Plug-and-Play Fault Detection and Control-reconfiguration for a Class of Nonlinear Large-scale Constrained Systems

Stefano Riverso, Francesca Boem, Giancarlo Ferrari-Trecate, and Thomas Parisini

***Abstract*—This paper deals with a novel Plug-and-Play (PnP) architecture for the control and monitoring of Large-Scale Systems (LSSs). The proposed approach integrates a distributed Model Predictive Control (MPC) strategy with a distributed Fault Detection (FD) architecture and methodology in a PnP framework. The basic concept is to use the FD scheme as an autonomous decision support system: once a fault is detected, the faulty subsystem can be unplugged to avoid the propagation of the fault in the interconnected LSS. Analogously, once the issue has been solved, the disconnected subsystem can be re-plugged-in. PnP design of local controllers and detectors allow these operations to be performed safely, i.e. without spoiling stability and constraint satisfaction for the whole LSS. The PnP distributed MPC is derived for a class of nonlinear LSSs and an integrated PnP distributed FD architecture is proposed. Simulation results in two paradigmatic examples show the effectiveness and the potential of the general methodology.**

I. Introduction

Nowadays, several man-made systems are characterized by a large number of states and inputs with a significant spatial distribution. triggering an increasing interest in the study of Systems-of-Systems [1] and Cyber-Physical Systems [2]. LSSs are often modeled as the interaction of many subsystems coupled through physical variables or communication channels [3]. When dealing with control of LSSs, centralized control architectures can be impractical due to computational, communication and reliability limits, and an alternative is offered by the adoption of decentralized and distributed approaches. The application domains for which the proposed approach may result useful are countless (for instance, energy efficient buildings, power networks, wind farms, cascade river reaches, etc.).

In the past, several decentralized (De) and distributed (Di) MPC schemes have been proposed for constrained LSS (see the recent survey [4] and the references therein, such as [5]). In the standard MPC control of LSSs, the prediction of the LSS behaviour is carried out through a nominal model of each subsystem and of the local interactions. However, in several applications, faults and malfunctions may occur thus possibly causing critical and unpredictable changes in the LSS dynamics. Hence, there is a need to devise fault diagnosis schemes (see, for example, [6], [7]) providing on-line the information about the health of the system and to exploit this information to reconfigure the controller so as to guarantee some degree of fault-tolerance (see the seminal paper [8]). Model-based schemes have emerged as prominent approaches to fault diagnosis of continuous and discrete-time systems [9]. As for centralized control, centralized FD architectures suffer of scalability and robustness issues. To overcome these limits, decentralized and distributed fault-tolerant control and fault diagnosis algorithms have been proposed (see [10], [11], [12], [13], [14], [15], [16], [17] as examples).

In this paper, the integration of a DiMPC scheme and a distributed FD architecture is proposed for the first time. Specifically, in the off-line control design phase we adopt a decentralized algorithm and we assume that the design of a local controller can use information at most from parents of the corresponding subsystem, i.e., subsystems that influence its dynamics. This implies that the whole model of the LSS is never used in any step of the synthesis process [3]. This approach has several advantages in terms of *scalability*: i) the communication flow at the design phase has the same topology of the coupling graph – usually sparse – ii) the local design of controllers and fault detectors can be conducted independently; iii) local design complexity scales with the number of parent subsystems only; iv) if a subsystem joins/leaves an existing network (plug-in/unplugging operation) at most children/parents subsystems have to retune their controllers and fault detectors. We refer to this kind of decentralized synthesis as PnP design, if – in addition – the plug-in and unplugging operations can be performed through a procedure for automatically assessing whether the operation does not spoil stability and constraint satisfaction for the overall LSS (see [18] and [19]). Different definitions of PnP design are given in [20], [21] and [22].

Novelties: The significant novelty presented in the paper[1] is the *integration of DiMPC and FD architectures in a PnP framework for nonlinear LSSs* (for centralized approaches, the interested reader is referred to [24], [25], [26] and the related work in [27]. Moreover, a centralized reconfiguration process, based on hybrid systems, is proposed in [28]). Similarly to the design of local controllers, we propose a PnP design method for local fault detection. Motivations for PnP MPC/FD are the following: i) when the behaviour of a subsystem is corrupted

The research leading to these results has received funding from the European Union Seventh Framework Programme [FP7/2007-2013] under grant agreement n° 257462 HYCON2 Network of excellence and from the RCUK Energy Programme (contract no: EP/L014343/1), project *Stability and Control of Power Networks with Energy Storage*

S. Riverso is with United Technologies Research Center Ireland, Cork, Ireland (riverss@utrc.utc.com), and with the Dipartimento di Ingegneria Industriale e dell'Informazione, Università degli Studi di Pavia, Italy (stefano.riverso@unipv.it)

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

G. Ferrari-Trecate is with the Dipartimento di Ingegneria Industriale e dell'Informazione, Università degli Studi di Pavia, Italy (giancarlo.ferrari@unipv.it)

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

[1] A preliminary version of this work has been presented at the 53rd IEEE Conference on Decision and Control [23].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2016.2535724, IEEE Transactions on Automatic Control

by a fault, we show how the subsystem can be automatically disconnected while preserving stability and constraint satisfaction at each time instant for all other subsystems; ii) when a faulty subsystem is repaired, it can be replugged-in without changing all existing local controllers and fault detectors. We highlight that, differently from [18] and [19], in this paper we design local MPC controllers for a class of nonlinear LSSs. As regards FD schemes – to the best of the authors knowledge – it is the first time that a PnP FD distributed architecture is proposed. Furthermore, in real application contexts, usually MPC controllers are designed based on the knowledge of a nominal model of the system. Therefore a FD scheme is needed to monitor the behaviour of the system. The proposed FD architecture is robust to modeling and measurement uncertainties. To achieve this goal, it considers local models that are different from those used in local MPC controllers. In fact, another novel contribution of this paper is the possibility to use different decompositions and different models for the control and the monitoring components. This feature is useful for applications: local controllers must compute local control inputs based on local available measurements only, sometimes with high sampling rates; on the other hand local fault detectors may work at a different rate and can keep advantage of the redundancy given by sharing some variables in order to improve estimation performances.

