Distributed Fault-Tolerant Control of Large-Scale Systems: an Active Fault Diagnosis Approach

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

***Abstract*—The paper proposes a methodology to effectively address the increasingly important problem of distributed fault-tolerant control for large-scale interconnected systems. The approach dealt with combines, in a holistic way, a distributed fault detection and isolation algorithm with a specific tube-based model predictive control scheme. A distributed fault-tolerant control strategy is illustrated to guarantee overall stability and constraint satisfaction even after the occurrence of a fault. In particular, each subsystem is controlled and monitored by a local unit. The fault diagnosis component consists of a passive set-based fault detection algorithm and an active fault isolation one, yielding fault-isolability subject to local input and state constraints. The distributed active fault isolation module – thanks to a modification of the local inputs – allows to isolate the fault that has occurred avoiding the usual drawback of controllers that possibly hide the effect of the faults. The Active Fault Isolation method is used as a decision support tool for the fault tolerant control strategy after fault detection. The distributed design of the tube-based model predictive control allows the possible disconnection of faulty subsystems or the reconfiguration of local controllers after fault isolation. Simulation results on a well-known power network benchmark show the effectiveness of the proposed methodology.**

I. Introduction

The problem of monitoring and controlling large-scale networks of interconnected dynamic systems (LSSs for short) currently attracts a significant interest in academia and industry [1]. In this respect, the ever increasing demand for reliability, dependability and safety requires the design of control systems able to compensate the effects of critical and unpredictable changes in the LSS's dynamics (such as faults and malfunctions), while maintaining the performance of the controlled system at some acceptable level (see, for instance [2]). This is the well-known paradigm of Fault Tolerant Control (FTC).

In this paper, we illustrate a design approach of a distributed FTC scheme that guarantees the overall stability of a LSS even after the fault-occurrence. The proposed framework is based on the integration of a distributed active fault isolation scheme and a suitable distributed controller reconfiguration strategy.

This work has been supported by the European Union's Horizon 2020 research and innovation programme under grant agreement No 739551 (KIOS CoE). This work has also been conducted as part of the research project *Stability and Control of Power Networks with Energy Storage* (STABLENET) which is funded by the RCUK Energy Programme (contract no: EP/L014343/1).

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

A. J. Gallo is with the Dept. of Electrical and Electronic Engineering at the Imperial College London, UK. (alexander.gallo12@imperial.ac.uk)

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

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

A. State of the Art and Motivations

In the literature, FTC methodologies are often subdivided into two main categories (see, for example, the survey [3]): *passive FTC* and *active FTC*. In qualitative terms, passive FTC refers to the design of controllers that are robust to the occurrence of potential faults without any reconfiguration or modification of the control system. Passive FTC techniques are well suited in low-dimensional applications in which the possibility of modifying the control system is not allowed, but their effectiveness in applications is rather limited.

In active FTC techniques (see, for instance, [4], [5], [6], [7]), a monitoring component is included in the control scheme providing a run-time Fault Detection and Isolation (FDI) decision about the possible occurrence of a fault or malfunction on the basis of input-output measurements. After fault detection, the controller may be suitably reconfigured according to the diagnosis decision to recover an acceptable performance of the closed-loop system. With a few exceptions [6], [7], [8], classical active FTC techniques show good performance only in scenarios where faults are detected and isolated correctly and instantaneously (see, for instance [4], [5]). These scenarios typically require assuming the absence of process and measurement disturbances [9], [10], [11]. This assumption is rather unrealistic in real use-cases, thus causing delays and errors in FDI, in turn possibly leading to instability, violation of state constraints, and the inability to implement the suitable controller after fault isolation [12].

Indeed, a major issue affecting most active FTC schemes relates to the possibly *conflicting* dynamic behaviors of the FDI scheme and the reconfigurable controller. More specifically, the feedback controller may hide the presence of faults by compensating their effects (see as example the simulation analysis in [13]), thus making the FDI task much more difficult or even impossible [14], [15] – as is well known, a similar issue affects several closed-loop identification techniques in poor excitation scenarios.

A radically different context arises in application use-cases allowing to affect the closed-loop dynamics by acting at run-time on the control inputs. This paves the way to the so-called *active FDI methodologies*. Active FDI approaches consist in suitably modifying the control input to improve fault detectability and isolability capabilities [16], [17], [18], [19], [20], [21], [22], [23]. This allows to possibly reduce detection and isolation time. The typical main limitation of active FDI techniques concerns high computational cost and complexity [24], [25]. This drawback restricts the applicability

of this approach to low-dimensional systems [25], [26], [27], [28], [29], even though some approaches have been suggested in the literature to alleviate the computational complexity (see as example [23]).

Coping with the above-mentioned computational complexity in the context of LSSs, dealt with in this paper, requires a *distributed approach*. Differently from currently available distributed/decentralized architectures for FDI (see as example [30], [31], [32], [33], [34], [35], [36]), in this paper the active FDI scenario is considered.

B. Objectives and Contributions

The main objective of the paper is the design of a *distributed active FTC* architecture for linear LSSs with bounded disturbances, where the LSS is monitored by a network of *local fault diagnosers*. Each diagnoser is based on a local *passive fault detection* scheme and a local *active fault isolation* tool. The network of diagnosers is integrated with a distributed tube-based Model Predictive Control (MPC) scheme (based on [37], [38]). After fault detection, the active fault isolation component aims at i) generating a control sequence able to guarantee the local isolation of the fault, while satisfying state constraints and stability properties, and at ii) subsequently allowing the reconfiguration of the local controllers according to a suitable decision-making process. The use of active fault isolation allows to possibly improve performance with respect to traditional passive approaches, in terms of isolation time and fault isolability. We take advantage of the scalable design of the local controllers to allow the possible disconnection of faulty subsystems when the local control reconfiguration is not feasible. In this way, the proposed distributed FTC strategy guarantees stability and constraint satisfaction for the overall LSS at any time, even after the occurrence of the fault. This approach differs from recent distributed/decentralized FTC techniques such as [34], [39], [40], [13] by exploiting the active FDI scenario.

Summing up, the main contributions of the paper are[1]:

- the design of a distributed and scalable Active Fault Isolation framework for large-scale interconnected systems; this represents a more challenging scenario, requiring to take into account the possibly unknown or uncertain influences between subsystems;
- the development of a distributed active FTC strategy for the reconfiguration of the network of systems and controllers, guaranteeing the overall stability of the LSS and constraint satisfaction even after the occurrence of a fault;
- a FTC strategy, where the opportunity to off-line explicitly solve the optimization problem for local active fault isolation permits to support decisions during the online monitoring and fault-tolerant control of the LSS (see Section V);
- the isolation of classes of faults where the parameters characterizing each faulty model are uncertain and may vary within a defined range of values. Furthermore, the possible presence of measurement noise is taken into account (Section VI) and extensive simulation analysis on a Power Network System benchmark are provided.

[1]Preliminary results have been presented in [41] in a decentralized scenario.

C. Organization of the Paper

In Section II, the considered problem is introduced. In Section III the adopted distributed control architecture is presented, while in Section IV we first propose a passive set-based fault detection method and then the active fault isolation approach. After that, the FTC strategy is explained in Section V. In Section VI we offer some possible directions in which the results can be extended. Finally, simulation results on a Power Network System are presented in Section VII and some conclusions are given in Section VIII.

II. Problem Formulation

A. System, model and features

Consider a discrete-time affine large scale system composed of N subsystems. Each subsystem $i \in \mathscr{N} = \{1,\dots,N\}$ obeys one of n_i possible dynamics (all known). When model $m_i \in \mathscr{M}_i = \{1,\cdots,n_i\}$ is active, the subsystem i is governed by the following set of equations

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

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

where $\mathbf{x}_i(k) \in \mathbb{R}^{n_{x_i}}$, $\mathbf{u}_i^{[m_i]}(k) \in \mathbb{R}^{n_{u_i}}$ denote respectively the states and the input vectors of subsystem i, with $\mathbf{x}_i(0) \in \mathbb{R}^{n_{x_i}}$ the state initial condition. The term $\mathbf{z}_i^{[m_i]}(k) \in \mathbb{R}^{n_{x_i}}$ accounts for the coupling with neighboring subsystems and the presence of disturbances $\mathbf{d}_i(k)$, where the set of neighbors 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 $\mathbf{A}^{[m]}$, where this latter represents the dynamic matrix of the overall system, with $m = [m_1,\dots,m_N]$. For each $i \in \mathscr{N}$, we assume $m_i = 1$ represents the nominal dynamics, while the other models describe possible faulty dynamics. We assume that the switch between nominal and faulty dynamics happens in an abrupt way. For the sake of notation simplicity, in the following the results will be presented assuming that each $m_i \neq 1$ represents a specific fault with known parameters, but everything can simply be extended to the case that each model is a class of faults described by interval matrices. The constant vector $\mathbf{r}_i^{[m_i]}$ is used to model constant bias. The following assumptions are required:

Assumption 1: The disturbance $\mathbf{d}_i(k)$ is bounded by a known set D_i, i.e. $\mathbf{d}_i(k) \in D_i, \forall k, \forall i$.

Assumption 2: The considered LSS allows the physical unplugging of subsystems.

Remark 1: The term Plug-and-Play denotes the property of distributed control and monitoring architectures to allow the plug-in/unplugging of some subsystems only requiring local operations and tests for the reconfiguration. Examples

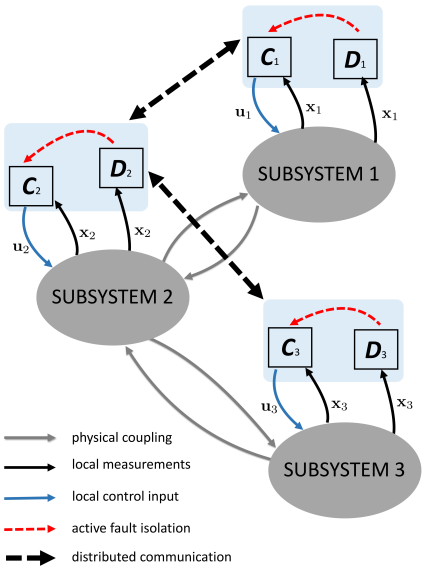

Fig. 1. The proposed distributed architecture. The subsystems are physically interconnected. Each subsystem is controlled by a local controller C_i and monitored by a local diagnoser D_i, both taking measurements from the local subsystems. Local controllers and diagnosers may communicate with neighboring subsystems in a distributed way. After fault detection, the active fault isolation tool may compute an input control sequence to allow the isolation of the fault.

