1} \\ &+ \Big[\mathbb{C}^\tau_{\mathbf{C}(j),\mathbf{A}_{L^j},\mathbf{B}(j',j)} + \mathbb{C}^\tau_{\mathbf{C}(j),\mathbf{A}_{L^j},\mathbf{A}_{L^{j,j'}}} \mathbb{B}^\tau_{\mathbf{A}(j),\mathbf{B}(j)} \\ &\qquad + \mathbf{C}(j',j)\mathbb{C}^\tau_{\mathbf{I},\mathbf{A}(j),\mathbf{B}(j)}\Big] \bar{\boldsymbol{u}}^j_k. \end{aligned} \tag{28}$$

Let us denote with $\mathbf{F}_{j,j'}$ and $\mathbf{G}_{j,j'}$ the matrices which multiply vectors $\bar{\mathbf{x}}^j_{k-\tau+1}$ and $\bar{\boldsymbol{u}}^j_k$ respectively, in (28). Further, we denote the fixed part of $\tilde{\mathscr{Y}}^{j,j'}$ by $\tilde{\mathscr{Y}}^{j,j',*}$. This includes the fixed offset $\mathbb{B}^\tau_{\mathbf{A}(j),\mathbf{I}}\mathbf{r}^j$ which was extracted from (28). All these notations allow to reformulate (23) as follows:

$$\mathbf{F}_{j,j'}\bar{\mathbf{x}}^j_{k-\tau+1} + \mathbf{G}_{j,j'}\bar{\boldsymbol{u}}^j_k \notin \tilde{\mathscr{Y}}^{j,j}(\mathscr{Z}^{j,j}) \oplus \{-\tilde{\mathscr{Y}}^{j,j',*}(\mathscr{Z}^{j,j})\}, \tag{29}$$

for all $j' \neq j$.

The resulting problem is non-convex: the vector of elements $\left[(\bar{\mathbf{x}}^j_{k-\tau+1})^\top \quad (\bar{\boldsymbol{u}}^j_k)^\top\right]^\top$ has to reside outside of a union of convex sets. The solution proposed here is to use the construction from [12] which exploits the zonotopic nature of the sets for a compact representation of the problem. A mixed integer formulation was employed to reformulate the complementarity condition resulting from the rewriting of the bilevel problem.

V. ILLUSTRATIVE EXAMPLE

We take the example from [12], where a second-order piecewise affine system is considered:

$$\mathbf{A}(1) = \begin{bmatrix} 0.6 & 0.2 \\ -0.4 & -0.2 \end{bmatrix}, \quad \mathbf{B}(1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$\mathbf{C}(1) = \begin{bmatrix} 1 & 0 \end{bmatrix}, \quad \mathbf{s}(1) = \begin{bmatrix} 1 \end{bmatrix}$$
$$\mathbf{B}_w(1) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \mathbf{D}_v(1) = \begin{bmatrix} 1 \end{bmatrix}, \quad \mathbf{r}(1) = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

with the next modifications for the four faulty models ($i = 2, \dots, 5$):

$$\mathbf{B}(2) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \mathbf{B}(3) = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$
$$\mathbf{A}(4) = \begin{bmatrix} 1.2 & 0.2 \\ -0.4 & -0.2 \end{bmatrix}, \quad \mathbf{A}(5) = \begin{bmatrix} 2.0 & 0.2 \\ -0.4 & -0.7 \end{bmatrix}.$$

The necessary sets, in zonotopic notation, are: $\mathbf{W} = \mathscr{Z}(0.5\mathbf{I}, \mathbf{0})$, $\mathbf{V} = \mathscr{Z}(0.2, \mathbf{0})$, the disturbance noises and $\bar{U} = \mathscr{Z}(9\mathbf{I}, \mathbf{0})$ and $\bar{X} = \mathscr{Z}(0.2\mathbf{I}, \mathbf{0})$, the bounds for the references.

We take the observation window $\tau = 5$ and proceed iteratively in order to reach the separation problem (29).

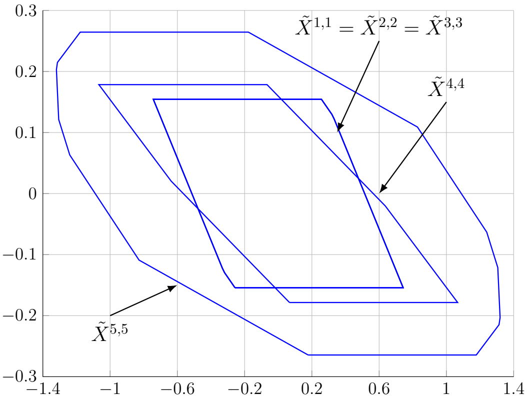
First, for each observer (11) we choose gain matrices L^j via a discrete Riccati equation (with penalty matrices $Q = \mathbf{I}$ and $R = \mathbf{I}$). Next, using the set-recurrence (19), we obtain the state and output estimation error bounds in the matched

[3] Variables $\bar{\mathbf{x}}^j_{k-\tau+2} \dots \bar{\mathbf{x}}^j_k$ do not appear since they can be expressed, via (14), through the former.

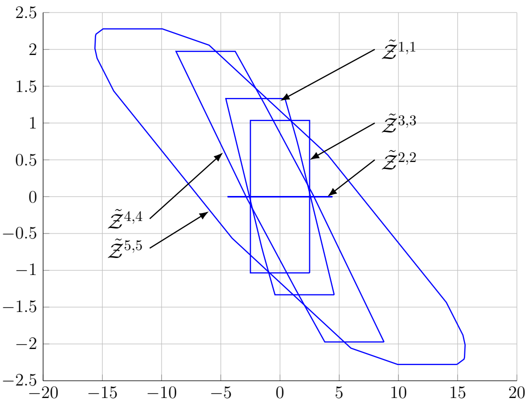
case. Note that, in order to simplify the construction we over-approximate the initialization value ($\{z_{k-\tau+1}\} \to \bar{X}$).