The paper is organized as follows. After providing a few notations and basic definitions in Section II, in Section III, we define the problem addressed in the paper and we introduce the dual decomposition of the LSS. Then, in Section IV, we design the nonlinear DiMPC architecture, while in Section V we derive the PnP distributed FD scheme. The fault detectability analysis is presented in Section VI. The reconfiguration process after unplugging and plugging-in operations are described in Section VII. In Section VIII, we apply the proposed architectures to a ring of coupled van der Pol Oscillators (vdPOs) and to a Power Network System (PNS). Finally, some concluding remarks are given in Section IX.

II. Basic Notations and Definitions

We use $a : b$ for the set of integers $\{a, a+1, \dots, b\}$. The symbols $\mathbb{R}_+$ and $\mathbb{R}_{0+}$ are the sets of positive real numbers, respectively excluding and including 0. The column vector with s components $v_1, \dots, v_s$ is $\mathbf{v} = (v_1, \dots, v_s)$. The symbols $\oplus$ and $\ominus$ denote the Minkowski sum and difference, respectively, i.e. $A = B \oplus C$ if $A = \{a : a = b + c, \text{ for all } b \in B \text{ and } c \in C\}$ and $A = B \ominus C$ if $a \oplus C \subseteq B, \ \forall a \in A$. Moreover, $\bigoplus_{i=1}^{s} G_i = G_1 \oplus \dots \oplus G_s$. For $\rho > 0$, $B_\rho(z) = \{x \in \mathbb{R}^n : ||x - z|| \leq \rho\}$ where $||\cdot||$ is the Euclidean norm in $\mathbb{R}^n$. Given a set $\mathbb{X} \subset \mathbb{R}^n$, convh$(\mathbb{X})$ denotes its convex hull. Function dist$(v, \mathbb{X})$ denotes the distance among a vector v and a set $\mathbb{X}$. The symbol $\mathbf{0}_r$ denotes a column vector in $\mathbb{R}^r$ with all elements equal to 0. Let $v, \ \bar{v} \in \mathbb{R}^s$, the inequality $|v| \leq \bar{v}$, component-wise means $|v_i| \leq \bar{v}_i, \ i = 1 : s$.

Definition 1 (RCI set)**.** *Consider the discrete-time linear system $x(t+1) = Ax(t) + Bu(t) + w(t)$, with $x(t) \in \mathbb{R}^n$, $u(t) \in \mathbb{R}^m$, $w(t) \in \mathbb{R}^n$ and subject to constraints $u(t) \in \mathbb{U} \subseteq \mathbb{R}^m$ and $w(t) \in \mathbb{W} \subset \mathbb{R}^n$. The set $\mathbb{X} \subseteq \mathbb{R}^n$ is an RCI set with respect to $w(t) \in \mathbb{W}$, if $\forall x(t) \in \mathbb{X}$ there exists $u(t) \in \mathbb{U}$ such that $x(t+1) \in \mathbb{X}, \ \forall w(t) \in \mathbb{W}$.*

III. System definition

Consider a class of discrete-time nonlinear LSSs composed of M subsystems, using two different decompositions of the system structural graph (see Figure 1). The control framework

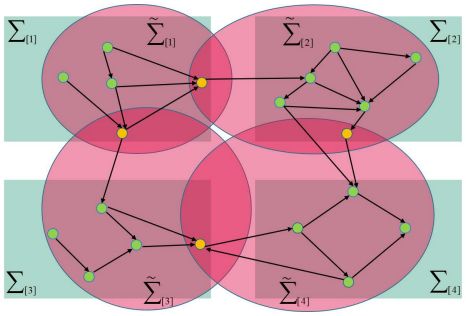


Fig. 1: Two different decompositions of the LSS structural graph: the non-overlapping subsystems of the control architecture (in green) and the overlapping subsystems of the fault diagnosis framework (in red). The small circles represent state and input variables; the yellow ones are the shared state variables.

considers a nonlinear model described by the following dynamics:

$$\Sigma_{[i]}: \quad x_{[i]}^+ = A_{ii}x_{[i]} + B_i[g_i(x_{[i]}, \psi_{[i]})u_{[i]} + h_i(x_{[i]}, \psi_{[i]})] + w_i(\psi_{[i]}) \quad (1)$$

where $x_{[i]} \in \mathbb{R}^{n_i}$, $u_{[i]} \in \mathbb{R}^{m_i}$, $i \in \mathcal{M} = \{1, \dots, M\}$, are the local state and input, respectively, at time t and $x_{[i]}^+$ stands for $x_{[i]}$ at time $t+1$. The k-th component of vector $x_{[i]}$ is specified by $x_{[i,k]}$. A similar notation is used for input and output variables. The vector of interconnection variables $\psi_{[i]} \in \mathbb{R}^{p_i}$ collects the states $\{x_{[j]}\}_{j \in \mathcal{N}_i}$ that influence the dynamics of $x_{[i]}$, where $\mathcal{N}_i$ is the set of parents of subsystem i defined as $\mathcal{N}_i = \{j \in \mathcal{M} : \frac{\partial x_{[i]}^+}{\partial x_{[j]}} \neq \mathbf{0}_{n_i}, i \neq j\}$. We also define $\mathcal{F}_i = \{k : i \in \mathcal{N}_k\}$ as the set of children of $\Sigma_{[i]}$. For $i \in \mathcal{M}$, $A_{ii} \in \mathbb{R}^{n_i \times n_i}$ represent the linear nominal dynamics, while $B_i \in \mathbb{R}^{n_i \times m_i}$, $g_i(\cdot) : \mathbb{R}^{n_i} \times \mathbb{R}^{p_i} \to \mathbb{R}$ and $h_i(\cdot) : \mathbb{R}^{n_i} \times \mathbb{R}^{p_i} \to \mathbb{R}^{m_i}$, consider possibly nonlinear nominal dynamics. Nonlinear dynamics can also include known relationships with parent subsystems by means of the interconnection variables. Instead, $w_i(\cdot) : \mathbb{R}^{p_i} \to \mathbb{R}^{n_i}$ represents the unknown possibly nonlinear coupling among subsystems and includes also modeling uncertainties.