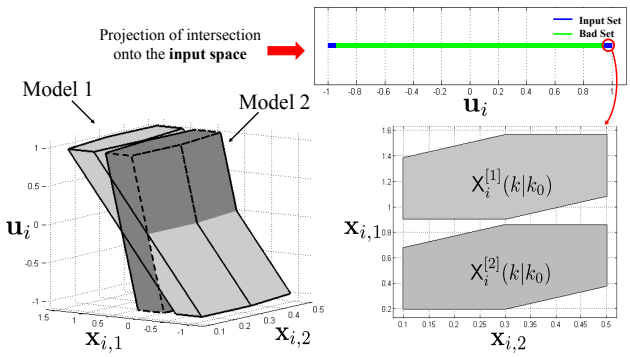

Fig. 2. Projection of the local state reachable sets onto the joint local state-input space (left). Projection of the intersection of the polytopes on the left into the input space (right, top). Choice of the local inputs to obtain state reachable sets separability (right bottom).

of systems satisfying Assumption 2 include water distribution networks, power networks, microgrids, etc. We refer the Reader to [37] for details about Plug-and-Play approaches.

B. A Glimpse on the Active FTC Approach

In order to obtain scalable control and monitoring procedures, each subsystem is governed by a local controller and monitored by a local fault diagnoser, as illustrated in Figure 1. Each local controller (see Section III) is subject to local input and state constraints

$$\mathbf{x}_i(k) \in X_i, \quad \mathbf{u}_i^{[m_i]}(k) \in U_i,$$

the influence of bounded neighboring subsystems states

$$\mathbf{x}_j(k) \in X_j, \quad j \in \mathscr{N}_i^{[m_i]},$$

and is robust to bounded disturbances (see Section III).

For each $i \in \mathscr{N}$, sets X_i, U_i, D_i are all zero-centered zonotopes [42] known a priori.

It is worth noting that the design of the local controllers relies on the knowledge of the sets X_j from the neighboring subsystems $j \in \mathscr{N}_i^{[m_i]}$.

MPC is a well suited technique to control systems subject to input and state constraints. In the following, we rely on the distributed approach presented in [38]. This scheme guarantees in a distributed way robust stability and constraint satisfaction for the overall system. Moreover, this approach is suitable to be integrated with an active fault diagnosis approach for FTC.

Each subsystem is monitored in healthy conditions by a local passive set-based fault detection method, following a similar approach to the one proposed in [43] in the centralized case. When a fault is detected in a local subsystem at time k_d, the related controller is put on stand-by to avoid that the feedback controller hides the effect of the fault, and a local active FDI procedure is triggered (Section IV-B). To enhance fault isolation, Active FDI aims to determine which dynamics subsystem i is subject to, by injecting a minimally harmful (in length and/or norm[2]) sequence $(\mathbf{u}_i^{[m_i]}(k_d), \cdots, \mathbf{u}_i^{[m_i]}(k_d + T_i - 1))$ able to guarantee that any possible state (or state sequence) of subsystem i at time $k_d + T_i$ is consistent with only one $m_i \in \mathscr{M}_i$ (see Figure 2). 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. Moreover, if feasible, the state is constrained to suitable sets, so that the local controllers can be reconfigured after fault isolation according to the identified model (see Section V). Note that, by pursuing a fast fault isolation, the advantage of active FDI, when compared to a passive FDI approach, is that it increases the chances of safely reconfiguring the controllers after isolation without losing stability. In fact, the fault could drive the state outside the feasibility area of the controller.

Assumption 3: In each subsystem, it is assumed that the diagnosis is fast enough to avoid the switching between models during $[k_d, \cdots, k_d + T_i]$.

Once the fault is isolated, the local controller is reconfigured in order to still guarantee the stability and constraint satisfaction of the overall system. Summing up, the main contribution of the paper is the distributed FTC strategy illustrated in Section V, which, based on local properties, guarantees that the presence of a fault does not compromise the stability of the network of interconnected systems.

Remark 2: The adoption of a distributed and scalable architecture allows to reduce the computational complexity of the proposed method, which depends linearly only on the number of neighboring subsystems.

[2]In this way, the action of the controller for Active Fault Isolation reasons is reduced in terms of time and magnitude of the input signal. High values of input signals could be not feasible nor safe for the system. Moreover, in general, it is better to minimize the isolation time in order to achieve a fast diagnosis decision and a prompt reconfiguration of the controllers to guarantee stability and constraint satisfaction.

C. Definitions

1) Basic notation: In the following, a tilde is used to indicate sequences of vectors associated with the model (1)-(2). More specifically, when referring to $\tilde{\mathbf{u}}_i^{[m_i]}(l:k), \tilde{\mathbf{z}}_i^{[m_i]}(l:k)$, the notation stands for $\tilde{\mathbf{u}}_i^{[m_i]}(l:k)=(\mathbf{u}_i^{[m_i]}(l),\ldots,\mathbf{u}_i^{[m_i]}(k-1))$, $\tilde{\mathbf{z}}_i^{[m_i]}(l:k)=(\mathbf{z}_i^{[m_i]}(l),\ldots,\mathbf{z}_i^{[m_i]}(k-1))$, while $\tilde{\mathbf{x}}_i(l:k) = (\mathbf{x}_i(l),\ldots,\mathbf{x}_i(k))$, for $\tilde{\mathbf{x}}_i(l:k)$. For a generic variable σ, the notation $\tilde{\sigma}(l:k|l)$ indicates that the sequence is computed at time l. For a set W, the notation $\tilde{W}_{\{k\}}=W\times\ldots\times W$ is used to indicate its k-th cartesian product.

2) Reachable sets: For each subsystem i, the state of model m_i, k-steps ahead, is given by the function $\phi_{i\{k\}}^{[m_i]}\left(\tilde{\mathbf{u}}_i^{[m_i]}(0:k),\mathbf{x}_i(0),\tilde{\mathbf{z}}_i^{[m_i]}(0:k)\right)$ 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. Given an initial condition $\mathbf{x}_i(k_0)$, a sequence $\tilde{\mathbf{u}}_i^{[m_i]}(k_0:k|k_0)$ and a set $\tilde{Z}_{i\{k-k_0\}}^{[m_i]}$ (which can be computed on the basis of sets X_j and D_i) the state *reachable set* at time k is defined as

$$\begin{aligned}&\mathsf{X}_i^{[m_i]}\left(\tilde{\mathbf{u}}_i^{[m_i]}(k_0:k|k_0),\mathbf{x}_i(k_0),\tilde{Z}_{i\{k-k_0\}}^{[m_i]}\right)\\&=\left\{\phi_{i\{k-k_0\}}^{[m_i]}\left(\tilde{\mathbf{u}}_i^{[m_i]}(k_0:k|k_0),\mathbf{x}_i(k_0),\tilde{\mathbf{z}}_i^{[m_i]}(k_0:k)\right):\right.\\&\qquad\left.\tilde{\mathbf{x}}_j(k_0:k)\in\tilde{X}_{j\{k-k_0\}},\forall j\in\mathscr{N}_i^{[m_i]},\ \tilde{\mathbf{d}}_i(k_0:k)\in\tilde{D}_{i\{k-k_0\}}\right\}.\end{aligned}$$

When clear from the context, the arguments of maps will be omitted, and with some abuse of notation the reachable sets will be denoted as $\mathsf{X}_i^{[m_i]}(k|k_0)$.

III. Scalable control strategies suitable for distributed FTC

The proposed FTC method assumes that in nominal conditions each subsystem is equipped with a local tube-based robust MPC controller which is designed, for each $i\in\mathscr{N}, m_i\in\mathscr{M}_i$, based on [38]. More specifically, in order to allow the design of the distributed Active Fault Isolation method in Section IV-B and of the FTC strategy for LSSs in Section V, the following notable features are required for the control architecture:

- Thanks to the distributed framework, leading to local low-dimension and the choice of a tube-based MPC control scheme, robust to the coupling with neighboring subsystems and to the disturbances, it is possible to explicitly compute the feasibility domains for the local controllers, i.e. the domain sets where stability and constraints satisfaction are guaranteed. This is a fundamental ingredient which will be used for the reconfiguration of local controllers after fault isolation if the local Active Fault Isolation problem is feasible (see (15a)-(15g) in Section IV-B and Assumption 4 below). As it will be later clarified, this will allow to guarantee the stability of the LSS even after the occurrence of a fault.
- The Plug-and-play feature (see [37] for details) is used to allow the possible disconnection of faulty subsystems, in the case that the presence of the fault may compromise local and/or global stability. In fact, if fault isolation is not feasible, or a safe control reconfiguration not possible, the disconnection of the faulty subsystem may avoid or reduce the propagation of the faults effect in the LSS. In this case (see Section V for details about the FTC strategy), at most neighboring controllers and diagnosers may be reconfigured.

The above features motivate our choice for the control architecture briefly summarized in Section III-A.

Assumption 4: The pair $(\mathbf{A}_{ii}^{[m_i]},\mathbf{B}_i^{[m_i]})$ is stabilizable for all $i\in\mathscr{N}$, $m_i\in\mathscr{M}_i$.

This assumption is only required for the sake of presentation simplicity, in order to allow the reconfiguration of the controllers after fault isolation. In this case, the local control laws are synthesized off-line for every model $m_i\in\mathscr{M}_i$. In the case the assumption does not hold for some faulty models $m_i\in\bar{\mathscr{M}}_i\subseteq\mathscr{M}_i^+\equiv\mathscr{M}_i\backslash\{1\}$, then the fault-tolerant control architecture can be designed anyway, requiring the unplugging of the faulty subsystem if the local controller cannot be reconfigured (see Section V for details).

The design of the control architecture in nominal conditions is not the main focus of this paper. The selected approach based on [38] is briefly described in the following section in order to introduce some notation and base the stability properties of the proposed FTC. Note that the approach can be used in a decentralized or in a distributed way, depending on the availability of communication resources.

A. Tube-Based MPC

According to a scalable tube-based robust MPC approach, the control action for each $i\in\mathscr{N}$ is given by the sum of two terms: i) a nominal input $\overline{\mathbf{u}}_i^{[m_i]}(k)$, obtained by solving, at each time step, a Finite Horizon Optimal Control Problem (FHOCP) [44] subject to the nominal model

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

and ii) a linear feedback term

$$\mathbf{K}_{ii}^{[m_i]}\left(\mathbf{x}_i(k)-\overline{\mathbf{x}}_i^{[m_i]}(k)\right)+\sum_{j\in\mathscr{N}_i}\delta_{ij}\mathbf{K}_{ij}^{[m_i]}\mathbf{x}_j(k),$$

designed so that $\mathbf{x}_i$ tracks the prediction of nominal model (3), where $\mathbf{K}_{ii}^{[m_i]}\in\mathbb{R}^{n_{u_i}\times n_{x_i}}$, $\mathbf{K}_{ij}^{[m_i]}\in\mathbb{R}^{n_{u_i}\times n_{x_j}}$ and $\delta_{ij}\in\{0,1\}$, $i,j\in\mathscr{N}$. The parameters δ_{ij} can be chosen by the designer to select the subsystems from which the local controller is receiving information. More specifically, when $\delta_{ij}=1\quad\forall i\in\mathscr{N},\ \forall j\in\mathscr{N}_i^{[m_i]}$, then the communication network coincides with the coupling graph, resulting in a distributed scenario. On the other hand, if $\delta_{ij}=0\quad\forall i\in\mathscr{N},\ \forall j\in\mathscr{N}_i^{[m_i]}$, then the control scheme is completely decentralized.

