A Decentralized Fault-Tolerant Control scheme based on Active Fault Diagnosis

Davide M. Raimondo, Francesca Boem, Alexander Gallo, Thomas Parisini

***Abstract*— This paper deals with a decentralized fault-tolerant control methodology based on an *Active Fault Diagnosis approach*. The proposed technique addresses the important problem of monitoring interconnected Large-Scale Systems (LSS). The fault diagnosis approach is made of a passive set-based fault detection method and an active fault isolation technique, able to guarantee isolability subject to local input and state constraints. The proposed scheme can be implemented locally in a decentralized way. A significant feature is the decentralized design constructed on tube-based Model Predictive Control to possibly allow the disconnection of faulty subsystems or the reconfiguration of local controllers. The Active Fault Diagnosis tool is designed to support the decision-making process for the control and monitoring of the LSS.**

I. Introduction

In recent years, the problem of monitoring Large-Scale Systems has attracted increasing interest in academia and industry. Some distributed architectures have been developed for distributed Fault Detection and Isolation (FDI) (see as example [1], [2], [3], [4], [5]). These works rely on passive FDI methods, in which the status of healthy of the system is analyzed by comparing input-output data for the closed-loop system with a process model or historical data. One of the issues when dealing with passive FDI approaches is that the feedback controller may hide the presence of faults by compensating their effects (see as example [6]) and making fault detection and isolation more difficult or even impossible. Instead, active FDI approaches consist in suitably modifying the control input to improve fault detectability and isolability capabilities [7], [8], [9]. However, one of the limitations of these approaches is the possibly high computational cost and complexity [10] that has prevented their use in the context of LSS systems. In order to overcome this issue, in this paper we propose a decentralized architecture, where a linear LSS composed of a (possibly large) number interconnected subsystems is considered and each subsystem is monitored by a *local fault diagnoser* (see [3]), implementing a passive set-based fault detection method and an active fault isolation approach, guaranteeing isolability subject to local input and state constraints. To the best of the authors' knowledge, this is the first time that an Active Fault Diagnosis approach is proposed in a decentralized architecture for the monitoring of LSS. Moreover, a decentralized active Fault Tolerant Control (FTC) scheme is proposed where – in healthy modes of behavior – the subsystems are robustly controlled by a decentralized tube-based Model Predictive Control (MPC) (similarly as in [11]) and monitored by a set-based passive fault detection method. After fault detection, the Active Fault Isolation tool supports the decision-making process. The goals are, if feasible, the isolation of the fault and the reconfiguration of the local controllers according to the new identified dynamics. We take advantage of the decentralized design of the local controllers to possibly allow the disconnection of faulty subsystems when the local control reconfiguration is not feasible.

In the literature, FTC methods are classified as either active or passive [12]. Passive FTC refers to the design of controllers that are robust to potential faults without modification, while active FTC schemes modify the control law in response to a fault [13], [14], [15], requiring therefore methods for the detection and isolation of the faults. These methods typically assume that the faults are detected and isolated correctly and instantaneously, or that the faults occur in the absence of disturbances and measurement noise so that FDI is fast and accurate. These assumptions do not hold in real systems and delays and errors in FDI can lead to problems such as instability, violation of state constraints, and the inability to implement the suitable controller after isolation [16]. These issues can be mitigated by the use of active FDI methods. The use of such methods in the context of active FTC has been limited to the centralized case [10], [17], [18]. As far as the distributed/decentralized case is concerned, the contributions about fault-tolerant schemes are more recent, but either they assume to know the FDI results as given correct elements (see [19], [20] as examples) or they use passive techniques, as in [6], where a distributed passive FDI is integrated with distributed MPC in a PnP scenario for nonlinear systems. On the other hand, the main contribution of the paper is a decentralized active FTC scheme using Active Fault Isolation, for the monitoring and control of interconnected subsystems.

II. Problem Formulation

Consider a discrete-time affine large scale system composed of N subsystems. Each subsystem obeys one of n_{m_i} possible dynamics (all known and observable). When model

This work has been conducted as part of the research project *Stability and Control of Power Networks with Energy Storage* (STABLE-NET) which is funded by the RCUK Energy Programme (contract no: EP/L014343/1).

D.M. Raimondo is with the Dept. of Electrical, Computer and Biomedical Engineering, University of Pavia, Italy. (davide.raimondo@unipv.it)

F. Boem is with the Dept. of Electrical and Electronic Engineering at the Imperial College London, UK. (f.boem@imperial.ac.uk)

A. Gallo is MEng student at the Imperial College London, UK. (alexander.gallo12@imperial.ac.uk)

T. Parisini is with the Dept. of Electrical and Electronic Engineering at the Imperial College London, UK, and also with the Dept. of Engineering and Architecture at University of Trieste, Italy. (t.parisini@gmail.com)

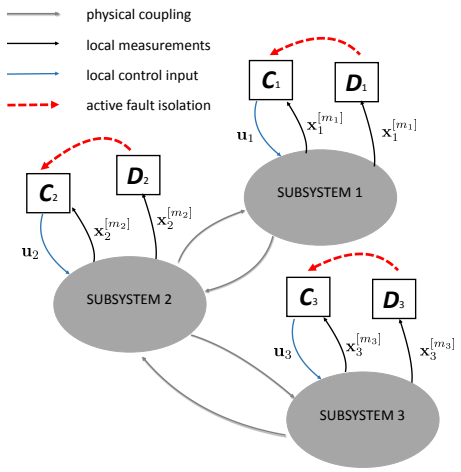

Fig. 1. The proposed decentralized architecture. The subsystems are physically interconnected. Each subsystem is controlled by a local controller C_i and monitored by a local diagnoser D_i, both taking measurements from the local subsystems. After fault detection, the Active fault isolation tool may compute an input control sequences to allow the isolation of the fault.