Remark 1. *The considered class of nonlinear functions is general: the only constraints are the matched dependence on the control input and the fact that the subsystems are input-decoupled. These two constraints are necessary for the design of the local tube-based controller in Section IV.*

We assume that the state vector is completely measurable. On the other hand, the distributed FD architecture monitors a state vector $\tilde{x}_{[i]}$ which is extended with respect to the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2016.2535724, IEEE Transactions on Automatic Control

controlled one, since in addition to $x_{[i]}$ it includes some variables $x_{[j,s]}$, $j \in \mathcal{N}_i$, that it "'shares"' with parent subsystems. These variables are a subset of the interconnection variables $\psi_{[i]}$ influencing the dynamics of i and are directly measured by the diagnoser monitoring the i-th subsystem. We call *shared* variables of i both the variables belonging to parents subsystems monitored also by subsystem i, and the variables of subsystem i monitored by children subsystems.

Remark 2. *In this paper, the structure of the subsystems, and hence the decomposition of the large-scale system and the choice of the variables that can be shared, is assumed to be given a priori. An in-depth discussion about optimality of the decomposition is out of the scope of this paper. Since shared variables are monitored by more than one subsystem, it is reasonable that they represent a connection between subsystems.*

Therefore, the model of the system dynamics exploited by the i-th local diagnoser can be described as:

$$\begin{aligned}\tilde{\Sigma}_{[i]}: \quad \tilde{x}^+_{[i]} =& \tilde{A}_{ii}\tilde{x}_{[i]} + \tilde{B}_i[\tilde{g}_i(\tilde{x}_{[i]}, \tilde{\psi}_{[i]}, u_{[i]}) + \tilde{h}_i(\tilde{x}_{[i]}, \tilde{\psi}_{[i]})] \\ &+ \tilde{w}_i(\tilde{\psi}_{[i]}) + \phi_i(\tilde{x}_{[i]}, \tilde{\psi}_{[i]}, u_{[i]}, t) \qquad (2a)\\ y_{[i]} =& \tilde{x}_{[i]} + \varrho_{[i]} \qquad (2b)\end{aligned}$$

where $\tilde{x}_{[i]} \in \mathbb{R}^{\tilde{n}_i}$, $u_{[i]} \in \mathbb{R}^{m_i}$, $y_{[i]} \in \mathbb{R}^{\tilde{n}_i}$ and $\varrho_{[i]} \in \mathbb{R}^{\tilde{n}_i}$, $i \in \mathcal{M}$, are the local state, input, output and unknown measurement error, respectively, for diagnosis purposes. The vector of interconnection variables $\tilde{\psi}_{[i]} \in \mathbb{R}^{\tilde{p}_i}$ collects any state and input variable of the parents subsystems influencing the dynamics of $\tilde{\Sigma}_{[i]}$, namely the variables $\psi_{[i]}$ not measured by the i-th diagnoser, plus any state and input variable of $j \in \mathcal{N}_i$ influencing the dynamics of the shared variables of i not controlled by i. As a consequence, the state matrix A_{ii} is extended to $\tilde{A}_{ii}$ to describe the linear dynamics of the state $\tilde{x}_{[i]}$, and similarly $\tilde{B}_i$ and functions $\tilde{g}_i$, $\tilde{h}_i$ and $\tilde{w}_i$, $i \in \mathcal{M}$. The fault detection model may also consider more complex dynamics (compared to the control model) by means of the general nonlinear functions $\tilde{g}_i$ and $\tilde{h}_i$. Instead, the function $\phi_i(\cdot) : \mathbb{R}^{\tilde{n}_i} \times \mathbb{R}^{\tilde{p}_i} \times \mathbb{R}^{m_i} \times \mathbb{R} \to \mathbb{R}^{\tilde{n}_i}$ represents the fault-function, capturing deviations of the dynamics of $\tilde{\Sigma}_i$ from the nominal healthy dynamics. Note that $\tilde{x}_{[i]}$ and $\tilde{\psi}_{[i]}$ are defined in a way such that computing the left hand side of (2) requires at most information from subsystems $\Sigma_{[j]}$, $j \in \mathcal{N}_i$. In other words only transmission of information from parent to child subsystems is required. This is a notable feature of the proposed approach. The following assumptions are in place.

Assumption 1. *(I) The pair (A_{ii}, B_i) is stabilizable, $\forall i \in \mathcal{M}$.*

(II) Subsystems $\Sigma_{[i]}$, $i \in \mathcal{M}$ are subject to the constraints

$$x_{[i]} \in \mathbb{X}_i,\ u_{[i]} \in \mathbb{U}_i,\ \varrho_{[i]} \in \mathbb{O}_i\,, \qquad (3)$$

where $\mathbb{X}_i$, $\mathbb{U}_i$ and $\mathbb{O}_i$ are compact, convex and contain the origin in their nonempty interior. Constraints (3) *also induce suitable state constraints on $\tilde{\Sigma}_{[i]}$, $i \in \mathcal{M}$, namely $\tilde{\mathbb{X}}_i$, collecting all the possible values that each component of the vector $\tilde{x}_{[i]}$ can have. Similarly, we denote with Ψ_i (resp. $\tilde{\Psi}_i$) constraints induced on interconnection variables $\psi_{[i]}$ (resp. $\tilde{\psi}_{[i]}$), i.e. they collect all possible values that variables $\psi_{[i]}$ (resp. $\tilde{\psi}_{[i]}$) can assume, given the state constraints in* (3)*.*

(III) Functions $w_i(\cdot)$ are bounded for all $i \in \mathcal{M}$, i.e. there are bounded sets $\mathbb{W}_i \subset \mathbb{R}^{n_i}$ such that $w_i(\Psi_i) \subseteq \mathbb{W}_i$. Moreover if $\bar{\Psi}_i \subset \hat{\Psi}_i$ then $w_i(\bar{\Psi}_i) \subset w_i(\hat{\Psi}_i)$.

(IV) Functions $g_i(x_{[i]}, \psi_{[i]})$ are such that

$$\mathbb{G}_i = \sup_{x_{[i]} \in \mathbb{X}_i, \psi_{[i]} \in \Psi_i} \frac{1}{\left|g_i(x_{[i]}, \psi_{[i]})\right|} < +\infty.$$

(V) The measurement error $\varrho_{[i]}$ is bounded for all $i \in \mathcal{M}$ at each time t, i.e. $|\varrho_{[i]}| \leq \bar{\varrho}_{[i]}$ component-wise.

Now, let us provide a formal characterization of the system's decomposition already described in qualitative terms.