Assumption 5: Matrices $\mathbf{K}_{ii}^{[m_i]}$ and $\mathbf{K}_{ij}^{[m_i]}$ can be locally designed as in [38] (Algorithm 1) to guarantee the overall stability of the LSS.

The resulting tube-based MPC feedback law for each subsystem is

$$\begin{aligned}\kappa_i^{[m_i]}(\bar{\mathbf{x}}_i^{[m_i]}(k))=\bar{\mathbf{u}}_i^{[m_i]}(k)+\mathbf{K}_{ii}^{[m_i]}(\mathbf{x}_i(k)-\overline{\mathbf{x}}_i^{[m_i]}(k))\\+\sum_{j\in\mathscr{N}_i^{[m_i]}}\delta_{ij}\mathbf{K}_{ij}^{[m_i]}\mathbf{x}_j(k).\end{aligned} \tag{4}$$

As previously stated, the nominal input $\overline{\mathbf{u}}_i^{[m_i]}(k)$ is obtained, at each time step, by applying only the first element of the FHOCP solution (receding horizon scheme). In order to obtain a robust MPC controller, besides the standard elements [44] (nominal dynamics (3), a quadratic cost, terminal state and terminal penalty satisfying standard assumptions in order to obtain recursive feasibility and stability) the FHOCP requires extra constraints which are now recalled (see [38] for further details).

Denote with $\mathbf{e}_i^{[m_i]}(k) \equiv \mathbf{x}_i(k) - \overline{\mathbf{x}}_i^{[m_i]}(k)$ the tracking error between the real state $\mathbf{x}_i(k)$, obtained by (1) applying (4), and the nominal state $\overline{\mathbf{x}}_i^{[m_i]}(k)$ (solution of the nominal model (3) with nominal input $\overline{\mathbf{u}}_i^{[m_i]}(k)$). The tracking error dynamics can be modelled as

$$\mathbf{e}_i^{[m_i]}(k+1) = \mathbf{A}_{K_{ii}}^{[m_i]} \mathbf{e}_i^{[m_i]}(k) + \mathbf{w}_i^{[m_i]}(k), \tag{5}$$

where, according to Ass. 5, $\mathbf{A}_{K_{ii}}^{[m_i]} \equiv \mathbf{A}_{ii}^{[m_i]} + \mathbf{B}_i^{[m_i]} \mathbf{K}_{ii}^{[m_i]}$ is designed to be Schur, and

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

Note that

$$\mathbf{w}_i^{[m_i]}(k) \in W_i^{[m_i]} \equiv \bigoplus_{j \in \mathscr{N}_i^{[m_i]}} (\mathbf{A}_{ij}^{[m_i]} + \delta_{ij} \mathbf{B}_i^{[m_i]} \mathbf{K}_{ij}^{[m_i]}) X_j \oplus D_i. \tag{6}$$

Thanks to the stability of $\mathbf{A}_{K_{ii}}^{[m_i]}$ and the boundedness of $W_i^{[m_i]}$ (resulting from the bounds $X_j, j \in \mathscr{N}_i^{[m_i]}$, and D_i), it is possible to prove that there exists a robust positively invariant set $E_i^{[m_i]} \subset \mathbb{R}^{n_{x_i}}$ such that $\mathbf{A}_{K_{ii}}^{[m_i]} E_i^{[m_i]} + W_i^{[m_i]} \subset E_i^{[m_i]}$. 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 (5) satisfies $\mathbf{e}_i^{[m_i]}(k) \in E_i^{[m_i]}$, $\forall k \in \mathbb{N}$, being $E_i^{[m_i]}$ a robust positively invariant set that can be computed as described in [45].

Finally, the extra constraints required by the FHOCP in order to obtain a tube-based robust MPC controller are the following:

- Initial constraint

$$\mathbf{x}_i(k) - \bar{\mathbf{x}}_i^{[m_i]}(k) \in E_i^{[m_i]}, \ \forall k \in \mathbb{N}.$$

- Tightened state and input constraints

$$\overline{U}_i^{[m_i]} \equiv U_i \ominus (\mathbf{K}_{ii}^{[m_i]} E_i^{[m_i]} \bigoplus_{j \in \mathscr{N}_i^{[m_i]}} \delta_{ij} \mathbf{K}_{ij}^{[m_i]} X_j), \tag{7}$$

$$\overline{X}_i^{[m_i]} \equiv X_i \ominus E_i^{[m_i]}. \tag{8}$$

Remark 3: Note that, in order to the FHOCP Problem to be feasible, it is necessary that both $\overline{U}_i^{[m_i]}$ and $\overline{X}_i^{[m_i]}$ are non-empty, i.e. the effect of the disturbance and the coupling between subsystems is required to be sufficiently small (see [44] for reference).

Let $\bar{F}_i^{[m_i]}$ denote the set of initial conditions $\bar{\mathbf{x}}_i^{[m_i]}$ for which the FHOCP problem is feasible. We define $\bar{F}_i^{[m_i]}$ as the local *feasibility domain* for the unperturbed dynamics. Such set is a polyhedron. Note that $\bar{\mathbf{u}}_i^{[m_i]}(k)$ is continuous and polyhedral piecewise affine (PPWA) over $\bar{F}_i^{[m_i]}$. This means that it is defined over a non-overlapping polyhedral partitioning of $\bar{F}_i^{[m_i]}$ and, over each partition $P_{i,r}^{[m_i]}$, $r \in \{1, \cdots, n_{r_i}^{[m_i]}\}$, the solution is affine

$$\bar{\mathbf{u}}_i^{[m_i]}(k) = \mathscr{K}_i^{[m_i]}(\bar{\mathbf{x}}_i^{[m_i]}(k)) = \Gamma_r \bar{\mathbf{x}}_i^{[m_i]}(k) + \mathrm{g}_r, \text{ if } \bar{\mathbf{x}}_i^{[m_i]}(k) \in P_{i,r}^{[m_i]}.$$

Denote $F_i^{[m_i]} = \bar{F}_i^{[m_i]} \oplus E_i^{[m_i]}$. $F_i^{[m_i]}$ is again a polyhedron which can be expressed by a set of linear inequalities.

Let us define $F^{[m]} = F_1^{[m_1]} \times \cdots \times F_N^{[m_N]}$, $E^{[m]} = E_1^{[m_1]} \times \cdots \times E_N^{[m_N]}$, $D^{[m]} = D_1^{[m_1]} \times \cdots \times D_N^{[m_N]}$, and denote with $\mathbf{x}$ the column vector collecting the state vectors $\mathbf{x}_i$, $i = 1, \ldots, N$. The scalable tube based MPC summarized above guarantees the robust stability to the set $E^{[m]}$ and constraint satisfaction for the overall LSS: if $\mathbf{x}(0) \in F^{[m]}, \forall i \in 1, \ldots, N$, then $\mathbf{x}(k) \in F^{[m]}, \forall k \in \mathbb{N}$, and $\lim_{k \to \infty} d(\mathbf{x}(k), E^{[m]}) \to 0$ [38].

Remark 4: The optimal value function $V(\bar{\mathbf{x}}_i^{[m_i]}(k))$ is convex, continuous and piecewise quadratic over $\bar{F}_i^{[m_i]}$ whose level sets are piecewise ellipsoidal invariant sets for the system (see [46] for further details). The feasibility set, value function and optimizer can be computed explicitly using, for example, the MPT toolbox [47].

Remark 5: The presence of communication between neighboring subsystems enables the design of distributed controllers which can exploit the knowledge (or partial knowledge) of some state variables of the neighbors. When compared to a fully decentralized approach, this knowledge can facilitate the stabilization of the overall system. Besides, in a distributed framework, the resulting disturbance $\mathbf{w}_i^{[m_i]}$ (Eq. (6)) is in general going to be smaller than the original $\mathbf{z}_i^{[m_i]}$, thus enhancing the performance of the proposed set-based fault diagnosis approach (see Section IV). More specifically, as it will be clear in the following, a smaller disturbance set implies a less conservative passive fault detection and increases the feasibility of the fault isolation problem.

Summing up, the considered scalable tube-based MPC guarantees global stability of the LSS in nominal conditions. Furthermore, thanks to the local low-dimension of the subsystems it is possible to explicitly compute the local feasible domains $F_i^{[m_i]}$, which will be used by the proposed FTC scheme (see Sections IV-B and V) to guarantee stability and constraint satisfaction for the LSS even after the occurrence of a fault. More specifically, after fault detection, the goal of the Active Fault Isolation is to design a local input sequence able to isolate the occurred fault, remaining in the local feasibility domains. In this way, it will be possible to reconfigure the local controller according to the isolated model and to continue guaranteeing local and global stability.

IV. Robust Fault Detection and Isolation

This section presents the distributed fault detection and isolation 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 $\mathbf{u}_i^{[1]}(k)$ is determined using the control law $\kappa_i^{[1]}$. At the same time, passive fault detection is done using a set-based approach as described in Section IV-A. After fault detection, in the interval $[k_d, k_{is}]$, active fault isolation is carried out, as described in Section IV-B.

A. Local Passive Fault Detection

According to the tube based MPC approach described in Section III-A, 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 or distributed way (depending on the available resources), the presence of a possible fault in subsystem i. At each time step $k+1$, given the nominal state $\bar{\mathbf{x}}_i^{[1]}(k+1)$ obtained by solving the FHOCP at time k, we compute the error $\mathbf{e}_i^{[1]}(k+1)$ between $\bar{\mathbf{x}}_i^{[1]}(k+1)$ and the real state $\mathbf{x}_i(k+1)$.

Fault detection sufficient condition. If, at any $k+1>0$,

$$\mathbf{e}_i^{[1]}(k+1) \notin E_i^{[1]}, \tag{9}$$

then, the nominal model $m_i = 1$ is not consistent with the behavior of the subsystem, i.e. a fault has occurred in subsystem i.

Structural detectability has been widely studied in the centralized case [43]. A complete detectability analysis of the proposed method is out of the scope of this paper, but it is worth noting that if a fault is not detectable, then it will not compromise the stability of the system thanks to the proposed FTC framework. On the other side, there is an important issue which needs to be addressed. If a fault in subsystem i leads to the violation of local constraints X_i, then, the stability of the overall system is compromised. The following theorem provides conditions to avoid, within the Plug-and-Play framework, this situation.