$m_i \in \mathscr{M}_i = \{1,\cdots,n_{m_i}\}$ is active, the subsystem $i \in \mathscr{N} = \{1,\ldots,N\}$ is governed by the following set of equations

$$\mathbf{x}_i^{[m_i]}(k+1) = \mathbf{A}_{ii}^{[m_i]}\mathbf{x}_i^{[m_i]}(k) + \mathbf{B}_i^{[m_i]}\mathbf{u}_i(k) + \mathbf{w}_i^{[m_i]}(k) + \mathbf{r}_i^{[m_i]} \quad (1)$$

$$\mathbf{w}_i^{[m_i]}(k) = \sum_{j\in\mathscr{N}_i} \mathbf{A}_{ij}^{[m_i]}\mathbf{x}_j^{[m_i]}(k) + \mathbf{d}_i(k) \quad (2)$$

where $\mathbf{x}_i^{[m_i]}(k) \in \mathbb{R}^{n_{x_i}}$, $\mathbf{u}_i(k) \in \mathbb{R}^{n_{u_i}}$ denote respectively the states and the inputs of subsystem i. The constant vector $\mathbf{r}_i^{[m_i]}$ is used to model additive faults, e.g. actuator offsets, while vector $\mathbf{w}_i^{[m_i]}(k) \in \mathbb{R}^{n_{x_i}}$ accounts for the coupling with neighbouring subsystems and the presence of process noise $\mathbf{d}_i(k)$. The set of neighbours to subsystem i is defined as $\mathscr{N}_i^{[m_i]} = \{j \in \mathscr{N} : \mathbf{A}_{ij}^{[m_i]} \neq 0, i \neq j\}$. Matrices $\mathbf{A}_{ij}^{[m_i]}, \forall i,j \in \mathscr{N}$ are blocks of matrix $\mathbf{A}^{[m_i]}$, where this latter represents the dynamic matrix of the overall system. It is assumed that $(\mathbf{A}_{ii}^{[m_i]}, \mathbf{B}_i^{[m_i]})$ is stabilizable for all $i \in \mathscr{N}$, $m_i \in \mathscr{M}_i$.

The objective of this work is to provide a decentralized FTC scheme which benefits of an active fault diagnosis strategy. Each subsystem is governed by a local controller and monitored by a local fault diagnoser, as illustrated in Fig. 1. Each subsystem is governed by a model predictive controller, subject to local input and state constraints, i.e. $\mathbf{x}_i^{[m_i]}(k) \in X_i, \mathbf{u}_i(k) \in U_i$, and robust to $\mathbf{w}_i^{[m_i]}(k) \in W_i^{[m_i]} = \sum_{j\in\mathscr{N}_i} \mathbf{A}_{ij}^{[m_i]} X_j + D_i$, with D_i bounding the process noise $\mathbf{d}_i(k)$. For each $i \in \mathscr{N}$, sets X_i, U_i, D_i, and consequently $W_i^{[m_i]}$, are all zero-centered zonotopes (see §III) known a priori. In order to guarantee robust stability and constraint satisfaction for the overall system, the local controllers are designed according to [21] (summarized in §IV). For each $i \in \mathscr{N}$, we assume $m_i = 1$ represents the nominal dynamics, while the other models describe possible faulty dynamics. The local control laws are synthesized off-line for every model $m_i \in \mathscr{M}_i$. Each subsystem is monitored in healthy conditions by a passive set-based fault detection method. When a fault is detected in a local subsystem at time k_d, the related controller is put in stand-by and a local active FDI procedure initiated (§V-B). Active FDI aims to determine which dynamics subsystem i is subject to, by injecting a minimally harmful (in length and/or norm) sequence $(\mathbf{u}_i(k_d),\cdots,\mathbf{u}_i(k_d+T_i-1))$ able to guarantee that any possible state (or state sequence) of subsystem i at time k_d+T_i is consistent with only one $m_i \in \mathscr{M}_i$. In order to not spoil the stability properties of the overall system, such procedure is performed while guaranteeing that the local subsystem evolves within its state bounds X_i, regardless of the active fault mode m_i. It is assumed that the diagnosis is fast enough to avoid the switching between models during $[k_d,\cdots,k_d+T_i]$. Moreover, we assume that there are no faults occurring in parallel on multiple subsystems, i.e. faults affect only one subsystem at a time. Once the fault is isolated, the local controller is reconfigured in order to still guarantee the stability and constraint satisfaction of the overall system.

III. Notation and Basic Definitions

A tilde is used to indicate sequences associated with (1)-(2). When referring to $\tilde{\mathbf{u}}_{i(l:k)}, \tilde{\mathbf{w}}_{i(l:k)}$, the notation stands for $\tilde{\sigma}_{(l:k)} = (\sigma(l),\ldots,\sigma(k-1))$, while $\tilde{\sigma}_{(l:k)} = (\sigma(l),\ldots,\sigma(k))$ for $\tilde{\mathbf{x}}_{i(l:k)}$ Similarly, one has $\tilde{\sigma}_{(k)} = (\sigma(0),\ldots,\sigma(k-1))$ or $\tilde{\sigma}_{(k)} = (\sigma(0),\ldots,\sigma(k))$. The notation $\tilde{\sigma}_{(l:k|l)}$ indicates that the sequence is computed at time l. For each subsystem i, the state of model m_i, k-steps ahead, is given by the function $\phi_{i\{k\}}^{[m_i]}(\tilde{\mathbf{u}}_{i(k)}, \mathbf{x}_i^{[m_i]}(0), \tilde{\mathbf{w}}_{i(k)}^{[m_i]})$ with $\phi_{i\{k\}}^{[m_i]} : \mathbb{R}^{n_{u_i}k} \times \mathbb{R}^{n_{x_i}} \times \mathbb{R}^{n_{x_i}k} \to \mathbb{R}^{n_{x_i}}$ the state solution map. The notation $\tilde{W}_{\{k\}} = W \times \ldots \times W$ is used to indicate the k-th cartesian product of a set W. *Zonotopes* are centrally symmetric convex polytopes. Denoting with $\mathbf{G} = [\mathbf{g}_1 \ \ldots \ \mathbf{g}_{n_g}] \in \mathbb{R}^{n\times n_g}$ the generator matrix and with $\mathbf{c} \in \mathbb{R}^n$ the zonotope center, the set can be expressed as $Z = \{\mathbf{G}\xi + \mathbf{c} : \|\xi\|_\infty \leq 1\}$, and compactly indicated as $Z = \{\mathbf{G}, \mathbf{c}\}$. The order of a zonotope is defined as n_g/n. Zonotopes complexity (which depends on the number of generators) can be reduced by outer approximating zonotopes using sets with less generators [22]. Given an initial condition $\mathbf{x}_i^{[m_i]}(k_0)$, a sequence $\tilde{\mathbf{u}}_{i(k_0:k|k_0)}$ and a set $\tilde{W}_{i\{k-k_0\}}^{[m_i]} = \{\mathbf{G}_{\tilde{W}_{i\{k-k_0\}}^{[m_i]}}, \mathbf{0}\}$ the state *reachable set* at time k is defined as