Definition 2 ([3])**.** *A decomposition of the LSS into subsystems $\Sigma_{[i]}$, $i \in \mathcal{M}$ is said* non-overlapping *if no state variables are shared between subsystems. Otherwise, the decomposition is termed* overlapping.

In this section, we have introduced the models and the two different decompositions of the LSS we are going to consider. For what concerns the control architecture, a *non-overlapping* decomposition is defined, so that each state component is controlled by only one local controller. On the other hand, an *overlapping* decomposition is proposed for the FD framework, which implies that the shared state variables may be monitored by more than one local diagnosers. In the following sections, we explain how to design a control and a FD architectures suitable for a PnP framework.

IV. Nonlinear tube-based distributed MPC

In this section, we illustrate the proposed distributed tube-based MPC controller. We design the controller so that it is able to guarantee stability of the LSS interconnected subsystems both during the healthy behaviour (when no faults are acting on the LSS) and during the reconfiguration process (when a faulty subsystem is detected and subsequently unplugged). More specifically, we derive the DiMPC controller such that it preserves overall feasibility and stability even when a faulty subsystem is disconnected.

Concerning the control architecture, we consider a non-overlapping decomposition of the LSS. Note that, in order to design the local controllers, the model in (1) is used where $w_i(\cdot)$ represents coupling terms only. In the following, we propose a distributed controller that can be designed in a PnP fashion by treating parent subsystems as bounded disturbances. Only for design purposes, as in [29], we define a nominal model for each subsystem (1)

$$\hat{\Sigma}_{[i]}: \quad \hat{x}^+_{[i]} = A_{ii}\hat{x}_{[i]} + B_i v_{[i]}\,, \qquad (4)$$

where $v_{[i]}$ is the input. As in [29] our goal is to relate inputs $v_{[i]}$ in (4) to $u_{[i]}$ in (1) and compute sets $\mathbb{Z}_i \subseteq \mathbb{X}_i$, $i \in \mathcal{M}$ such that

$$x_{[i]}(0) \in \hat{x}_{[i]}(0) \oplus \mathbb{Z}_i \Rightarrow x_{[i]}(t) \in \hat{x}_{[i]}(t) \oplus \mathbb{Z}_i,\ \forall t \geq 0. \quad (5)$$

In other terms, as in [18] and [19], we want to confine $x_{[i]}(t)$ in a tube around $\hat{x}_{[i]}(t)$ of section $\mathbb{Z}_i$. Assume that if $x_{[i]} \in \mathbb{Z}_i$ there exists $u_{[i]} = \bar{\kappa}_i(x_{[i]}) : \mathbb{Z}_i \to \mathbb{U}_i$ such that $x^+_{[i]} \in \mathbb{Z}_i$,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2016.2535724, IEEE Transactions on Automatic Control

$\forall x_{[j]} \in \mathbb{X}_j,\ j \in \mathcal{N}_i$. Therefore if $x_{[i]} \in \hat{x}_{[i]} \oplus \mathbb{Z}_i$ and the controller

$$\mathcal{C}_{[i]} : u_{[i]} = g_i(x_{[i]}, \psi_{[i]})^{-1}[-h_i(x_{[i]}, \psi_{[i]}) + v_{[i]} + \bar{\kappa}_i(x_{[i]} - \bar{x}_{[i]})] \quad (6)$$

is used, where $\bar{x}_{[i]} = \hat{x}_{[i]}$, then, for all $v_{[i]}$, we have $x^+_{[i]} \in \hat{x}^+_{[i]} \oplus \mathbb{Z}_i$. Controller $\mathcal{C}_{[i]}$ is based on the well-known idea of "canceling" the nonlinearities in the state equations. This is possible because in (1) the nonlinear terms are matched, i.e. they can be directly modified through the control input $u_{[i]}$ [30].

Remark 3. *We highlight that the proposed controller can be easily generalized to the case where $w_i(\cdot)$ represents both coupling terms and model uncertainties. We refer the interested reader to Chapter 7 of [31] where robustness has been studied for linear LSSs.*

We note that controller $\mathcal{C}_{[i]}$ is *distributed* since it depends on the state variables of parent subsystems by means of the interconnection variables, that have to be communicated during online phases between neighbouring control stations. Following [29], the next goal is to compute tightened constraints $\hat{\mathbb{X}}_i \subseteq \mathbb{X}_i$ and $\mathbb{V}_i \subseteq \mathbb{U}_i$ in order to guarantee that

$$\hat{x}_{[i]} \in \hat{\mathbb{X}}_i \text{ and } v_{[i]} \in \mathbb{V}_i \Rightarrow x^+_{[i]} \in \mathbb{X}_i \text{ and } u_{[i]} \in \mathbb{U}_i,$$

at all time instants. Tightened state constraints must satisfy the following inclusions

$$\hat{\mathbb{X}}_i \oplus \mathbb{Z}_i \subseteq \mathbb{X}_i\,, \quad (7a)$$

$$\mathbb{G}_i\,(\mathbb{H}_i \oplus \mathbb{V}_i \oplus \mathbb{U}_{z_i}) \subseteq \mathbb{U}_i\,, \quad (7b)$$

where $\mathbb{H}_i = h_i(\mathbb{X}_i, \Psi_i)$ and $\mathbb{U}_{z_i} = \bar{\kappa}_i(\mathbb{Z}_i)$. Obviously, as in nonlinear tube-based MPC theory, the evaluation of sets $\mathbb{G}_i$ and $\mathbb{H}_i$ can be very challenging. Estimates of these sets can be obtained using methods of reachability analysis for nonlinear systems, as those discussed in [32]. Therefore, since we want to stabilize the nominal subsystems (4) and to guarantee satisfaction of tightened state constraints, we need to solve online the following *local* MPC problem $\mathbb{P}^N_i(x_{[i]}(t))$:

$$\min_{\substack{\hat{x}_{[i]}(0) \\ v_{[i]}(0:N_i-1)}} \sum_{k=0}^{N_i-1} \ell_i(\hat{x}_{[i]}(k), v_{[i]}(k)) + V_{f_i}(\hat{x}_{[i]}(N_i)) \quad (8a)$$

$$x_{[i]}(t) - \hat{x}_{[i]}(0) \in \mathbb{Z}_i \quad (8b)$$

$$\hat{x}_{[i]}(k+1) = A_{ii}\hat{x}_{[i]}(k) + B_i v_{[i]}(k) \quad k \in 0 : N_i - 1 \quad (8c)$$