Theorem 1: Define $\mathscr{M}_i^+ \equiv \mathscr{M}_i \backslash \{1\}$. Assume there exists a polyhedral set $\bar{S}_i^{[1]} \subseteq \bar{F}_i^{[1]}$ which is invariant for the nominal dynamics (3) and such that, for all $m_i \in \mathscr{M}_i^+$

$$A_{ii}^{[m_i]}\left(\bar{S}_i^{[1]} \oplus E_i^{[1]}\right) \oplus B_i^{[m_i]}\left(\mathscr{K}_i^{[1]}(\bar{S}_i^{[1]}) \oplus K_{ii}^{[1]} E_i^{[1]}\right) \bigoplus_{j \in \mathscr{N}_i^{[m_i]}} \left(\mathbf{A}_{ij}^{[m_i]} + \delta_{ij} B_i^{[m_i]} \mathbf{K}_{ij}^{[1]}\right) X_j \oplus D_i + r_i^{[m_i]} \subseteq X_i. \tag{10}$$

Then, the restriction of the operation of each subsystem (2) to $\bar{S}_i^{[1]} \oplus E_i^{[1]}$ rather than $F_i^{[1]}$ guarantees that the occurrence of any fault $m_i \in \mathscr{M}_i^+$ cannot compromise the stability of the overall system.

Proof: The nominal invariance of $\bar{S}_i^{[1]}$ guarantees, if $\mathbf{x}_i \in \bar{S}_i^{[1]} \oplus E_i^{[1]}$, recursive feasibility and convergence to $E_i^{[1]}$ for any fault which can be interpreted as disturbance (i.e. whose effect is not distinguishable from $e_i^{[1]} \in E_i^{[1]}$) [44]. In the opposite case, two scenarios are possible:

- $\mathbf{x}_i(k+1) \in \bar{S}_i^{[1]} \oplus E_i^{[1]}$ but $e_i^{[1]}(k+1) \notin E_i^{[1]}$. Then a fault is detected and can be either isolated (using the procedure described in the following section) or the system unplugged. In any case, the stability of the overall system does not get compromised since the local subsystem does not leave X_i.
- $\mathbf{x}_i(k+1) \notin \bar{S}_i^{[1]} \oplus E_i^{[1]}$. In this case, in order to not compromise the stability of the overall system, it is necessary to guarantee that $\mathbf{x}_i(k+1) \subseteq X_i$ for any fault $m_i \in \mathscr{M}_i^+$. Recall that the nominal input $\bar{\mathbf{u}}_i^{[1]}(k)$ can be expressed by the mapping $\mathscr{K}_i^{[1]}(\bar{\mathbf{x}}_i^{[1]})$ and the input for the perturbed system is given by (4) with $m_i = 1$. Note that, the FHOCP has among its constraints $\mathbf{x}_i(k) - \bar{\mathbf{x}}_i^{[1]}(k) \in E_i^{[1]}$. Now, if the FHOCP was feasible at time k, $\bar{\mathbf{x}}_i^{[1]}(k) \in \bar{S}_i^{[1]}$. Then, taking any possible dynamics of the i-th subsystem (2) in closed-loop with (4), and replacing any occurrence of $\bar{\mathbf{x}}_i^{[1]}(k)$ with $\bar{S}_i^{[1]}$, $\mathbf{x}_i(k) - \bar{\mathbf{x}}_i^{[1]}(k)$ with $E_i^{[1]}$, $\mathbf{x}_j(k)$ with X_j and $\mathbf{d}_i$ with D_i, leads exactly to condition (10) which guarantees that the faulty dynamics will not leave the space X_i. Under the assumption of a Plug-and-Play scenario, when $\mathbf{x}_i(k+1) \in X_i \setminus (\bar{S}_i^{[1]} \oplus E_i^{[1]})$ it is always possible to unplug the i-th subsystem so to avoid violation of the state constraints for the neighboring subsystems and, consequently, preserve the overall stability. ■

Remark 6: Finding polyhedral invariant sets within $\bar{F}_i^{[1]}$ for the nominal dynamics can be obtained by following the procedure provided in, e.g. [48]. An iterative procedure can be applied, using for example bisection, in order to find the biggest invariant set satisfying (10). Note that, using e.g. the MPT toolbox, it is possible to compute explicitly mapping $\mathscr{K}_i^{[1]}(\bar{\mathbf{x}}_i^{[1]})$ and therefore verify (10) through set inclusions.

Remark 7: Note that (10) is quite different from requiring robust stability in presence of faults. Indeed it is a much weaker condition which guarantees only that in one step there will not be any violation of the local state constraints. Note also that invariance of set $\bar{S}_i^{[i]}$ is necessary to guarantee the recursive feasibility of condition (10).

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, dealing with conservative results. For this reason, in the following, we suggest to use a distributed version of the active FDI scheme proposed in [19].

B. Local Active Fault Isolation

Suppose condition (9) is verified at time k_d, indicating that a fault occurred at some time 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 complete. At time k_d, the active model $m_i \neq 1$ is unknown.

After fault detection, the control law defined in (4) is deactivated and the following input strategy

$$\mathbf{u}_i^{[m_i]}(k) = \bar{\mathbf{u}}_i(k) + \sum_{j \in \mathscr{N}_i} \delta_{ij} \mathbf{K}_{ij}^{[m_i]} \mathbf{x}_j(k) \tag{11}$$

is used for isolation, where $\bar{\mathbf{u}}_i(k)$ will be designed according to (15a)-(15g) to separate the different possible faulty models. Note that, the local feedback component has been removed since feedback compensation could make isolation more difficult. On the other side, as the influence of the neighbors is treated as a disturbance to the local dynamics, it continues to be minimized through $\mathbf{K}_{ij}^{[m_i]}$, in order to tighten the uncertainty sets $W_i^{[m_i]}$.

By using (11), system (1)-(2) can be rewritten as

$$\begin{aligned} \mathbf{x}_i(k+1) &= \mathbf{A}_{ii}^{[m_i]} \mathbf{x}_i(k) + \mathbf{B}_i^{[m_i]} \bar{\mathbf{u}}_i(k) + \mathbf{w}_i^{[m_i]}(k) + \mathbf{r}_i^{[m_i]} \\ \mathbf{w}_i^{[m_i]}(k) &= \sum_{j \in \mathscr{N}_i^{[m_i]}} (\mathbf{A}_{ij}^{[m_i]} + \delta_{ij} \mathbf{B}_i^{[m_i]} \mathbf{K}_{ij}^{[m_i]}) \mathbf{x}_j(k) + \mathbf{d}_i(k). \end{aligned} \tag{12}$$

With a slight abuse of notation we redefine

$$\phi_{i\{k\}}^{[m_i]}(\tilde{\tilde{\mathbf{u}}}_i(0:k),\mathbf{x}_i(0),\tilde{\mathbf{w}}_i^{[m_i]}(0:k))$$

as the solution map related to (12). Similarly, we redefine the state reachable sets according to system (12)

$$\begin{aligned}\mathsf{X}_i^{[m_i]}&\left(\tilde{\tilde{\mathbf{u}}}_i(k_0:k|k_0),\mathbf{x}_i(k_0),\tilde{W}_{i\{k-k_0\}}^{[m_i]}\right)\\&=\left\{\phi_{i\{k-k_0\}}^{[m_i]}(\tilde{\tilde{\mathbf{u}}}_i(k_0:k|k_0),\mathbf{x}_i(k_0),\tilde{\mathbf{w}}_i^{[m_i]}(k_0:k)):\right.\\&\qquad\left.\tilde{\mathbf{w}}_i^{[m_i]}(k_0:k)\in\tilde{W}_{i\{k-k_0\}}\right\}.\end{aligned}\tag{13}$$

The objective of the distributed active fault isolation is to isolate the local malfunction by driving the system to a state condition consistent with only one faulty model. In other words, for any couple of models $\alpha_i,\ \beta_i\in\mathscr{M}_i^+,\alpha_i\neq\beta_i$, we look for existence of a local sequence $\tilde{\tilde{\mathbf{u}}}_i(k_d:k_d+T_i|k_d)$ leading to $\mathbf{x}_i^{[\alpha_i]}(k_d+T_i)\neq\mathbf{x}_i^{[\beta_i]}(k_d+T_i)$, for all $(\tilde{\mathbf{w}}_i^{[\alpha_i]}(k_d:k_d+T_i),\tilde{\mathbf{w}}_i^{[\beta_i]}(k_d:k_d+T_i))\in\tilde{W}_i^{[\alpha_i]}\times\tilde{W}_i^{[\beta_i]}$, where $\mathbf{x}_i^{[\alpha_i]}(k_d+T_i)$ and $\mathbf{x}_i^{[\beta_i]}(k_d+T_i)$ denote the value of the state variables T_i steps after fault detection, evolving from $\mathbf{x}_i^{[\alpha_i]}(k_d)=\mathbf{x}_i^{[\beta_i]}(k_d)=\mathbf{x}_i(k_d)$ according to (1), with models α_i and β_i, respectively.

This corresponds to verify the separation of the state reachable sets at time k_d+T_i, i.e.

$$\begin{aligned}\mathsf{X}_i^{[\alpha_i]}(\tilde{\tilde{\mathbf{u}}}_i(k_d:k_d+T_i|k_d),\mathbf{x}_i(k_d))\cap\\ \mathsf{X}_i^{[\beta_i]}(\tilde{\tilde{\mathbf{u}}}_i(k_d:k_d+T_i|k_d),\mathbf{x}_i(k_d))=\emptyset\end{aligned}\tag{14}$$

for all the possible faulty dynamics in $\mathscr{M}_i^+$ (assuming that $\mathscr{M}_i$ is exhaustive). For ease of reading, in the following, the dependence of the reachable sets on $\tilde{W}_i^{[\alpha_i]}$, $\tilde{W}_i^{[\beta_i]}$ will be omitted.

In order to compute the minimally harmful (in terms of length/norm) input sequence guaranteeing diagnosis we solve the following optimization problem:

$$\min_{\tilde{\tilde{\mathbf{u}}}_i(k_d:k_d+T_i|k_d)}\left\|\tilde{\tilde{\mathbf{u}}}_i(k_d:k_d+T_i|k_d)\right\|_2^2\tag{15a}$$

$$\text{subject to}\quad\text{dynamics }(1)-(2)\tag{15b}$$

$$\mathbf{x}_i^{[m_i]}(k_d)=\mathbf{x}_i(k_d),\quad\forall m_i\in\mathscr{M}_i^+\tag{15c}$$

$$\mathbf{u}_i^{[m_i]}(k)\in U_i,\quad k\in[k_d,k_d+T_i-1]\tag{15d}$$

$$\mathsf{X}_i^{[m_i]}(k|k_d)\subseteq X_i,\quad k\in[k_d,k_d+T_i-1]\tag{15e}$$

$$\mathsf{X}_i^{[m_i]}(k_d+T_i|k_d)\subseteq\bar{S}_i^{[m_i]}\oplus E_i^{[m_i]},\quad\forall m_i\in\mathscr{M}_i^+\tag{15f}$$

$$\mathsf{X}_i^{[\alpha_i]}(k_d+T_i|k_d)\cap\mathsf{X}_i^{[\beta_i]}(k_d+T_i|k_d)=\emptyset,\quad\alpha_i\neq\beta_i\tag{15g}$$

with increasing $T_i=1,\cdots$ until the problem becomes feasible or a T_{max} is attained. Note that T_{max} is a design parameter, giving a limit to the maximum number of steps to have fault isolation.