$$\mathsf{X}_{i(k|k_0)}^{[m_i]}(\tilde{\mathbf{u}}_{i(k_0:k|k_0)}, \mathbf{x}_i^{[m_i]}(k_0), \tilde{W}_{i\{k-k_0\}}^{[m_i]})$$
$$= \{\phi_{i\{k_0-k\}}^{[m_i]}(\tilde{\mathbf{u}}_{i(k_0:k|k_0)}, \mathbf{x}_i^{[m_i]}(k_0), \tilde{\mathbf{w}}_{i(k_0:k)}^{[m_i]}) : \tilde{\mathbf{w}}_{i(k_0:k)}^{[m_i]} \in \tilde{W}_{i\{k-k_0\}}^{[m_i]}\}$$

When clear from the context, the arguments of sets and maps will be omitted. Thanks to zonotope properties (5)-(7) in [23], by iterating the state dynamics (1), one obtains suitable matrices $\tilde{\mathbf{B}}_{w_i\{k-k_0\}}^{[m_i]}$, etc., such that

$$\mathsf{X}_{i(k|k_0)}^{[m_i]} = \left\{ \left[\tilde{\mathbf{B}}_{w_i\{k-k_0\}}^{[m_i]} \mathbf{G}_{\tilde{W}_{i\{k-k_0\}}^{[m_i]}} \right], \phi_{i\{k-k_0\}}^{[m_i]}(\tilde{\mathbf{u}}_{i(k_0:k|k_0)}, \mathbf{x}_i(k_0)^{[m_i]}, \mathbf{0}) \right\}$$

Note that $\tilde{\mathbf{u}}_{i(k_0:k|k_0)}$ affects only the center of these sets.

IV. Decentralized MPC

The proposed FTC method assumes that each subsystem is equipped with a tube-based robust MPC controller which

is designed, for each $i \in \mathcal{N}, m_i \in \mathcal{M}_i$, according to [21]. The approach is briefly recalled in the following.

In a decentralized tube-based robust MPC approach, the control action for each $i \in \mathcal{N}$ is given by the sum of two terms: (i) a nominal input, obtained by solving, at each k, an optimal control problem subject to the nominal model

$$\overline{\mathbf{x}}_i^{[m_i]}(k+1) = \mathbf{A}_{ii}^{[m_i]}\overline{\mathbf{x}}_i^{[m_i]}(k) + \mathbf{B}_i^{[m_i]}\overline{\mathbf{u}}_i(k) + \mathbf{r}_i^{[m_i]} \tag{3}$$

and (ii) a linear feedback term designed to track the prediction of this nominal model. These terms are here described in reverse order.

Let $\mathbf{K}_i^{[m_i]} \in \mathbb{R}^{n_{u_i} \times n_{x_i}}$ be so that $\mathbf{A}_{K_i}^{[m_i]} \equiv \mathbf{A}_{ii}^{[m_i]} + \mathbf{B}_i^{[m_i]}\mathbf{K}_i^{[m_i]}$ is Schur. Define $\mathbf{e}_i^{[m_i]}(k) \equiv \mathbf{x}_i^{[m_i]}(k) - \overline{\mathbf{x}}_i^{[m_i]}(k)$ the tracking error between the nominal state $\overline{\mathbf{x}}_i^{[m_i]}(k)$, solution of (3) with nominal input $\overline{\mathbf{u}}_i(k)$, and the real state $\mathbf{x}_i^{[m_i]}(k)$, obtained by solving (1) with $\mathbf{u}_i(k) = \overline{\mathbf{u}}_i(k) + \mathbf{K}_i^{[m_i]}(\mathbf{x}_i^{[m_i]}(k) - \overline{\mathbf{x}}_i^{[m_i]}(k))$. This error obeys the dynamics

$$\mathbf{e}_i^{[m_i]}(k+1) = \mathbf{A}_{K_i}^{[m_i]}\mathbf{e}_i^{[m_i]}(k) + \mathbf{w}_i^{[m_i]}(k) \tag{4}$$

Thanks to the stability of $\mathbf{A}_{K_i}^{[m_i]}$ and the boundedness of $W_i^{[m_i]}$ (resulting from the bounds $X_j, j \in \mathcal{N}_i$), $\exists E_i^{[m_i]} \subset \mathbb{R}^{n_{x_i}}$ such that $\mathbf{A}_{K_i}^{[m_i]} E_i^{[m_i]} + W_i^{[m_i]} \subset E_i^{[m_i]}$. If $\mathbf{e}_i^{[m_i]}(0) \in E_i^{[m_i]}$ and $\mathbf{w}_i^{[m_i]}(k) \in W_i^{[m_i]}$, $\forall k \in \mathbb{N}$, then the solution of (4) satisfies $\mathbf{e}_i^{[m_i]}(k) \in E_i^{[m_i]}$, $\forall k \in \mathbb{N}$. $E_i^{[m_i]}$ is a robust positively invariant set and can be computed as described in [24]. We select $E_i^{[m_i]}$ to be the minimal robust positively invariant set. Note that the computation of each $E_i^{[m_i]}$ requires the knowledge of the state constraints of the neighbouring subsystems $\mathcal{N}_i^{[m_i]}$ only.