$$\hat{x}_{[i]}(k) \in \hat{\mathbb{X}}_i,\ v_{[i]}(k) \in \mathbb{V}_i \quad k \in 0 : N_i - 1 \quad (8d)$$

$$\hat{x}_{[i]}(N_i) \in \hat{\mathbb{X}}_{f_i} \quad (8e)$$

In (8), $N_i > 0$ is the control horizon, $\ell_i(\cdot) : \mathbb{R}^{n_i \times m_i} \to \mathbb{R}_{0+}$ is the stage cost, $V_{f_i}(\cdot) : \mathbb{R}^{n_i} \to \mathbb{R}_{0+}$ is the final cost and $\hat{\mathbb{X}}_{f_i}$ is the terminal set. Furthermore, following [29], in (6) we set

$$v_{[i]}(t) = v_{[i]}(0|t), \qquad \bar{x}_{[i]}(t) = \hat{x}_{[i]}(0|t) \quad (9)$$

where $v_{[i]}(0|t)$ and $\hat{x}_{[i]}(0|t)$ are optimal values of the variables $v_{[i]}(0)$ and $\hat{x}_{[i]}(0)$ in the MPC-i problem (8). Note that in (9) we defined the variable $\bar{x}_{[i]}$ depending on the nominal state $\hat{x}_{[i]}$, i.e. the state of the dynamics of the subsystem $\Sigma_{[i]}$ without coupling terms. Note also that the re-definition of $\bar{x}_{[i]}$ as in (9) is at the core of the tube-MPC scheme proposed in [29].

Algorithm 1 summarizes the steps needed for computing function $\bar{\kappa}_i(\cdot)$ in (6), sets $\mathbb{Z}_i$, $\mathbb{U}_{z_i}$, $\hat{\mathbb{X}}_i$, $\mathbb{V}_i$, $\hat{\mathbb{X}}_{f_i}$ and functions $\ell_i(\cdot)$ and $V_{f_i}(\cdot)$. During the design phases, the sets $\mathbb{X}_i$ are communicated to child subsystems, while sets $\mathbb{X}_j$ are received from fathers.

Algorithm 1 Design of controller $\mathcal{C}_{[i]}$ for subsystem $\Sigma_{[i]}$

Input: A_{ii}, B_i, $\mathbb{X}_i$, $\mathbb{U}_i$, $g_i(\cdot)$, $h_i(\cdot)$, $w_i(\cdot)$, $\mathcal{N}_i$, $\mathcal{F}_i$
Output: controller $\mathcal{C}_{[i]}$

(I) Send sets $\mathbb{X}_i$ to child subsystems $j \in \mathcal{F}_i$
(II) Receive sets $\mathbb{X}_j$ from parent subsystems $j \in \mathcal{N}_i$
(III) Compute the set

$$\mathbb{W}_i = w_i(\Psi_i) \quad (10)$$

and choose $\bar{\mathbb{Z}}^0_i$ such that $\mathbb{X}_i \supseteq \bar{\mathbb{Z}}^0_i \supseteq \mathbb{W}_i \oplus B_{\omega_i}(0)$ for a sufficiently small $\omega_i > 0$. If $\bar{\mathbb{Z}}^0_i$ does not exist, then **stop** (the controller $\mathcal{C}_{[i]}$ cannot be designed)
(IV) Check the LP feasibility condition in Step (ii) of Algorithm 1 in [19]. If it is not verified, then **stop** (the controller $\mathcal{C}_{[i]}$ cannot be designed)
(V) Execute Steps (iii) and (iv) of Algorithm 1 in [19]. They provide the MPC-i problem and the function $\bar{\kappa}_i(\cdot)$ defined as in (25) in [19]

Steps (IV) and (V) of Algorithm 1, that provide constraints in (7), are the most computationally expensive because involve Minkowski sums and differences of polytopic sets. The interested reader is referred to Sections 3.1-3.3 in [19], where we show how to avoid burdensome computations exploiting results from [33] and how to compute a suitable function $\bar{\kappa}_i$ in (6) through LP. We also highlight that Step (IV) is the core of the algorithm: by checking the LP feasibility condition in Step (ii) of Algorithm 1 in [19], we are able to verify if there exists a set $\mathbb{Z}_i$ guaranteeing $\mathbb{Z}_i \subseteq \mathbb{X}_i$ and (5). This is possible using a suitable parametrization of the RCI set $\mathbb{Z}_i$, as proposed in [33]. Note also that, by construction, $\mathbb{W}_i \subseteq \mathbb{Z}_i$ and, therefore, the condition $\mathbb{Z}_i \subseteq \mathbb{X}_i$ is more difficult to fulfill for large sets $\mathbb{W}_i$ modeling coupling uncertainties.

Next, we give the main results on stability and constraints satisfaction for the network of subsystems controlled by distributed controllers $\mathcal{C}_{[i]}$. It is in fact important for the proposed fault-tolerance scheme to be able to work in presence of disturbances, also in healthy conditions.

Theorem 1. *Let Assumption 1 hold. Assume state-feedback controllers $\mathcal{C}_{[i]}$ are computed using Algorithm 1 and define $\mathbf{x}(t) = (x_{[1]}, \ldots, x_{[M]})$. Let $\mathbb{X}^N_i = \{s_{[i]} \in \mathbb{X}_i :$ (8) is feasible for $x_{[i]}(t) = s_{[i]}\}$ be the feasibility region for the MPC-i problem and $\mathbb{X}^N = \prod_{i \in \mathcal{M}} \mathbb{X}^N_i$. Then, the origin of the closed-loop system is asymptotically stable. Moreover, $\mathbb{X}^N$ is a region of attraction for the origin and $\mathbf{x}(0) \in \mathbb{X}^N$ guarantees state and input constraints are fulfilled at all time instants.*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2016.2535724, IEEE Transactions on Automatic Control

Proof: The proof of Theorem 1 is given in Appendix A. ■

Remark 4. *Notice that Algorithm 1 provides an off-line decentralized procedure for designing distributed PnP regulators and that it can be executed in parallel for all subsystems. Therefore, as shown in [18], [19] and as we will see jointly with the FD architecture presented in Sections VII and VII-B, plug-in or unplugging operations involve only the update of a limited number of controllers. Differently from [18] and [19] (where only linear subsystems have been considered), the proposed regulator allows to control subsystems described by matched nonlinearities and nonlinear couplings with parents.*