As explained in [19], in the case of zonotope sets, the size of the state reachable sets does not depend on the input sequence (the input affects only the center of these sets). This property allows to replace (15e), (15f) in problem (15a)-(15g) with simpler constraints (see [41]). According to [19], the problem above can be reformulated as a mixed-integer quadratic program (MIQP) which can be solved using, e.g. CPLEX [49].

According to Section II-C, for a given input sequence and an initial state condition $\mathbf{x}_i(k_d)$, the reachable set $\mathsf{X}_i^{[m_i]}(k|k_d)$ contains all the possible values of $\mathbf{x}_i(k)$. Therefore, for each $m_i\in\mathscr{M}_i^+$, constraint (15e) ensures that $\mathbf{x}_i(k)\in X_i$ for all $k\in[k_d,k_d+T_i-1]$. Similarly, for each $m_i\in\mathscr{M}_i$, constraint (15f) ensures that $\mathbf{x}_i^{[m_i]}(k_d+T_i)\in\bar{S}_i^{[m_i]}\oplus E_i^{[m_i]}$, that is, at the end of the isolation horizon it will be possible to reconfigure the MPC and to control the local state, guaranteeing stability and constraint satisfaction. As shown in Section III, 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 $m_i\in\mathscr{M}_i$.

This is summarized in the following result.

Proposition 1: If Problem (15a)-(15g) is feasible, robust stability and constraint satisfaction are guaranteed for the overall LSS by applying the input sequence (11), with $\tilde{\tilde{\mathbf{u}}}_i(k_d:k_d+T_i|k_d)$ computed solving (15a)-(15g), and reconfiguring the i-th local controller using the control law $\kappa_i^{[m_i]}$ designed in Section III-A for the isolated model $m_i\neq 1$.

Proof: The proof follows from the result in [44] for the stability in healthy conditions using tube-based controllers. In Problem (15a)-(15g), the satisfaction of constraint (15e) ensures that local state constraints continue to be guaranteed, thus not endangering stability and constraints satisfaction in neighboring subsystems and in the rest of the LSS. The satisfaction of constraint (15f) ensures that at the end of the isolation horizon the local MPC problem will be feasible for any model $m_i\in\mathscr{M}_i^+$, thus allowing the computation of the control law $\kappa_i^{[m_i]}$, which guarantees robust stability and constraint satisfaction for the overall LSS. ■

Remark 8: Note that the satisfaction of constraint (15f) may be difficult in general. However, if problem (15a)-(15g) is not feasible, we can still unplug the subsystem where the fault was detected and still preserve the overall stability (see Section V).

It is worth noting that as far as the i-th subsystem continues to guarantee local state constraints X_i, reconfiguration of neighboring subsystems is not needed, no matter whether the fault in i involves only local dynamics (matrix $\mathbf{A}_{ii}$) or the interconnection dynamics $\mathbf{A}_{ij}$: only subsystem i needs to be reconfigured. Moreover, the unplugging of a subsystem is always possible, by implying only a contraction of the set $W_j^{[m_j]}$ in the child subsystems j for which $i\in\mathscr{N}_j^{[m_j]}$.

Finally, by injecting $\tilde{\tilde{\mathbf{u}}}_i(k_d:k_d+T_i|k_d)$, solution of problem (15a)-(15g), into subsystem i, fault isolation is obtained in at most T_i steps by verifying which reachable set $\mathsf{X}_i^{[m_i]}(k|k_d)$ the real $\mathbf{x}_i(k_d+T_i)$ belongs to. Since the problem above guarantees the isolability for all the possible realizations of $\tilde{\mathbf{w}}_i^{[m_i]}(k_d:k_d+T_i)$, it is possible to obtain an earlier isolation if at time $k<k_d+T_i$, $\mathbf{x}_i(k)$ is already consistent with one model m_i only. Rather than applying the entire sequence $\tilde{\tilde{\mathbf{u}}}_i(k_d:k_d+T_i|k_d)$, it is possible to apply the Active FDI approach above in a closed-loop fashion by re-solving problem (15a)-(15g) at each time step with the newly available state (see e.g. [50]). While this approach will increase active FDI performance, it comes at the price of increased complexity.

V. FTC Strategy

In this section, the tools introduced in the previous sections are integrated for the proposed FTC strategy. At time $k=0$, the nominal model $m_i=1$ is active. During healthy nominal behaviour, before fault detection, each subsystem is controlled by the decentralized/distributed tube-based MPC introduced in Section III-A and monitored by the passive fault detection method in Section IV-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 Section IV-B) is activated. Three possible scenarios can be in place, illustrated in Fig. 3 and described in the following.

Scenario 1 - Isolation and Control reconfiguration

There exists a control input sequence so that Problem (15a)-(15g) is feasible, i.e.

i) it is possible to separate the reachable sets of the different faulty dynamics (achieving therefore fault isolation), i.e.

$$\mathsf{X}_i^{[\alpha_i]}(k_d+T_i|k_d)\cap\mathsf{X}_i^{[\beta_i]}(k_d+T_i|k_d)=\emptyset,\forall\alpha_i\neq\beta_i,\ \alpha_i,\beta_i\in\mathscr{M}_i^+.$$

ii) the state after fault isolation is guaranteed to remain in the domain of attraction:

$$\mathsf{X}_i^{[m_i]}(k_d+T_i|k_d)\subseteq\bar{S}_i^{[m_i]}\oplus E_i^{[m_i]},\quad\forall m_i\in\bar{\mathscr{M}}_i.$$

The reconfiguration of the i-th local controller is therefore feasible using the control law $\kappa_i^{[m_i]}$ designed in Section III-A for the identified model $m_i\neq 1$. In this first scenario, applying the input sequence (11), with $\tilde{\tilde{\mathbf{u}}}_i(k_d:k_d+T_i|k_d)$ computed by the Active Fault Isolation tool (15a)-(15g), the fault is isolated at most at time k_d+T_i, identifying which model $m_i\in\mathscr{M}_i^+$ is acting in the local subsystem i. Furthermore, the computed input guarantees that $\mathbf{x}_i(k_d+T_i)\in\bar{S}_i^{[m_i]}\oplus E_i^{[m_i]}$. At time k_d+T_i, once the novel "nominal" dynamics is isolated, its controller is implemented continuing to guarantee the stability of the LSS; it will not be necessary to disconnect the faulty subsystem or to reconfigure neighboring subsystems because, since the local controller continues to satisfy local state constraints X_i, the influence of the reconfigured subsystem i on the neighboring subsystems $j\in\mathscr{N}_i^{[}m_i]$ remains bounded by $W_j^{[m_j]}$, as before the local control reconfiguration of i.

Scenario 2 - Isolation and Unplugging

There exists a control input sequence so that it is possible to achieve correct fault isolation, i.e. there exists a solution for Problem (15a) satisfying

$$\mathsf{X}_i^{[\alpha_i]}(k_d+T_i|k_d)\cap\mathsf{X}_i^{[\beta_i]}(k_d+T_i|k_d)=\emptyset,\quad\alpha_i\neq\beta_i,$$

but we cannot satisfy constraint (15f), that is, we cannot guarantee the reconfiguration properties $\mathbf{x}_i(k_d+T_i)\in\bar{S}_i^{[m_i]}\oplus E_i^{[m_i]}$ at the end of the Active Fault Isolation process for some $m_i\in\bar{\mathscr{M}}_i$. The stability of the system is anyway guaranteed thanks to constraint (15e). 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 (15f) 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 - Unplugging

It is not possible to find a local control input sequence so to achieve fault isolation, i.e. Problem (15a)-(15g) is not feasible even without constraint (15f). 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.

Plug-and-Play approaches [37] can be used to design the local controllers so to allow Plug-and-Play operations, providing conditions for the plug-in of novel subsystems. In this case, after the problem is solved in the disconnected faulty subsystem, it can be re-plugged into the network of the LSS, by checking before whether the conditions for the plug-in are satisfied. Note that, when using a Plug-and-Play approach, the design of the controller for subsystem i requires at most information about the subsystem under control and its neighbors.

The entire procedure is repeated if and when a new fault occurs. As presented in this section, Active Fault Diagnosis can be seen as an important tool to support the decision-making process for the control and monitoring of the LSS.

Note that an active input is used for local fault isolation, but not for fault detection. This avoids conflicts between fault detectability and control objectives that would degrade nominal performance. Conversely, the input is not restricted by stability or performance considerations during fault isolation. However, state constraints are enforced, as well as the condition that a stabilizing controller can be implemented after isolation. Overall stability follows provided that the active input design problem is feasible.

VI. Extensions

In this section, some extensions to the previous results are briefly illustrated.

A. Explicit solution of the Active Fault Isolation problem

It is worth noting that Problem (15a)-(15g) can be solved explicitly as a function of the state $\mathbf{x}_i(k_d)$ for each $i\in\mathscr{N}$ (see [24] for the details in the centralized case). This represents an additional tool that can be used by the proposed distributed Fault Tolerant Control Architecture as a support decision scheme. By solving Problem (15a)-(15g) for every state of the state constraint space, it is possible to build a map of the state space. At fault detection time, by measuring the state $\mathbf{x}_i(k_d)$, it is already possible to know which FTC scenario (Scenario 1, 2 or 3) will occur depending on the feasibility of Problem (15a)-(15g), and it is possible to take an immediate decision about the action to take to guarantee LSS safe operation. In the simulation Section we show the use of this tool in an example (see Figure 7).