A robust MPC controller can be obtained, for each subsystem i, by appending the feedback term $\mathbf{K}_i^{[m_i]}(\mathbf{x}_i^{[m_i]}(k) - \overline{\mathbf{x}}_i^{[m_i]}(k))$ to a nominal input $\overline{\mathbf{u}}_i(k)$, obtained by solving the finite horizon optimal control problem (FHOCP) below for system (3)

$$\min_{\substack{\bar{\mathbf{x}}_i^{[m_i]} \\ \bar{\mathbf{u}}_{i(k:k+\mathsf{N}-1)}^{[m_i]}}} \sum_{t=k}^{k+\mathsf{N}-1} \left[\bar{\mathbf{x}}_i^{[m_i]}(t)^{\mathrm{T}}\mathbf{Q}_i^{[m_i]}\bar{\mathbf{x}}_i^{[m_i]}(t) + \bar{\mathbf{u}}_i^{[m_i]}(t)^{\mathrm{T}}\mathbf{R}_i^{[m_i]}\bar{\mathbf{u}}_i^{[m_i]}(t)\right] + \bar{\mathbf{x}}_i^{[m_i]}(k+\mathsf{N})^{\mathrm{T}}\mathbf{P}_i^{[m_i]}\bar{\mathbf{x}}_i^{[m_i]}(k+\mathsf{N})$$

$$\begin{aligned}
\text{subj. to} \quad & \text{dynamics (3)} \\
& \bar{\mathbf{x}}_i^{[m_i]}(k) \in \mathbf{x}_i^{[m_i]}(k) \oplus E_i^{[m_i]} \\
& \bar{\mathbf{x}}_i^{[m_i]}(t) \in \overline{X}_i^{[m_i]},\ t \in [k, \mathsf{N}-1] \\
& \bar{\mathbf{u}}_i^{[m_i]}(t) \in \overline{U}_i^{[m_i]},\ t \in [k, \mathsf{N}-1] \\
& \bar{\mathbf{x}}_i^{[m_i]}(k+\mathsf{N}) \in \overline{X}_{f_i}^{[m_i]}
\end{aligned}$$

where $\mathbf{Q}_i^{[m_i]} \geq 0, \mathbf{R}_i^{[m_i]} > 0$. The terminal set $\overline{X}_{f_i}^{[m_i]} \subseteq \overline{X}_i^{[m_i]}$ and the terminal penalty $\mathbf{P}_i^{[m_i]} \in \mathbb{R}^{n_{x_i} \times n_{x_i}}$, and the matrix gain $\mathbf{K}_i^{[m_i]} \in \mathbb{R}^{n_{u_i} \times n_{x_i}}$ are computed in order to satisfy the usual stability conditions for (3) (Assumptions 2 and 3 in [25]). The problem above is required to satisfy the tightened constraints $\overline{U}_i^{[m_i]} \equiv U_i \ominus \mathbf{K}_i^{[m_i]} E_i^{[m_i]}$ and $\overline{X}_i^{[m_i]} \equiv X_i^{[m_i]} \ominus E_i^{[m_i]}$.

Remark 1: Note that, in order Problem (5) to be feasible, it is necessary that both $\overline{U}_i^{[m_i]}$ and $\overline{X}_i^{[m_i]}$ are non-empty. In order this to hold, the effect of the process noise and the coupling between subsystems is required to be sufficiently small.

Let $\bar{F}_i^{[m_i]}$ denote the set of initial conditions $\bar{\mathbf{x}}_i^{[m_i]}$ for which the problem above is feasible. Let $F_i^{[m_i]} = \bar{F}_i^{[m_i]} \oplus E_i^{[m_i]}$. Denoting the optimizers of the FHOCP as $(\tilde{\bar{\mathbf{x}}}_{i(k:k+\mathsf{N})}^{[m_i]}, \tilde{\bar{\mathbf{u}}}_{i(k:k+\mathsf{N}-1)}^{[m_i]})$, the tube-based MPC feedback law $\kappa_i^{[m_i]} : F_i^{[m_i]} \to \mathbb{R}^{n_{u_i}}$ is defined as

$$\kappa_i^{[m_i]}(\mathbf{x}_i^{[m_i]}(k)) = \bar{\mathbf{u}}_i^{[m_i]}(k) + \mathbf{K}_i^{[m_i]}(\mathbf{x}_i^{[m_i]}(k) - \bar{\mathbf{x}}_i^{[m_i]}(k)) \tag{5}$$

Finally, the following theorem summarizes the properties of the robust MPC scheme above.

Theorem 1: Assume that $\mathbf{x}_i^{[m_i]}(0) \in F_i^{[m_i]}$ and $\mathbf{w}_i^{[m_i]}(k) \in W_i^{[m_i]}$, $\forall k \in \mathbb{N}$ and that no faults have occurred in the LSS. Then the system (1) in closed loop with $\kappa_i^{[m_i]}$ satisfies $(\mathbf{u}_i^{[m_i]}(k), \mathbf{x}_i^{[m_i]}(k)) \in U_i \times F_i$, $\forall k \in \mathbb{N}$, and $\lim_{k\to\infty} d(\mathbf{x}_i^{[m_i]}(k), E_i^{[m_i]}) \to 0$ exponentially fast.

Proof: The result follows from [21]. ■

Define $m = [m_1, \cdots, m_N]$, $F^{[m]} = F_1^{[m_1]} \times \cdots \times F_N^{[m_n]}$, $E^{[m]} = E_1^{[m_1]} \times \cdots \times E_N^{[m_n]}$. The decentralized tube based MPC summarized above guarantees the robust stability of set $E^{[m]}$ and constraint satisfaction for the overall system: if $\mathbf{x}^{[m]}(0) \in F^{[m]}, \forall i \in \mathcal{N}$, then $\mathbf{x}^{[m]}(k) \in F^{[m]}, \forall k \in \mathbb{N}$, and $\lim_{k\to\infty} d(\mathbf{x}^{[m]}(k), E^{[m]}) \to 0$.

V. Robust Fault Detection and Isolation

This section presents the FDI procedures used in the proposed FTC approach. In the time interval $[0, k_d]$, the nominal model $m_i = 1$ is believed to be active and $\mathbf{u}_i(k)$ is determined using $\mathbf{K}_i^{[1]}$. At the same time, passive fault detection is done using a set-based approach as described in §V-A. After fault detection, in the interval $[k_d, k_{is}]$, active fault isolation is carried out, as described in §V-B.