Next, to obtain bounding sets (20) we proceed as follows: using the results from [17] we obtain the feedback matrices K^j; compute the invariant set associated to the lifted tracking error $\boldsymbol{\mathscr{z}}_k$ as in[4] (8) and lastly, we project to the $\mathbf{z}_k$ subspace.

We illustrate in Fig. 2 the resulted sets for each mode of functioning. The first figure shows the $\tilde{\mathscr{X}}^{jj}$ sets obtained in the case $\tau = 5$. The second figure shows the sets $\tilde{\mathscr{Z}}^{jj}$ which incorporate the former sets into their description and show that the closed-loop system is stable in closed-loop. We have now



(a) $\tilde{\mathscr{X}}^{j,j}$ sets



(b) $\tilde{\mathscr{Z}}^{j,j}$ sets

Fig. 2: Illustration of bounding sets for state estimation and tracking errors (for $\tau = 5$).

the tools to compute the transitional sets (21). Applying the set-recurrence and taking the tracking error bounds obtained earlier we construct the fixed part of the output sets, $\tilde{\mathscr{Y}}^{j,j',*}$, as they appear in (29).

Computing matrices $\mathbf{F}_{j,j'}, \mathbf{G}_{j,j'}$ and putting (29) in the mixed-integer formalism of [12] we obtain a non-convex optimization problem whose solution is a feasible initial reference state $x^j_{k-\tau+1}$ and sequence $u^j_{k-\tau+1} \ldots u^j_k$ which ensures FDI form the point of view of the j-th observer.

[4]We fix the value $k^* = 5$ in (9) and obtain the corresponding scaling factors λ.

VI. CONCLUSIONS

We have used here a bank of finite-window observers and an artificially-induced feedback delay to simplify the set construction and guarantee the exactness of an FDI mechanism. Zonotopes have been used extensively due to their theoretical and numerical properties. Further work will be done for the implementation of a FDI-aware reference governor and for the bounding of the transitional sets sparked by a fault occurrence.

ACKNOWLEDGMENT

The work has been funded by a grant of the Romanian National Authority for Scientific Research and Innovation, CNCS-UEFISCDI, project number PN-II-RU-TE-2014-4-2713.

REFERENCES

[1] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and fault-tolerant control*. Springer, 2006.

[2] M. M. Seron, X. W. Zhuo, J. A. De Doná, and J. Martinez, "Multisensor switching control strategy with fault tolerance guarantees," *Automatica*, vol. 44, no. 1, pp. 88–97, 2008.

[3] 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*, vol. 83, no. 12, pp. 2622–2640, 2010.

[4] M. M. Seron, J. A. De Doná, and S. Olaru, "Fault tolerant control allowing sensor healthy-to-faulty and faulty-to-healthy transitions," 2012, iEEE Transactions on Automatic Control, scheduled for July 2012, DOI: 10.1109/TAC.2011.2178716.

[5] F. Blanchini and S. Miani, *Set-theoretic methods in control*. Birkhauser, 2007.

[6] F. Stoican, S. Olaru, M. M. Seron, and J. A. De Doná, "Reference governor design for tracking problems with fault detection guarantees," *Journal of Process Control*, vol. 22, no. 5, pp. 829–836, 2012.

[7] F. Xu, S. Olaru, V. Puig, C. Ocampo-Martinez, and S.-I. Niculescu, "Sensor-fault tolerance using robust mpc with set-based state estimation and active fault isolation," *International Journal of Robust and Nonlinear Control*, 2016.

[8] M. Althoff, O. Stursberg, and M. Buss, "Computing reachable sets of hybrid systems using a combination of zonotopes and polytopes," *Nonlinear analysis: hybrid systems*, vol. 4, no. 2, pp. 233–249, 2010.

[9] L. J. Guibas, A. Nguyen, and L. Zhang, "Zonotopes as bounding volumes," in *Proceedings of the fourteenth annual ACM-SIAM symposium on Discrete algorithms*. Society for Industrial and Applied Mathematics, 2003, pp. 803–812.

[10] M. Althoff and B. H. Krogh, "Zonotope bundles for the efficient computation of reachable sets," in *Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on*. IEEE, 2011, pp. 6814–6821.

[11] M. Althoff, "Cora 2015 manual," *TU Munich*, vol. 85748, 2015.

[12] J. K. Scott, R. Findeisen, R. D. Braatz, and D. M. Raimondo, "Input design for guaranteed fault diagnosis using zonotopes," *Automatica*, vol. 50, no. 6, pp. 1580–1589, 2014.

[13] W. Kühn, "Rigorously computed orbits of dynamical systems without the wrapping effect," *Computing*, vol. 61, no. 1, pp. 47–67, 1998.

[14] K. Fukuda, "From the zonotope construction to the Minkowski addition of convex polytopes," *Journal of Symbolic Computation*, vol. 38, no. 4, pp. 1261–1272, 2004.

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

[16] S. Rakovic, E. Kerrigan, K. Kouramas, and D. Mayne, *Invariant approximations of robustly positively invariant sets for constrained linear discrete-time systems subject to bounded disturbances*. Department of Engineering University of Cambridge, Tech. Rep. CUED/F-INFENG/TR 473 (2004), 2004.

[17] W. Michiels and S.-I. Niculescu, *Stability, Control, and Computation for Time-Delay Systems: An Eigenvalue-Based Approach*. SIAM, 2014.