B. Measurement noise

To allow focusing on the main results and to simplify the presentation, in the previous sections the measurement noise

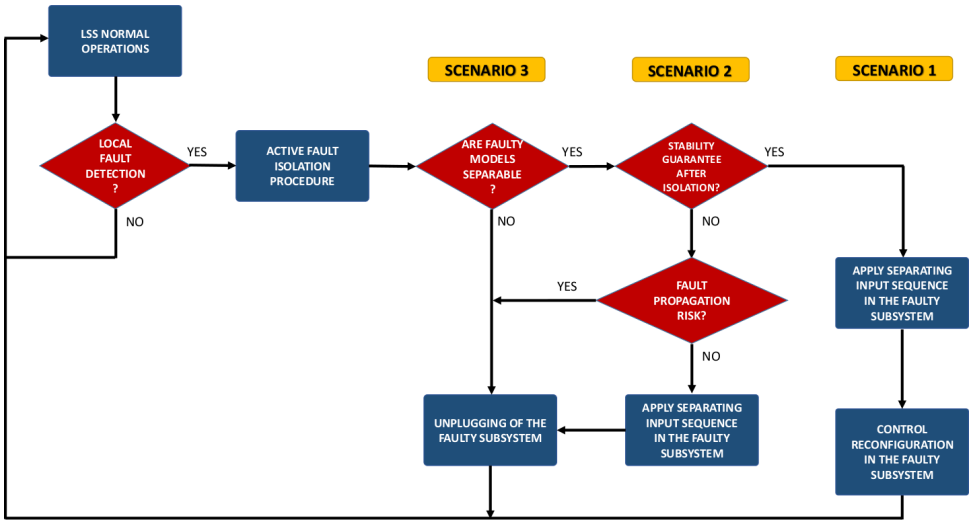

Fig. 3. The proposed FTC strategy. Three possible scenarios are considered by the Active Fault Isolation procedure.

has not been considered. However, it is possible to extend the proposed approach to the case that the local output equation can be described by

$$\mathbf{y}_i^{[m_i]}(k) = \mathbf{C}_i \mathbf{x}_i(k) + \mathbf{v}_i(k),$$

where $\mathbf{y}_i^{[m_i]}(k) \in \mathbb{R}^{n_{x_i}}$ denotes the output vector of subsystem i, vector $\mathbf{v}_i(k)$ represents the measurement noise and $\mathbf{C}_i$ is the output matrix. In this paper, we do not consider sensor faults. We assume that the pair $(\mathbf{A}_{ii}^{[m_i]}, \mathbf{C}_i)$ is observable for each $i \in \mathcal{N}$. The following assumption is required:

Assumption 6: The measurement noise $\mathbf{v}_i(k)$ is bounded by a known set $\mathbf{v}_i(k) \in V_i, \forall k, \forall i \in \mathcal{N}$, being V_i zero-centered zonotopes which are known a priori.

The output reachable set has to be defined accordingly

$$\mathrm{Y}_i^{[m_i]}(k|k_0) = \mathbf{C}_i \mathrm{X}_i^{[m_i]}(\tilde{\mathbf{u}}_i^{[m_i]}(k_0:k|k_0), \mathbf{x}_i(k_0), \tilde{W}_{i\{k-k_0\}}^{[m_i]}) \oplus V_i.$$

The local control law can be computed in a distributed way by means of an output-feedback model predictive control, for example as in [51], which uses a distributed state observer. Then, a similar procedure for distributed fault diagnosis as the one proposed in Sections IV-A and IV-B can be used. Differently from Section IV-A, in this scenario with measurement noise, the set-based observer output estimation error is used for passive fault detection, instead of (9). For the active fault isolation, Problem (15a)-(15g) should be updated, requiring the separability of the output reachable sets:

$$\mathrm{Y}_i^{[\alpha_i]}(k_d + T_i|k_d) \cap \mathrm{Y}_i^{[\beta_i]}(k_d + T_i|k_d) = \emptyset, \quad \alpha_i \neq \beta_i;$$

instead of (15g), and tightening the controller domain constraint in (15f) as proposed in [50] in a set-valued observer-based centralized scenario.

Note that set $E_i^{[m_i]}$ and tightened state and input constraints $\bar{X}_i^{[m_i]}$ and $\bar{U}_i^{[m_i]}$ will also be affected by V_i.

C. Parameter uncertainty in faulty model

It is possible to extend the proposed method to include uncertainty in the parameters of the models of the faulty dynamics.

We consider the case of classes of faults, each described by parameters that can vary in a bounded interval. To take this into account in Problem (15a)-(15g), we redefine the faulty models' dynamics in (1)-(2) using the unknown parameters' averages, while including the uncertainties in redefined sets $W_i^{[m_i]}$. Specifically, we redefine:

$$A_{ii} = A_{ii_{nom}}^{[m_i]} \pm \Delta A_{ii}^{[m_i]} \tag{16}$$

where $A_{ii_{nom}}^{[m_i]}$ is obtained by averaging the uncertain parameters, and $\Delta A_{ii}^{[m_i]}$ is the maximum positive deviation to the matrix caused by the uncertainty of the fault parameters. Similar notation can be used for all other matrices in (1)-(2).

To account for the parameter uncertainty in Problem (15a)-(15g), sets $W_i^{[m_i]}$ (6) are redefined as:

$$W_i^{[m_i]} = \bigoplus_{j \in \mathcal{N}_i^{[m_i]}} \left((\mathbf{A}_{ij_{nom}}^{[m_i]} + \mathbf{B}_{i_{nom}}^{[m_i]} \mathbf{K}_{ij}^{[m_i]}) + (\Delta \mathbf{A}_{ij}^{[m_i]} + \Delta \mathbf{B}_i^{[m_i]} \mathbf{K}_{ij}^{[m_i]}) \right) X_j \oplus \Delta \mathbf{A}_{ii}^{[m_i]} X_i^{[m_i]} \oplus \Delta \mathbf{B}_i^{[m_i]} U_i^{[m_i]} \oplus D_i. \tag{17}$$

VII. Simulation Results

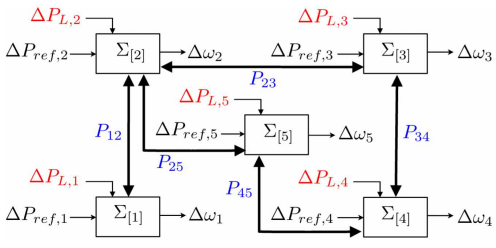

Fig. 4. Power Network System with 5 generation areas, interconnected as in Scenario 2 of [37].

In this section we show the effectiveness of the proposed distributed FTC methodology, applying it on a Power Network System (PNS) [37] composed of 5 generation areas which are

interconnected through tie-lines. Specifically, we consider the case described in Scenario 2 of [37], illustrated in Figure 4. We assume that the communication network between local controllers mirrors the physical coupling graph.

In the simulations, we firstly design the distributed tube-based MPC controller to regulate each area during nominal operation, and for each faulty model in $\mathscr{M}_i^+, \forall i \in \mathscr{N}$. Performance of the proposed set-based passive fault detection and active fault isolation strategies is shown in the case of a fault occurring on one of the interconnected subsystems. If feasible, isolation may be followed by the reconfiguration of the subsystem controller to accommodate the isolated fault.

The dynamics of each subsystem, equipped with primary control and linearised around the equilibrium, are:

$$\begin{aligned} \dot{\mathbf{x}}_i &= \mathbf{A}_{ii}^{[m_i]}\mathbf{x}_i + \mathbf{B}_i^{[m_i]}\mathbf{u}_i^{[m_i]} + \mathbf{L}_i^{[m_i]}\Delta P_{L_i} + \mathbf{w}_i^{[m_i]}, \quad (18) \\ \mathbf{w}_i^{[m_i]} &= \sum_{j \in \mathscr{N}_i^{[m_i]}} \mathbf{A}_{ij}^{[m_i]}\mathbf{x}_j + \mathbf{d}_i, \end{aligned}$$

where $\mathbf{x}_i = (\Delta\theta_i, \Delta\omega_i, \Delta P_{m_i}, \Delta P_{v_i})'$ is the local state, $\mathbf{u}_i^{[m_i]} = \Delta P_{ref_i}$ is the control input of each area, ΔP_{L_i} is the local power load and $\mathscr{N}_i^{[m_i]}$ is the set of neighboring areas directly connected to subsystem i through tie-lines. More specifically, the matrices of system (18) are

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

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

The values of the parameters are defined as in [37] for the nominal model $m_i = 1$. Each subsystem is subject to the following constraints on $\mathbf{x}_i$ and $\mathbf{u}_i^{[m_i]}$: $|\Delta\theta_i| \leq 0.1, |\Delta\omega_i| \leq 0.2, |\Delta P_{m_i}| \leq 5, |\Delta P_{v_i}| \leq 5, |\Delta P_{ref_i}| \leq 5$ for all subsystems. For each generation area, discrete-time models as in (1) are obtained by discretizing (18) with a sampling time $T_s = 1$ sec. Disturbance $\mathbf{d}_i$ is assumed to be bounded by D_i, a zonotope defined in generator notation as $D_i = \{10^{-4}\mathbf{I}_{n_{x_i}}, 0\}$, where $\mathbf{I}_{n_{x_i}}$ is the n_{x_i}-dimensional identity matrix. The noise level is comparable to other examples in the literature [51], [52]. Local control matrices $\mathbf{K}_{ii}^{[m_i]}$ and $\mathbf{K}_{ij}^{[m_i]}$ are designed for each subsystem i, for every model $m_i \in \mathscr{M}_i$, using the PnPMPC toolbox for MATLAB [53]. The goal of the control is the Automatic Generation Control (AGC) layer to maintain the frequency in each area. As regards the FDI architecture, each area is equipped with a local fault diagnoser.

A. Example 1

In the first example, each area of the PNS can be affected by three different faults, characterized by a change of the value of the inertia parameter $H_i^{[m_i]}$. From an electrical point of view, this represents a loss of the generation capability in the considered generation area. The value of the inertia parameter

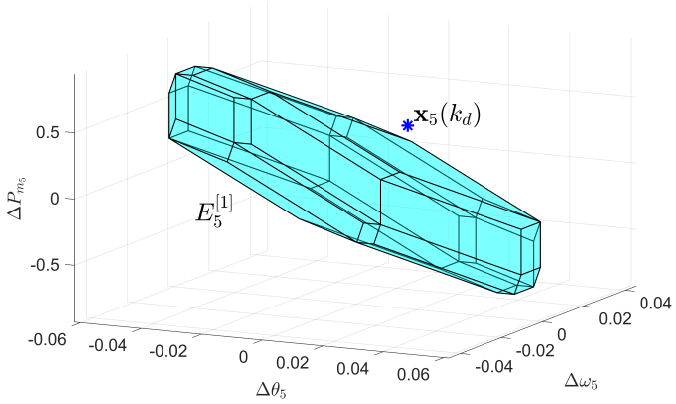

Fig. 5. Fault detection of Area 5 at time $k_d = 5$. A 3D plot of the measurement $\mathbf{x}_5(5)$ (indicated with a blue star) and the corresponding detection tube $E_5^{[1]}$ centered in $\bar{\mathbf{x}}_5^{[1]}(5)$, both projected on $(\Delta\theta_5, \Delta\omega_5, \Delta P_{m_5})$. Detection occurs, as the measurement lies outside of the zonotope tube.

for the nominal model $m_i = 1$ is $H_1^{[m_1]} = 12$ and for the the faulty models $m_i = 2,3,4$ the values of the inertia parameters are $H_2^{[m_2]} = 2.35$, $H_3^{[m_3]} = 2.6$, and $H_4^{[m_4]} = 2.85$.

At time $k_f = 3$, the inertia constant in Area 5 decreases from $H_5 = 12$ to $H_5 = 2.35$, corresponding to a reduction of approximately 80% of the inertia value. Following the occurrence of the fault at k_f, the set-based passive fault detection method detects the fault at time $k_d = 5$. At this time the measured state $\mathbf{x}_5(k_d)$ lies outside the zonotopic tube $E_5^{[1]}$ centred in the system's nominal state $\bar{\mathbf{x}}_5^{[1]}(k_d)$, as can be seen in Figure 5[3].