A. Passive Fault Detection

According to the tube based MPC approach described above, if $\mathbf{e}_i^{[m_i]}(0) \in E_i^{[m_i]}$ and $\mathbf{w}_i^{[m_i]}(k) \in W_i^{[m_i]}$, $\forall k \in \mathbb{N}$, then $\mathbf{e}_i^{[m_i]}(k) \in E_i^{[m_i]}$, $\forall k \in \mathbb{N}$. This property is very useful for detecting, in a decentralized way, the presence of a possible fault in subsystem i. At each time step $k+1$, given the nominal state $\overline{\mathbf{x}}_i^{[m_i]}(k+1)$ obtained by solving the FHOCP at time k, we compute the error $\mathbf{e}_i^{[m_i]}(k+1)$ between $\overline{\mathbf{x}}_i^{[m_i]}(k+1)$ and the real state $\mathbf{x}_i^{[m_i]}(k+1)$. If, at any $k+1 > 0$,

$$\mathbf{e}_i^{[1]}(k+1) \notin E_i^{[1]} \tag{6}$$

then, the nominal model $m_i = 1$ is not consistent with the behaviour of the subsystem, i.e. a fault has occurred in subsystem i. While this approach allows to detect the presence of a fault, due to the presence of $\mathbf{w}_i^{[m_i]}$ the passive isolation of the malfunction could be challenging. For this reason, in the following, we suggest to use a decentralized version of the active FDI scheme proposed in [8].

B. Active Fault Isolation

Suppose condition (6) is verified at time k_d, indicating that a fault occurred at some k_f with $0 \leq k_f < k_d$. Assume no further faults occur in the LSS between k_f and the time k_{is} at which isolation is completed. Moreover, assume that, for the system which is affected by a fault, the state dynamics stays within bounds between k_f and k_d. At k_d, the active model m_i is unknown except that $m_i \neq 1$.

Denote with $\hat{\mathbf{x}}_i(k_d)$ the state value at time k_d (the superscript argument is omitted, since, at this stage, the nature of the fault is unknown). Define $\mathscr{M}_i^+ \equiv \mathscr{M}_i \backslash \{1\}$. The objective of decentralized active fault isolation is to isolate the local malfunction by driving the system to a state condition which can be explained by one faulty model only. In other words, given $\mathbf{x}_i^{[\alpha_i]}(k_d) = \hat{\mathbf{x}}_i(k_d)$, $\mathbf{x}_i^{[\beta_i]}(k_d) = \hat{\mathbf{x}}_i(k_d)$, we look for the existence of a local sequence $\tilde{\mathbf{u}}_{i(k_d:k_d+T_i|k_d)}$ leading to $\mathbf{x}_i^{[\alpha_i]}(k_d+T_i) \neq \mathbf{x}_i^{[\beta_i]}(k_d+T_i)$, for all $(\tilde{\mathbf{w}}^{[\alpha_i]}_{i(k_d:k_d+T_i|k_d)}, \tilde{\mathbf{w}}^{[\beta_i]}_{i(k_d:k_d+T_i|k_d)}) \in W_i^{[\alpha_i]} \times W_i^{[\beta_i]}$, and all $\alpha_i \neq \beta_i$ with $\alpha_i, \beta_i \in \mathscr{M}_i^+$. This corresponds to verifying the separation of the state reachable sets at time k_d+T_i, i.e. $\mathsf{X}^{[\alpha_i]}_{i(k_d+T_i|k_d)}(\tilde{\mathbf{u}}_{i(k_d:k_d+T_i|k_d)}, \hat{\mathbf{x}}_i(k_d)) \cap \mathsf{X}^{[\beta_i]}_{i(k_d+T_i|k_d)}(\tilde{\mathbf{u}}_{i(k_d:k_d+T_i|k_d)}, \hat{\mathbf{x}}_i(k_d)) = \emptyset$ for all the possible faulty dynamics $\mathscr{M}_i^+$ (assuming that $\mathscr{M}_i$ is exhaustive). For ease of reading, in the following, the dependence of the reachable sets on $W_i^{[\alpha_i]}$, $W_i^{[\beta_i]}$ will be omitted. In order to obtain the minimally harmful (in terms of length/norm) input sequence guaranteeing diagnosis we solve

$$\min_{\tilde{\mathbf{u}}_{i(k_d:k_d+T_i|k_d)}} \|\tilde{\mathbf{u}}_{i(k_d:k_d+T_i|k_d)}\|_2^2 \tag{7}$$

$$\begin{aligned}
\text{subj. to} \quad & \text{dynamics } (1)-(2) && (8)\\
& \mathbf{x}_i^{[m_i]}(k_d) = \hat{\mathbf{x}}_i(k_d), \quad \forall m_i \in \mathscr{M}_i^+ && (9)\\
& \mathbf{u}_i(k) \in U_i, \quad k \in [k_d, k_d+T_i-1] && (10)\\
& \mathsf{X}^{[m_i]}_{i(k|k_d)} \subseteq X_i^{[m_i]}, \quad k \in [k_d, k_d+T_i-1] && (11)\\
& \mathsf{X}^{[m_i]}_{i(k_d+T_i|k_d)} \subseteq F_i^{[m_i]}, \quad \forall m_i \in \mathscr{M}_i^+ && (12)\\
& \mathsf{X}^{[\alpha_i]}_{i(k_d+T_i|k_d)} \cap \mathsf{X}^{[\beta_i]}_{i(k_d+T_i|k_d)} = \emptyset, \quad \alpha_i \neq \beta_i && (13)
\end{aligned}$$

with increasing $T_i = 1, \cdots$ until the problem becomes feasible or a T_{max} is attained. For each $i \in \mathscr{M}_i^+$, constraint (11) ensures that $\mathbf{x}_i^{[m_i]}(k) \in X_i^{[m_i]}$ for all $k \in [k_d, k_d+T_i-1]$. Similarly, for each $i \in \mathscr{M}_i^+$, the constraint (12) ensures that, at the end of the isolation horizon, $\mathbf{x}_i^{[m_i]}(k_d+T_i) \in F_i^{[m_i]}$. As shown in §IV, the satisfaction of this constraint ensures that the controller $\kappa_i^{[m_i]}$ can be feasibly implemented at time k_d+T_i for any possible fault $m_i \in \mathscr{M}^+$. According to [8], the problem above can be reformulated as a mixed-integer quadratic program (MIQP) which can be solved using, e.g. CPLEX [26].

Remark 2: Note that, the satisfaction of constraint (12) may be difficult in general. However, if problem (7) is not feasible, we can still unplug the subsystem where the fault was detected and still preserve the overall stability (see §VI).