V. The Fault Detection Architecture

In this section, we design a distributed FD architecture for the considered PnP framework. Each subsystem is equipped with a local diagnoser. According to the classical model-based FD approach, an estimate $\hat{\tilde{x}}_{[i]}$ of the local state variables is computed; the estimation error $\epsilon_{[i]} \triangleq y_{[i]} - \hat{\tilde{x}}_{[i]}$ is compared component-wise with a suitable time-varying detection threshold $\bar{\epsilon}_{[i]} \in \mathbb{R}_+^{\tilde{n}_i}$, hence obtaining a local fault decision classifying the status of the subsystem either as healthy or faulty. If the residual crosses the threshold, under an appropriate setting we can conclude that a fault has occurred. The condition $|\epsilon_{[i,k]}(t)| \leq \bar{\epsilon}_{[i,k]}(t), \forall k = 1 : \tilde{n}_i$ is a necessary (but generally not sufficient) condition for the hypothesis $\mathcal{H}_i$: "Subsystem $\tilde{\Sigma}_{[i]}$ is healthy". If the condition is violated at some time instant, then the hypothesis $\mathcal{H}_i$ is falsified.

In the PnP framework, the diagnosers are designed so to guarantee the absence of false alarms and the convergence of the estimator error both during healthy operating conditions and during the reconfiguration process: the healthy subsystems diagnosers have to continue to work properly also when the faulty subsystem(s) is (are) unplugged and then plugged-in after problem solution.

A. The Fault Detection Estimator

For detection purposes, each subsystem is equipped with a local nonlinear estimator, based on the local model $\tilde{\Sigma}_{[i]}$ in (2). The k-th non-shared state variable of $\tilde{\Sigma}_{[i]}$ can be estimated as

$$\begin{aligned}\hat{\tilde{x}}^+_{[i,k]} =& \lambda(\hat{\tilde{x}}_{[i,k]} - y_{[i,k]}) + \tilde{A}_{ii,k} y_{[i]} + \tilde{B}_{i,k}[\tilde{g}_i(y_{[i]}, z_{[i]}, u_{[i]}) \\ &+ \tilde{h}_i(y_{[i]}, z_{[i]})],\end{aligned}$$

where the filter parameter is chosen in the interval $0 < \lambda < 1$ in order to guarantee convergence properties, $z_{[i]} = \tilde{\psi}_{[i]} + \theta_{[i]}$ is the vector of measured interconnection variables available for diagnosis, $\theta_{[i]}$ collects the involved measurement error $\varrho_{[j]}$, $j \in \mathcal{N}_i$, $\tilde{A}_{ii,k}$ and $\tilde{B}_{i,k}$ are the k-th row of matrices $\tilde{A}_{ii}$ and $\tilde{B}_i$, respectively. Using the shared variable $\tilde{x}_{[i,k_i]} = \tilde{x}_{[j,k_j]}$, where k_i and k_j are the k_i-th and k_j-th components of vectors $\tilde{x}_{[i]}$ and $\tilde{x}_{[j]}$, respectively, we can take advantage of the redundancy by using a kind of deterministic consensus protocol (see [13], [15]). In the following, $\mathbb{S}^k$ is the set of subsystems $\tilde{\Sigma}_{[i]}$ sharing a given state variable k of the LSS. The estimates of shared variables are provided by

$$\begin{aligned}\hat{\tilde{x}}^+_{[i,k_i]} =& \lambda(\hat{\tilde{x}}_{[i,k_i]} - y_{[i,k_i]}) + \sum_{j \in \mathbb{S}^k} W^k_{i,j} \Big[\hat{\tilde{x}}_{[j,k_j]} - \hat{\tilde{x}}_{[i,k_i]} \\ &+ \tilde{A}_{jj,k_j} y_{[j]} + \tilde{B}_{j,k_j}[\tilde{g}_j(y_{[j]}, z_{[j]}, u_{[j]}) + \tilde{h}_j(y_{[j]}, z_{[j]})]\Big] \quad (11)\end{aligned}$$

where, for each shared component k, $W^k_{i,j}$ are the components of a row-stochastic matrix W^k, which will be defined in Subsection V-C, and is designed to allow plugging-in and unplugging operations. By now, notice that W^k collects the consensus weights used by $\tilde{\Sigma}_{[i]}$ to weight the terms communicated by $\tilde{\Sigma}_{[j]}$, with $j \in \mathbb{S}^k$, to monitor component k. In fact, as regards variables estimation, each subsystem communicates with parents and children subsystems sharing that variable. We also note that (11) holds also for the case of non-shared variables, since, in this case, $\mathbb{S}^k = \{i\}$, and $W^k_{i,i} = 1$ by definition. In the following, for the sake of simplicity, we drop the subscript of the shared component index k, that is we write $\tilde{x}_{[i,k]}$ instead of $\tilde{x}_{[i,k_i]}$.

B. The detection threshold

In order to define an appropriate threshold for FD, we analyze the dynamics of the local diagnoser estimation error when the subsystem is healthy. Defining W^k such that $\sum_{j \in \mathbb{S}^k} W^k_{i,j} = 1$ and since for shared variables $\forall i, j \in \mathbb{S}^k$ it holds

$$\begin{aligned}&\tilde{A}_{ii,k}\tilde{x}_{[i]} + \tilde{B}_{i,k}[\tilde{g}_i(\tilde{x}_{[i]}, \tilde{\psi}_{[i]}, u_{[i]}) + \tilde{h}_i(\tilde{x}_{[i]}, \tilde{\psi}_{[i]})] \\ &\quad = \tilde{A}_{jj,k}\tilde{x}_{[j]} + \tilde{B}_{j,k}[\tilde{g}_j(\tilde{x}_{[j]}, \tilde{\psi}_{[j]}, u_{[j]}) + \tilde{h}_j(\tilde{x}_{[j]}, \tilde{\psi}_{[j]})],\end{aligned}$$

the k-th state estimation error dynamics is given by

$$\begin{aligned}\epsilon^+_{[i,k]} = \sum_{j \in \mathbb{S}^k} W^k_{i,j} \Big[&\lambda\epsilon_{[j,k]} - \tilde{A}_{jj,k}\varrho_{[j]} + w_{j,k}(\tilde{\psi}_{[j]}) \\ &+ \tilde{B}_{j,k}(\Delta\tilde{g}_{j,k} + \Delta\tilde{h}_{j,k}) - \lambda\varrho_{[j,k]}\Big] + \lambda\varrho_{[i,k]} + \varrho^+_{[i,k]},\end{aligned}$$

where $\Delta\tilde{g}_{j,k} \triangleq \tilde{g}_{j,k}(\tilde{x}_{[j]}, \tilde{\psi}_{[j]}, u_{[j]}) - \tilde{g}_{j,k}(y_{[j]}, z_{[j]}, u_{[j]})$ and $\Delta\tilde{h}_{j,k} \triangleq \tilde{h}_{j,k}(\tilde{x}_{[j]}, \tilde{\psi}_{[j]}) - \tilde{h}_{j,k}(y_{[j]}, z_{[j]})$.