After local fault detection, the local Active Fault Isolation tool is initialized. The optimization Problem (15a)-(15g) is solved using CPLEX. The tool returns the isolating input $\bar{\mathbf{u}}_5(5) = -0.2979$ which, after $T_i = 1$ time step, separates the reachable sets of the dynamics given by the faulty models $m_i \in \mathscr{M}_5^+$, and is able to exclude all faults except the correct one, i.e. $\mathbf{x}_5(k_d + T_i) \in \mathsf{X}_5^{[m_5]}(k_d + T_i | k_d)$ only for $m_5 = 2$. In Figure 6 we show the 3D projection onto the space defined by the states $(\Delta\theta_5, \Delta\omega_5, \Delta P_{m_5})$ of the reachable sets $\mathsf{X}_5^{[m_5]}(k_d + T_i | k_d), \forall m_5 \in \mathscr{M}_5^+$, as well as the projection of $\mathbf{x}_5(k_d + T_i)$. Once the isolating input is computed and applied, and the correct faulty model is identified, the subsystem is reconfigured in order to accommodate the fault to which it is subject. Hence, since Problem (15a)-(15g) is feasible, Scenario 1 of the FTC strategy is implemented, and the controller for area 5 is changed from the one designed for $m_5 = 1$ to that for $m_5 = 2$, resuming normal operation for the LSS.

Furthermore, we show in this scenario that the tool introduced in Section VI-A, based on the off-line solution of Problem (15a)-(15g), can be considered for decision support in the FTC strategy . This allows the local fault diagnosers to immediately check after fault detection which reconfiguration strategy will be feasible (Scenario 1, 2 or 3 of Figure 3) as a function of the state $\mathbf{x}_i(k_d)$. We show in Figure 7 a map representing a portion of the state space for the considered

[3]We use a 3D projection of the states $(\Delta\theta_5, \Delta\omega_5, \Delta P_{m_5})$ to visualize that the state is not contained within the set

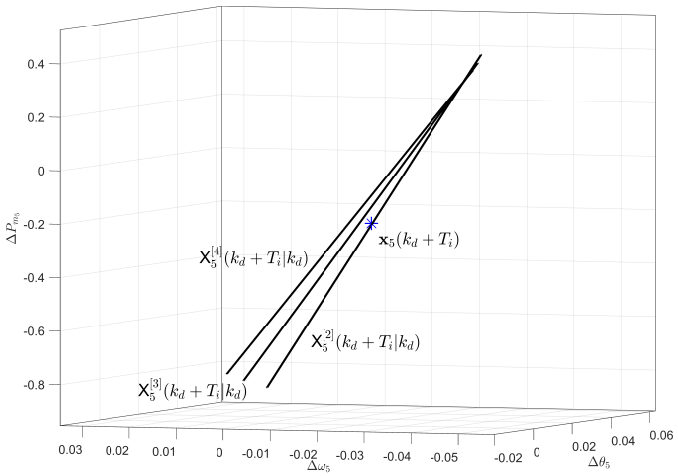

Fig. 6. Measured state $\mathbf{x}_5(6)$ (blue asterisk) at time $k = k_d + T_i = 6$, together with reachable sets $\mathsf{X}_5^{[m_5]}(6|5), m_5 \in \mathscr{M}_5^+$, separated by isolating input $\bar{\mathbf{u}}_5(5) = -0.2979$. Projection on components $(\Delta\theta_5, \Delta\omega_5, \Delta P_{m_5})$. Note that there is no intersection among the reachable sets.

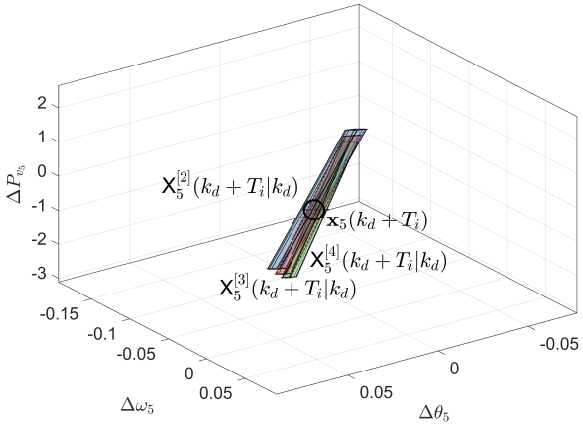

Fig. 8. Reachable sets $\mathsf{X}_5^{[m_5]}(6|5), m_5 \in \mathscr{M}_5^+$, separated by isolating input $\bar{\mathbf{u}}_5(5) = -1.0266$, and measured state $x_{[5]}(6) \in \mathsf{X}_5^{[2]}(6|5)$ (asterisk with black bold circle). Projection on components $(\Delta\theta_5, \Delta\omega_5, \Delta P_{v_5})$.

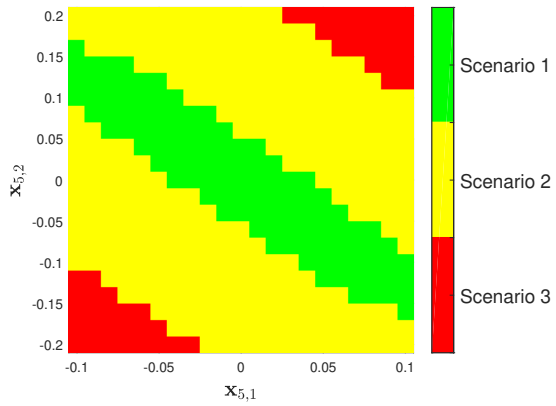

Fig. 7. Map of the first two state components of X_5 (with the other components equal to $\Delta P_{m_5} = 0$, $\Delta P_{v_5} = 0$): for each cell of the grid the FTC scenario to be implemented. The green and yellow areas are the ones from where it is actually possible to separate the considered fault models and have fault isolation.

PNS example: each cell of the map has a different color depending on the FTC strategy that can be applied if the fault detection occurs when the state is in that area. The portion of state space that was considered is $|\Delta\theta_5| \leq 0.1$, $|\Delta\omega_5| \leq 0.2$, $\Delta P_{m_5} = 0$, $\Delta P_{v_5} = 0$. The map was obtained by explicitly solving Problem (15a)-(15g) for 441 points in the state space separated from each other by constant step sizes of 0.01 and 0.02 in the $\Delta\theta_5$ and $\Delta\omega_5$ directions, respectively.

B. Example 2

In this second example, we assume, similarly to Section VI-C, that the possible faulty models for Area 5, i.e. $m_5 \in \mathscr{M}_5^+$, are no longer defined by a single value of the fault parameter, as they were in Example 1. We consider that fault parameter $H_5^{[m_5]}$ is uncertain, and, for $m_5 = 1,2,3,4$ can take values inside an interval as follows: $H_5^{[1]} = 12 \pm 0.1$, $H_5^{[2]} = 2.35 \pm 0.1$, $H_5^{[3]} = 2.60 \pm 0.1$, and $H_5^{[4]} = 2.85 \pm 0.1$.

To deal with the parametric uncertainty, we redefine the matrices in model (18) as defined in (16)[4]. ΔA_{ii} and other deviation matrices are calculated using MATLAB's INTLAB toolbox [54], which allows operations on intervals. Hence, we redefine sets $W_i^{[m_i]}$ as in (17).

As in the first example, each area is locally equipped with a regulator and a fault diagnoser. Again, at $k_f = 3$ the model describing Area 5 dynamics changes from $m_5 = 1$ to $m_5 = 2$. The passive fault diagnosis tool again detects the fault at $k_d = 5$. Hence the Active Fault Isolation tool solves Problem (15a)-(15g), calculating the separating input sequence to be applied to the faulty subsystem, $\bar{\mathbf{u}}_5 = -1.0266$, with $T_i = 1$. In Figure 8 we show the three dimensional projection of the reachable sets onto the states $(\Delta\theta_5, \Delta\omega_5, \Delta P_{v_5})$[5]. Finally, the diagnoser applies the separating input to the faulty subsystem, and is therefore able to isolate the correct class of faults affecting the local dynamics. Unfortunately, in order for Problem (15a)-(15g) to be feasible, constraint (15f) $\mathsf{X}_5^{[m_5]}(k_d + T_i|k_d) \subseteq F_5^{[m_5]}$ has to be relaxed to $\mathsf{X}_5^{[m_5]}(k_d + T_i|k_d) \subseteq X_5$. We therefore implement Scenario 2 of the FTC strategy: after local fault isolation, the unplugging of the faulty area is required to maintain overall stability properties of the PNS.

Acknowledgment. We would like to acknowledge Prof. Giancarlo Ferrari-Trecate and Dr. Stefano Riverso for many fruitful discussions and research interactions on scalable Plug-and-Play distributed control and for help and suggestions on using the PnPMPC Matlab Toolbox [53].

VIII. Concluding Remarks

In this paper, a scalable distributed FTC scheme has been presented for the monitoring of interconnected subsystems, using Active Fault Isolation. After fault detection, the proposed method allows to guarantee whether it is possible to correctly

[4]Note here that the uncertainty on $H_5^{[m_5]}$ influences all matrices, due to dynamics discretization.

[5]The apparent intersection of the reachable sets is caused by their projections from four-dimensional to three-dimensional space.

isolate the fault in a finite 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. The presence of measurement noise has been investigated. Extensive simulation results are provided on a Power Network System to show the effectiveness of the proposed approach, considering also classes of faults where the parameters characterizing each faulty model are uncertain and may vary within a defined range of values.

As a future work, we will investigate the use of other active fault diagnosis techniques in distributed and scalable scenarios, such as hybrid stochastic-deterministic approaches and the design of references instead of input sequences.

REFERENCES

[1] T. Samad and A. M. Annaswamy (eds.), "The impact of control technology," *IEEE Control Systems Society*, 2011, available at www.ieeecss.org.

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

[3] 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.

[4] J. Prakash, S. Narasimhan, and S. C. Patwardhan, "Integrating model based fault diagnosis with model predictive control," *Industrial & Engineering Chemistry Research*, vol. 44, no. 12, pp. 4344–4360, 2005.

[5] M. Kettunen, P. Zhang, and S.-L. Jämsä-Jounela, "An embedded fault detection, isolation and accommodation system in a model predictive controller for an industrial benchmark process," *Computers and Chemical Engineering*, vol. 32, no. 12, pp. 2966–2985, 2008.

[6] B. Jiang, M. Staroswiecki, and V. Cocquempot, "Fault accommodation for nonlinear dynamic systems," *IEEE Transactions on Automatic Control*, vol. 51, no. 9, pp. 1578–1583, 2006.

[7] J. Lan and R. J. Patton, "A new strategy for integration of fault estimation within fault-tolerant control," *Automatica*, vol. 69, pp. 48–59, 2016.

[8] 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.