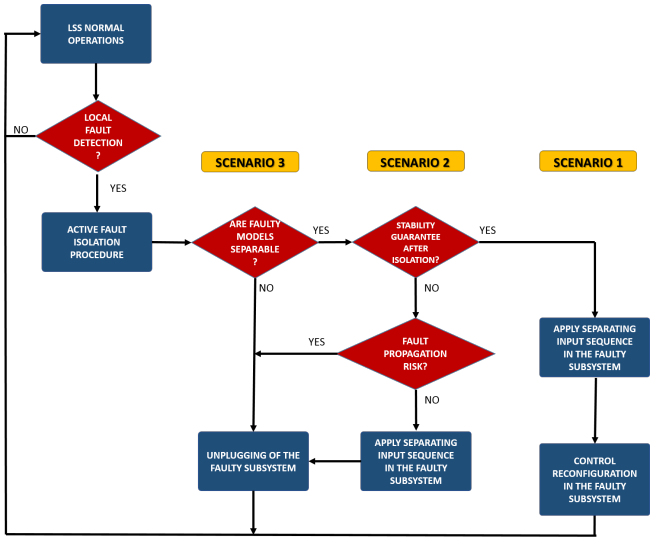

Fig. 2. The proposed FTC strategy. Three possible scenarios are considered by the Active Fault Isolation procedure.

Finally, by injecting $\tilde{\mathbf{u}}_{i(k_d:k_d+T_i|k_d)}$, solution of problem (7), into subsystem i, fault isolation is obtained in at most T_i steps by verifying which reachable set $\mathsf{X}^{[m_i]}_{i(k|k_d)}$ the real $\mathbf{x}_i(k_d+T_i)$ belongs to. Since the problem above guarantees the isolability for all the possible realizations of $\tilde{\mathbf{w}}_i^{[m_i]}$, it is possible to obtain an earlier isolation, i.e. at time $k < k_d+T_i$ $\mathbf{x}_i(k)$ is already consistent with one model m_i only. Note that, rather than applying the entire sequence $\tilde{\mathbf{u}}_{i(k_d:k_d+T_i|k_d)}$, it is possible to apply the Active FDI approach above in a closed-loop fashion by re-solving problem (7) at each time step with the newly available state [27].

VI. FTC Strategy

In this section we detail how we can use the tools we have introduced in the previous sections for the proposed FTC strategy. At time $k=0$, the nominal model $m=1$ is active. During healthy nominal behaviour, before fault detection, each subsystem is controlled by the decentralized tube-based MPC introduced in §IV and monitored by the passive fault detection method in §V-A. At time k_f, a single fault occurs in subsystem i and is detected at time $k_d > k_f$ (if the effect of the fault cannot be explained by the local uncertainties represented by $\mathbf{w}_i^{[m_i]}$). At time k_d, the Active Fault Isolation tool (see §V-B) is activated. Three possible scenarios can be in place, illustrated in Figure 2.

Scenario 1. There exists a control input sequence so that Problem (7) is feasible, i.e. *i)* it is possible to separate the reachable sets of the different faulty dynamics (achieving therefore fault isolation) *ii)* the state after fault isolation is guaranteed to remain in the domain of attraction, making feasible the reconfiguration of the i-th local controller designed as in §IV for the identified model $m_i \neq 1$. More specifically, applying the input computed by the Active Fault Isolation tool, the fault is isolated at most at time k_d+T_i, identifying which model $m_i \in \mathscr{M}_i$, $m_i \neq 1$ is acting in the local subsystem i. Furthermore, the computed input

guarantees that $\mathbf{x}_i^{[m_i]}(k_d+T_i) \in F_i^{[m_i]}$. At time k_d+T_i, once to the novel "nominal" dynamics is isolated, its controller is implemented continuing to guarantee the stability of the LSS; it will be not necessary to disconnect the faulty subsystem or to reconfigure neighbouring subsystems, since the local controller continues to satisfy local state constraints X_i and therefore the influence of the reconfigured subsystem i for the computation of W_j in the neighbouring subsystems $j \in \mathcal{N}_i$ remains bounded as before the local control reconfiguration of i.

Scenario 2. There exists a control input sequence so that it is possible to achieve correct fault isolation, but we cannot guarantee stability properties $x_i^{[m_i]}(k_d+T_i) \in F_i^{[m_i]}$ at the end of the Active Fault Isolation process for some $i \in \mathcal{M}^+$. Depending on the level of criticality of the considered application, the operator/decision system can decide whether to immediately disconnect the faulty subsystem or to continue with the local fault isolation without constraint (12) in order to understand the source of the problem. Again, after fault isolation we may decide to disconnect the faulty subsystem or we can use the additional knowledge to take a decision.

Scenario 3. It is not possible to find a local control input sequence so to achieve fault isolation (Problem (7) is not feasible even without constraint (12)). We can therefore decide to immediately disconnect the faulty subsystem in order to avoid or reduce the propagation of the fault effects in the network of the LSS. The unplugging of a subsystem is always possible, by implying only a contraction of the set W_j in the neighboring subsystems $j \in \mathcal{N}_i$, thus not spoiling neighbouring subsystems' state constraints.

The entire procedure is repeated if and when a new fault occurs.

VII. Simulation example

In this section, we show the effectiveness of the proposed decentralized FTC architecture on a power network system, composed of 5 generation areas connected through tie-lines, as described for Scenario 2 of the Appendix in [28]. The dynamics of each area, equipped with primary control and linearized around the equilibrium value for all variables, are described by the following continuous time model

$$\begin{aligned} \dot{\mathbf{x}}_i^{[m_i]} &= \mathbf{A}_{ii}^{[m_i]}\mathbf{x}_i^{[m_i]} + \mathbf{B}_i^{[m_i]}\mathbf{u}_i + \mathbf{L}_i^{[m_i]}\Delta P_{L_i} + \mathbf{w}_i^{[m_i]} \quad (14) \\ \mathbf{w}_i^{[m_i]} &= \sum_{j\in\mathcal{N}_i} \mathbf{A}_{ij}^{[m_i]}\mathbf{x}_j^{[m_i]} + \mathbf{d}_i \end{aligned}$$