As in [15], using the triangular inequality, we can bound the estimation error, guaranteeing no false-positive alarms. By taking the absolute value of $\epsilon^+_{[i,k]}$ component-wise, we get

$$\begin{aligned}|\epsilon^+_{[i,k]}| \leq \sum_{j \in \mathbb{S}^k} W^k_{i,j} \Big[&\lambda|\epsilon_{[j,k]}| + |\tilde{A}_{jj,k}\varrho_{[j]}| + \lambda|\varrho_{[j,k]}| \\ &+ |\tilde{B}_{j,k}(\Delta\tilde{g}_{j,k} + \Delta\tilde{h}_{j,k})| + |w_{j,k}(\tilde{\psi}_{[j]})|\Big] \\ &+ \lambda|\varrho_{[i,k]}| + |\varrho^+_{[i,k]}|.\end{aligned}$$

Therefore, we define the following time-varying threshold $\bar{\epsilon}_{[i,k]}$ that *can be computed in a distributed way*:

$$\begin{aligned}\bar{\epsilon}^+_{[i,k]} = \sum_{j \in \mathbb{S}^k} W^k_{i,j} \Big[&\lambda\bar{\epsilon}_{[j,k]} + \Big|\tilde{A}_{jj,k}\Big| \bar{\varrho}_{[j]} + \bar{w}_{j,k}(z_{[j]}) \\ &+ \Big|\tilde{B}_{j,k}\Big| (\Delta\bar{g}_j + \Delta\bar{h}_j) + \lambda\bar{\varrho}_{[j,k]}\Big] + \lambda\bar{\varrho}_{[i,k]} + \bar{\varrho}^+_{[i,k]}, \quad (12)\end{aligned}$$

where $\Delta\bar{g}_j = \max_{\tilde{x}_{[j]} \in \tilde{\mathbb{X}}_j, \tilde{\psi}_{[j]} \in \tilde{\Psi}_j} |\Delta\tilde{g}_j(t)|$ and $\Delta\bar{h}_j = \max_{\tilde{x}_{[j]} \in \tilde{\mathbb{X}}_j, \tilde{\psi}_{[j]} \in \tilde{\Psi}_j} ||\Delta\tilde{h}_j(t)||_\infty$. It is worth noting that Assumption 1 implies that the state and input variables are

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2016.2535724, IEEE Transactions on Automatic Control

bounded; hence all quantities in (12) are bounded as well; moreover, it is possible to define $\forall i,\ k$ at each time step a bound $\bar{w}_{i,k}$, so that $\left|w_{i,k}(z_{[i]})\right| \leq \bar{w}_{i,k}(z_{[i]})$; $\bar{\varrho}_{[i,k]}$ is defined in Assumption 1. The threshold dynamics (12) can be initialized with $\bar{\epsilon}_{[i,k]}(0) = \bar{\varrho}_{[i,k]}(0)$.

Remark 5. *For FD purposes, the communication between subsystems is limited. It is not necessary, in general, that each diagnoser knows the model of parent subsystems. Instead, in the shared case* (11)*, it is sufficient that each subsystem $\tilde{\Sigma}_{[j]}$ sends to subsystems $i \in \mathbb{S}^k$ only a limited number of variables: the interconnection variables $z_{[i]}$ and the consensus terms for estimates ($\hat{\tilde{x}}_{[j,k_j]}$ and $\tilde{A}_{jj,k_j} y_{[j]} + \tilde{B}_{j,k_j}[\tilde{g}_j(y_{[j]}, z_{[j]}, u_{[j]}) + \tilde{h}_j(y_{[j]}, z_{[j]})$) and thresholds ($\lambda(\bar{\epsilon}_{[j,k]} + \bar{\varrho}_{[j,k]}) + \left|\tilde{A}_{jj,k}\right| \bar{\varrho}_{[j]} + \left|\tilde{B}_{j,k}\right| (\Delta\bar{g}_j + \Delta\bar{h}_j) + \bar{w}_{j,k}(z_{[j]})$), locally computed.*

The threshold in (12) guarantees the absence of false-positive alarms before the occurrence of the fault caused by the uncertainties. On the other hand, this is a conservative result since it does not allow to detect faults whose magnitude is lower than the uncertainties magnitude in the system dynamics. This issue is formalized in the fault detectability section (Section VI), where we consider also the issue that the fault may be hidden by the control action.

C. The consensus matrix

In this subsection, we explain how to properly define the consensus matrix in order to allow for PnP operations. Consensus is applied to the shared variables, i.e. state variables representing the interconnection between two or more subsystems, measured and monitored by more than one diagnoser. For PnP capabilities, we use a time-varying weighting matrix W^k whose dimension is equal to the maximum number of subsystems that can be plugged in sharing that variable. This is not a restrictive assumption since it is possible to choose a dimension as large as wanted. Each row can have non null elements only on correspondence of connected (plugged-in) subsystems. In the case that, at a given time, the variable is not shared (and hence at most one subsystem is using it) the only non-null weight is the one corresponding to the considered subsystem (this does not affect the convergence of the FD estimator as illustrated in Subsection V-D).