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

[10] C. Ocampo-Martinez and V. Puig, "Fault-tolerant model predictive control within the hybrid systems framework: Application to sewer networks," *International Journal of Adaptive Control & Signal Processing*, vol. 23, no. 8, pp. 757–787, 2009.

[11] R. C. Shekar and J. M. Maciejowski, "Robust predictive control with feasible contingencies for fault tolerance," in *Preprints of the 18th IFAC World Congress*, Milano, Italy, 2011, pp. 4666–4671.

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

[13] 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," *IEEE Transactions on Automatic Control*, vol. 61, no. 12, pp. 3963–3978, 2016.

[14] A. E. Ashari, R. Nikoukhah, and S. L. Campbell, "Effects of feedback on active fault detection," *Automatica*, vol. 48, no. 5, pp. 866–872, 2012.

[15] V. Venkatasubramanian, R. Rengaswamy, K. Yin, and S. Kavuri, "A review of process fault detection and diagnosis: Part I: Quantitative model-based methods," *Computers and Chemical Engineering*, vol. 27, no. 3, pp. 293–311, 2003.

[16] 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.

[17] I. Punčochář, J. Široky, and M. Šimandl, "Constrained active fault detection and control," *IEEE Transactions on Automatic Control*, vol. 60, no. 1, pp. 253–258, 2015.

[18] S. Cheong and I. R. Manchester, "Input design for discrimination between classes of LTI models," *Automatica*, vol. 53, pp. 103–110, 2015.

[19] 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.

[20] 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.

[21] J. Škach, I. Punčochář, and F. L. Lewis, "Optimal active fault diagnosis by temporal-difference learning," in *IEEE 55th Conference on Decision and Control (CDC)*, 2016, pp. 2146–2151.

[22] F. Harirchi, S. Z. Yong, E. Jacobsen, and N. Ozay, "Active model discrimination with applications to fraud detection in smart buildings," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 9527–9534, 2017.

[23] F. Blanchini, D. Casagrande, G. Giordano, S. Miani, S. Olaru, and V. Reppa, "Active fault isolation: A duality-based approach via convex programming," *SIAM Journal on Control and Optimization*, vol. 55, no. 3, pp. 1619–1640, 2017.

[24] D. M. Raimondo, R. D. Braatz, and J. K. Scott, "Active fault diagnosis using moving horizon input design," in *European Control Conference (ECC)*, 2013, pp. 3131–3136.

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

[26] F. Shi and R. J. Patton, "Fault estimation and active fault tolerant control for linear parameter varying descriptor systems," *International Journal of Robust and Nonlinear Control*, vol. 25, no. 5, pp. 689–706, 2015.

[27] 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*, vol. 27, no. 8, pp. 1260–1283, 2017.

[28] L. Ferranti, Y. Wan, and T. Keviczky, "Predictive flight control with active diagnosis and reconfiguration for actuator jamming." *IFAC-PapersOnLine*, vol. 48, no. 23, pp. 166–171, 2015.

[29] F. Xu, V. Puig, C. Ocampo-Martinez, and X. Wang, "Set-valued observer-based active fault-tolerant model predictive control," *Optimal Control Applications and Methods*, vol. 38, no. 5, pp. 683–708, 2017.

[30] R. J. 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.

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

[32] 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.

[33] J. Lan and R. J. Patton, "Decentralized fault estimation and fault-tolerant control for large-scale interconnected systems: An integrated design approach," in *UKACC 11th International Conference on Control*. IEEE, 2016, pp. 1–6.

[34] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, "Distributed fault diagnosis and fault-tolerant control," in *Diagnosis and Fault-Tolerant Control*. Springer, 2016, pp. 467–518.

[35] M. Davoodi, N. Meskin, and K. Khorasani, "Simultaneous fault detection and consensus control design for a network of multi-agent systems," *Automatica*, vol. 66, pp. 185–194, 2016.

[36] 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*, vol. 62, no. 1, pp. 18–33, 2017.

[37] 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.

[38] S. Riverso and G. Ferrari-Trecate, "Plug-and-play distributed model predictive control with coupling attenuation," *Optimal Control Applications and Methods*, vol. 36, no. 3, pp. 292–305, 2015.

[39] 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.

[40] 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.

[41] D. M. Raimondo, F. Boem, A. J. Gallo, and T. Parisini, "A decentralized fault-tolerant control scheme based on active fault diagnosis," in *IEEE 55th Conference on Decision and Control*, 2016, pp. 2164–2169.

[42] 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.
[43] 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.
[44] 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.
[45] S. V. Raković, E. C. Kerrigan, K. I. Kouramas, and D. Q. Mayne, "Invariant approximations of the minimal robust positively invariant set," *IEEE Transaction on Automatic Control*, vol. 50, no. 3, pp. 406–410, 2005.
[46] A. Bemporad, M. Morari, V. Dua, and E. N. Pistikopoulos, "The explicit linear quadratic regulator for constrained systems," *Automatica*, vol. 38, no. 1, pp. 3–20, 2002.
[47] M. Herceg, M. Kvasnica, C. N. Jones, and M. Morari, "Multi-parametric toolbox 3.0," in *European Control Conference*, no. EPFL-CONF-186265, 2013.
[48] A. Alessio, A. Bemporad, M. Lazar, and W. P. M. H. Heemels, "Convex polyhedral invariant sets for closed-loop linear MPC systems," in *45th IEEE Conference on Decision and Control*, 2006, pp. 4532–4537.
[49] *IBM ILOG CPLEX V12.2 User's Manual for CPLEX*, 2012.
[50] D. M. Raimondo, G. R. Marseglia, R. D. Braatz, and J. K. Scott, "Closed-loop input design for guaranteed fault diagnosis using set-valued observers," *Automatica*, vol. 74, pp. 107–117, 2016.
[51] S. Riverso, M. Farina, and G. Ferrari-Trecate, "Plug-and-play state estimation and application to distributed output-feedback model predictive control," *European Journal of Control*, vol. 25, pp. 17–26, 2015.
[52] N. Zhou, D. Meng, and S. Lu, "Estimation of the dynamic states of synchronous machines using an extended particle filter," *IEEE Transactions on Power Systems*, vol. 28, no. 4, pp. 4152–4161, 2013.
[53] S. Riverso, A. Battocchio, and G. Ferrari-Trecate, "PnPMPC: a toolbox for MatLab," 2012.
[54] S. Rump, "INTLAB - INTerval LABoratory," in *Developments in Reliable Computing*, T. Csendes, Ed. Dordrecht: Kluwer Academic Publishers, 1999, pp. 77–104, http://www.ti3.tuhh.de/rump/.

PLACE PHOTO HERE

Francesca Boem received the Ph.D. degree in Information Engineering in 2013, from the University of Trieste, Italy. She was Post-Doc at the University of Trieste with the Machine Learning Group from 2013 to 2014. From 2014 to 2018, she was Research Associate at the Dept. of Electrical and Electronic Engineering, Imperial College London. Since April 2018 Dr. Boem is a Lecturer in the Department of Electronic and Electrical Engineering at University College London (UCL). Since 2015 she has been part of the team at Imperial College which has been awarded the flagship EU H2020-WIDESPREAD-TEAMING project for the development of the EU KIOS Research and Innovation Centre of Excellence, a strategic partnership between University of Cyprus and Imperial College London. Dr. Boem has been awarded the Imperial College Research Fellowship in February 2018 and the Alliance Hubert Curien grant by the British Council in March 2019. Her current research interests include distributed fault diagnosis and fault-tolerant control methods for large-scale networked systems and security of control systems. Dr. Boem is member of the IFAC Technical Committee SAFEPROCESS and Associate Editor for the IEEE Control System Society Conference Editorial Board and for the EUCA Conference Editorial Board.

PLACE PHOTO HERE

Alexander J. Gallo received the MEng in Electrical and Electronic Engineering from Imperial College, London, UK, in 2016. He is currently pursuing a PhD at the Electrical and Electronic Engineering Department, Imperial College, London, UK, with the Control and Power Research Group. His research interests include distributed fault diagnosis for large-scale systems, as well as distributed methods for secure control of cyber physical systems.

PLACE PHOTO HERE

Davide M. Raimondo received the Ph.D. in Electronics, Computer Science and Electrical Engineering from the University of Pavia, Italy, in 2009. From January 2009 to December 2010 he was a postdoctoral fellow in the Automatic Control Laboratory, ETH Zurich, Switzerland. From December 2010 to May 2015 he was assistant professor at University of Pavia. He has held visiting positions at the Massachusetts Institute of Technology, University of Seville, Vienna University of Technology, University of Konstanz. Prof. Raimondo is currently an associate professor and head of the educational Process Control Laboratory in the Department of Electrical, Computer and Biomedical Engineering at University of Pavia, Italy. He is the author or co-author of more than 85 papers published in refereed journals, edited books, and refereed conference proceedings. He serves/served as subject editor for the journals IEEE Transactions on Control Systems Technology (2019-) and Optimal Control Applications and Methods (2015-2018) and as CEB member of IEEE Control Systems Society. His current research interests include advanced battery management systems, active fault diagnosis and fault-tolerant control, model predictive control and optimization. In 2017, Prof. Raimondo, with co-authors, received the 2014-2016 Automatica Paper Prize Award.

PLACE PHOTO HERE

Thomas Parisini received the Ph.D. degree in Electronic Engineering and Computer Science in 1993 from the University of Genoa. He was with Politecnico di Milano and since 2010 he holds the Chair of Industrial Control and is Director of Research at Imperial College London. He is a Deputy Director of the KIOS Research and Innovation Centre of Excellence, University of Cyprus. Since 2001 he is also Danieli Endowed Chair of Automation Engineering with University of Trieste. In 2009-2012 he was Deputy Rector of University of Trieste. In 2018, he received an Honorary Doctorate from University of Aalborg, Denmark. He authored or co-authored more than 300 research papers in archival journals, book chapters, and international conference proceedings. His more recent research interests include monitoring, diagnosis, control and security of large-scale interconnected nonlinear systems with applications in smart grids, power electronics and industrial process control. He is a co-recipient of the IFAC Best Application Paper Prize of the Journal of Process Control, Elsevier, for the three-year period 2011-2013 and of the 2004 Outstanding Paper Award of the IEEE Trans. on Neural Networks. In 2016 he was awarded as Principal Investigator at Imperial of the H2020 European Union flagship Teaming Project KIOS Research and Innovation Centre of Excellence led by University of Cyprus. In 2012 he was awarded an ABB Research Grant dealing with energy-autonomous sensor networks for self-monitoring industrial environments. Thomas Parisini currently serves as Vice-President for Publications Activities of the IEEE Control Systems Society and during 2009-2016 he was the Editor-in-Chief of the IEEE Trans. on Control Systems Technology and since 2018 he is the Editor in Chief of the European Journal of Control. Since 2017, he is also Editor for Control Applications of Automatica. Among other activities, he was the General Co-Chair of the 2013 IEEE Conference on Decision and Control. Prof. Parisini is a Fellow of the IEEE and of the IFAC.