where $\mathbf{x}_i^{[m_i]} = (\Delta\theta_i, \Delta\omega_i, \Delta P_{m_i}, \Delta P_{v_i})$ is the local state, $\mathbf{u}_i = \Delta P_{ref_i}$ is the control input of each area, and ΔP_{L_i} is the local power load and $\mathcal{N}_i$ is the set of neighbouring areas directly connected to subsystem i through tie-lines. More specifically, the matrices of system (14) are

$$\mathbf{A}_{ii}^{[m_i]} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -\frac{\sum_{j\in\mathcal{N}_i} P_{ij}}{2H_i^{[m_i]}} & -\frac{D_i}{2H_i^{[m_i]}} & \frac{1}{2H_i^{[m_i]}} & 0 \\ 0 & 0 & -\frac{1}{T_{t_i}} & \frac{1}{T_{t_i}} \\ 0 & -\frac{1}{R_i T_{g_i}} & 0 & -\frac{1}{T_{g_i}} \end{bmatrix}, \mathbf{B}_i^{[m_i]} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \frac{1}{T_{g_i}} \end{bmatrix},$$

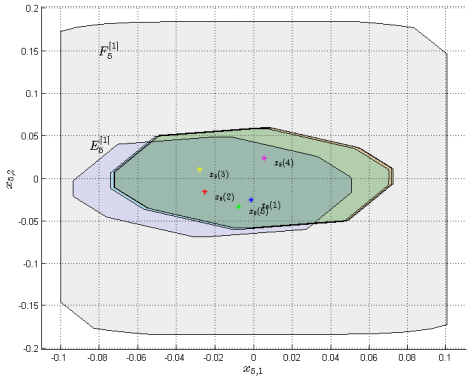

Fig. 3. Area 5. A 2D plot of the measurement $\mathbf{x}_5(k)$ (the blue star), the corresponding detection tube $E_5^{[1]}(k)$ centered in $\bar{\mathbf{x}}_5^{[1]}(k)$, and the domain of attraction $F_5^{[1]}$, for $k = 1,\ldots,5$, projected on the first two components.

$$\mathbf{A}_{ij}^{[m_i]} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ \frac{P_{ij}}{2H_i^{[m_i]}} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \mathbf{L}_i^{[m_i]} = \begin{bmatrix} 0 \\ -\frac{1}{2H_i^{[m_i]}} \\ 0 \\ 0 \end{bmatrix}$$

with the parameters and values as defined in [28] for the nominal model $m_i = 1$. We define three faulty models for the subsystem 5: $H_5^{[2]} = 2.5$, $H_5^{[3]} = 2.7$, $H_5^{[4]} = 2.95$. We consider similar values for the faulty inertia constants, thus making the isolation problem even more challenging. Each subsystem is subject to constraints on the state $\Delta\theta_i$ and on the input ΔP_{ref_i} as defined in Appendix B of [28]. We obtain discrete-time models as in (1) by discretizing model (14) with 1 sec sampling time. We assume the process noise $\mathbf{d}_i$ of the discretized model is bounded by a zonotope $D_i = \{0.01\mathbf{I}, 0\}$, with $\mathbf{I}$ the identity matrix. The matrices $\mathbf{K}_i^{[m_i]}$ of each subsystem have been computed, for all $m_i \in \mathcal{M}_i$ using the PnPMPC toolbox for MatLab [29]. The goal of the control is the design of the AGC layer control in order to restore the frequency in each area next to step loads.

At time $k_f = 3$ the inertia constant in area 5 is decreased from $H_5 = 12$ to $H_5 = 2.5$, corresponding to a reduction of about the 80% of the inertia. From an electrical point of view, this represents that the generation area has lost some local generators. In Figure 3, we illustrate the measurements and the tubes around the nominal state of the local subsystem 5, projected on the first two state components for $k = 1,\ldots,5$. It is possible to see that the state $\mathbf{x}_5(k)$ is contained in the tube $k = 1,\ldots,5$; therefore, there is no detection before $k = 6$. At time $k_d = 6$, the passive local set-based fault detection method is able to detect the fault. We can see in Figure 4 that the measurement $\mathbf{x}_5$ at time 6 lies outside[1] the corresponding detection tube $E_5^{[1]}$ centered in $\bar{\mathbf{x}}_5^{[1]}(6)$, and therefore we have detection. We then activate the local Active Fault Isolation tool. Problem (7) was solved using CPLEX. After $T_i = 1$ step, at time $k_{is} = 7$ the computed control input $\mathbf{u}_5(6) = 0.0767$ is able to separate the reachable sets of the different dynamics and to exclude all the faults but the correct one, i.e. $m_5 =$

[1]We use a 3D plot, projecting onto the first three components, to show that the measurement is not contained in the set.

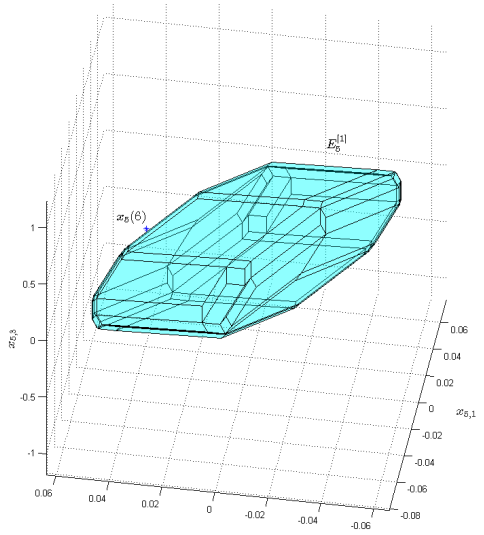

Fig. 4. Area 5 at time $k = 6$. A 3D plot of the measurement $\mathbf{x}_5(6)$ (indicated with a blue star) and the corresponding detection tube $E_5^{[1]}$ centered in $\bar{\mathbf{x}}_5^{[i]}(6)$, projected on the first three components.

2. It was then possible to reconfigure the local controller according to the identified novel dynamics. Since the state has 4 components, it is not possible to show the separation of the reachable sets in a plot.

VIII. Concluding Remarks

In this paper, a novel decentralized FTC scheme has been proposed for the monitoring of interconnected subsystems, using Active Fault Isolation. After fault detection, the proposed method allows to determine whether it is possible to correctly isolate the fault in a limited number of steps and to safely reconfigure local controllers or if the disconnection of the faulty subsystem is preferable in order to reduce the propagation of the effects of the fault. As a future work, we are going to investigate a distributed architecture and the presence of measurement noise and we will provide extensive simulation analysis.

References

[1] R. Patton, C. Kambhampati, A. Casavola, P. Zhang, S. Ding, and D. Sauter, "A generic strategy for fault-tolerance in control systems distributed over a network," *European Journal of Control*, vol. 13, no. 2-3, pp. 280–296, 2007.

[2] I. Shames, A. M. Teixeira, H. Sandberg, and K. H. Johansson, "Distributed fault detection for interconnected second-order systems," *Automatica*, vol. 47, no. 12, pp. 2757–2764, 2011.

[3] F. Boem, R. Ferrari, T. Parisini, and M. Polycarpou, "Distributed fault detection and isolation of continuous-time nonlinear systems," *European Journal of Control*, vol. 5-6, pp. 603–620, 2011.

[4] V. Reppa, M. M. Polycarpou, and C. G. Panayiotou, "Decentralized isolation of multiple sensor faults in large-scale interconnected nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 60, no. 6, pp. 1582–1596, 2015.

[5] F. Boem, R. M. G. Ferrari, C. Keliris, T. Parisini, and M. M. Polycarpou, "A distributed networked approach for fault detection of large-scale systems," *IEEE Transactions on Automatic Control*, 2017 (to appear).

[6] S. Riverso, F. Boem, G. Ferrari-Trecate, and T. Parisini, "Plug-and-play fault detection and control-reconfiguration for a class of nonlinear large-scale constrained systems (to appear)," *IEEE Transactions on Automatic Control*, 2017.

[7] A. E. Ashari, R. Nikoukhah, and S. L. Campbell, "Active robust fault detection in closed-loop systems: Quadratic optimization approach," *IEEE Transactions on Automatic Control*, vol. 57, no. 10, pp. 2532–2544, 2012.

[8] 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.

[9] S. M. Tabatabaeipour, "Active fault detection and isolation of discrete-time linear time-varying systems: a set-membership approach," *International Journal of Systems Science*, vol. 46, no. 11, pp. 1917–1933, 2015.

[10] M. Simandl and I. Puncochar, "Active fault detection and control: Unified formulation and optimal design," *Automatica*, vol. 45, no. 9, pp. 2052–2059, 2009.

[11] S. Riverso, M. Farina, and G. Ferrari-Trecate, "Plug-and-play decentralized model predictive control for linear systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 10, pp. 2608–2614, 2013.

[12] J. Jiang and X. Yu, "Fault-tolerant control systems: A comparative study between active and passive approaches," *Annual Reviews in Control*, vol. 36, no. 1, pp. 60–72, 2012.

[13] J. Prakash, S. Narasimhan, and S. Patwardhan, "Integrating model based fault diagnosis with model predictive control," *Ind. Eng. Chem. Res.*, vol. 44, no. 12, pp. 4344–4360, 2005.

[14] A. Yetendje, M. Seron, and J. De Dona, "Robust MPC design for fault tolerance of constrained multisensor linear systems," in *Conference on Control and Fault-Tolerant Systems*, 2010, pp. 752–758.

[15] X. Zhang, T. Parisini, and M. M. Polycarpou, "Adaptive fault-tolerant control of nonlinear uncertain systems: an information–based diagnostic approach," *IEEE Transactions on Automatic Control*, vol. 49, pp. 1259–1274, 2004.

[16] S. Sun, L. Dong, C. An, and W. Liu, "Fault-tolerant control design for linear systems with input constraints and actuator failures," in *Proc. of the Chinese Control and Decision Conference*, 2009, pp. 5278–5283.

[17] D. M. Raimondo, G. R. Marseglia, R. Braatz, and J. K. Scott, "Fault-tolerant model predictive control with active fault isolation," in *Conference on Control and Fault-Tolerant Systems (SysTol)*. IEEE, 2013, pp. 444–449.

[18] F. Xu, S. Olaru, V. Puig, C. Ocampo-Martínez, and S. Niculescu, "Sensor-fault tolerance using robust mpc with set-based state estimation and active fault isolation," in *IEEE Conference on Decision and Control*, 2014, pp. 4953–4958.

[19] S. Bodenburg and J. Lunze, "Plug-and-play reconfiguration of locally interconnected systems with limited model information," *IFAC-PapersOnLine*, vol. 48, no. 22, pp. 20–27, 2015.

[20] M. Staroswiecki and A. M. Amani, "Fault-tolerant control of distributed systems by information pattern reconfiguration," *International Journal of Adaptive Control and Signal Processing*, vol. 29, no. 6, pp. 671–684, 2015.

[21] D. Q. Mayne, M. M. Seron, and S. V. Raković, "Robust model predictive control of constrained linear systems with bounded disturbances," *Automatica*, vol. 41, no. 2, pp. 219–224, 2005.

[22] 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.

[23] J. K. Scott, G. R. Marseglia, L. Magni, R. D. Braatz, and D. M. Raimondo, "A hybrid stochastic-deterministic input design method for active fault diagnosis," in *IEEE Conference on Decision and Control*, 2013, pp. 5656–5661.

[24] S. Rakovic, E. Kerrigan, K. Kouramas, and D. Mayne, "Invariant approximations of the minimal robust positively invariant set," *IEEE Transaction on Automatic Control*, vol. 50, no. 3, pp. 406–410, 2005.

[25] D. Mayne, S. Rakovic, R. Findeisen, and F. Allgower, "Robust output feedback model predictive control of constrained linear systems," *Automatica*, vol. 42, no. 7, pp. 1217–1222, 2006.

[26] *IBM ILOG CPLEX V12.2 User's Manual for CPLEX*, 2012.

[27] D. Raimondo, R. Braatz, and J. Scott, "Active fault diagnosis using moving horizon input design," in *Proc. of the European Control Conference*, 2013, pp. 3131–3136.

[28] S. Riverso, "Distributed and plug-and-play control for constrained systems," Ph.D. dissertation, Università degli Studi di Pavia, 2014.

[29] S. Riverso, A. Battocchio, and G. Ferrari-Trecate, "PnPMPC: a toolbox for MatLab," 2012.