Indeed, the introduction of the proposed time-varying consensus matrix is advantageous from a second perspective. Since the proposed threshold is conservative, it is important to choose it as small as possible. Therefore, in the case of shared variables, similarly as in [34], we design a time-varying consensus-weighting matrix W^k able to minimize the adaptive threshold with respect to the consensus weights, by choosing the smallest threshold term from all the threshold additive terms in (12). In this consensus protocol, it is convenient to weight more the subsystem which has got the lowest threshold component, hence the subsystem that has lower uncertainty in its measurements and in the local model. These aims can be achieved by defining the following consensus matrix, where each (i,j)-th component is computed as:

$$W^k_{i,j} = \begin{cases} 1 & \text{if } j = \arg\min_{j \in \mathbb{S}^k} \lambda(\bar{\epsilon}_{[j,k]} + \bar{\varrho}_{[j,k]}) + \left|\tilde{A}_{jj,k}\right| \bar{\varrho}_{[j]} \\ & \quad + \left|\tilde{B}_{j,k}\right| (\Delta\bar{g}_j + \Delta\bar{h}_j) + \bar{w}_{j,k}(z_{[j]}) \\ 0 & \text{otherwise} \end{cases} \tag{13}$$

At each time-step each local fault-diagnoser receives estimates and consensus terms of variable $\tilde{x}_{[i,k]}$ only from the subsystems sharing it at that specific time. Then, it selects the contribution affected by "smaller uncertainty". It is worth noting that the set $\mathbb{S}^k$ is time-varying and collects only the subsystems that share variable k and that are connected to the LSS at that specific time instant. As briefly discussed in Section VI, fault-detectability may be improved by this approach. The intuitive idea is that the consensus approach used to estimate the shared variables allows to decrease the uncertainty on those variables, thus reducing the conservativeness of the proposed thresholds and improving fault detectability. The shared variables may then be chosen in order to improve the detectability of some faults we are interested to detect. In the architecture proposed in this paper using the designed time-varying consensus matrix, sharing some variables always improves (or does not change) detectability properties. Given the particular structure of the considered networked subsystems with bounded coupling, the choice of the shared variables is constrained by Assumption 1(III). In this paper anyway, the structure of the subsystems, and so the decomposition of the large-scale system and the choice of the variables that can be shared, is assumed to be given a priori.

D. Estimator convergence

Next, we address the convergence properties of the overall estimator before the possible occurrence of a fault, that is for $t < T_0$. Towards this end, we introduce a vector formulation of the state error equation for sake of compacting the notation, just for analysis purposes. Specifically, we introduce the extended estimation error vector $\epsilon_{k,E}$, which is a column vector collecting the estimation error vectors of the N_k subsystems sharing the k-th state component: $\epsilon_{k,E} \triangleq \text{col}\left(\epsilon_{[j,k]} :\ j \in \mathbb{S}^k\right)$. Hence, the dynamics of $\epsilon_{k,E}$ can be described as:

$$\epsilon^+_{k,E} = W^k \Big[\lambda\epsilon_{k,E} + \tilde{A}_{k,E}\varrho_E + \tilde{B}_{k,E}(\Delta\tilde{g}_E + \Delta\tilde{h}_E) + w_{k,E} - \lambda\varrho_{k,E}\Big] + \lambda\varrho_{k,E} + \varrho^+_{k,E}, \tag{14}$$

where $\varrho_{k,E}$ is a column vector, collecting the corresponding k_j value of vector $\varrho_{[j]}$, i.e. $\varrho_{[j,k_J]}$, for each $j \in \mathbb{S}^k$; $\tilde{A}_{k,E}$ is a block matrix with N_k rows and $n_E = \sum_{j=1}^{N_k} \tilde{n}_J$ columns, $j \in \mathbb{S}^k$, where the elements on the diagonal are the row vectors $\tilde{A}_{jj,k}$; $\tilde{B}_{k,E}$ is defined in an analogous way. Finally, ϱ_E, $\Delta\tilde{g}_E$, $\Delta\tilde{h}_E$ and u_E are column vectors collecting the vectors $\varrho_{[j]}$, $\Delta\tilde{g}_j$, $\Delta\tilde{h}_j$ and $u_{[j]}$, with $j \in \mathbb{S}^k$, respectively, $w_{k,E}$ is defined in an analogous way. The following convergence result is now in place.

Proposition 1. *System* (14)*, where the consensus matrix is given by* (13)*, is BIBO stable.*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2016.2535724, IEEE Transactions on Automatic Control

Proof: The proof is carried out exploiting the one reported in [34] in a purely distributed fault-diagnosis framework. Specifically, since W^k is a stochastic matrix, its norm is always equal to 1. Therefore, since $0 < \lambda < 1$, then also $||\lambda W^k(t)|| \leq \gamma < 1$, with $0 < \gamma < 1$. Let us define:

$$U_{k,E}(t) = W^k(t) \Big[\tilde{A}_{k,E}\varrho_E(t) + \tilde{B}_{k,E}(\Delta\tilde{g}_E(t) + \Delta\tilde{h}_E(t)) + w_{k,E}(t) - \lambda\varrho_{k,E}(t)] + \lambda\varrho_{k,E}(t) + \varrho_{k,E}(t+1).$$

We have:

$$\begin{aligned} &||\epsilon_{k,E}(t+1)|| \leq ||\lambda W^k(t)\epsilon_{k,E}(t)|| + ||U_{k,E}(t)|| \\ &\leq ||\lambda W^k(t)||||\lambda W^k(t-1)|| \dots ||\lambda W^k(0)||||\epsilon_{k,E}(0)|| \\ &+ \sum_{j=1}^{t} ||\lambda W^k(t)||||\lambda W^k(t-1)|| \dots ||\lambda W^k(j)||||U_{k,E}(j)|| \\ &\leq \gamma^t||\epsilon_{k,E}(0)|| + \sum_{j=1}^{t}\gamma^{t-j}||U_{k,E}(j)|| \\ &\leq \frac{1}{1-\gamma}\sup_{j\geq 1}||U_{k,E}(j)|| \end{aligned}$$

For $t \to \infty$, the state of the unforced system converges to zero and the series converges to a bounded value (see results in [35]). Moreover, using results in [36] for unforced systems, we can state that a system $x(t+1) = A(t)x(t)$, with $A(t) \in \text{convh}(A_1, \dots, A_N)$ is exponentially stable iff $\exists$ a sufficiently large integer q such that $||A_{i_1} A_{i_2} \dots A_{i_q}|| \leq \gamma < 1$, $\forall (i_1, \dots, i_q) \in \{1, \dots, N\}^q$. In our case, therefore, we only need to analyze matrix $W^k(t)$. Since each row of $W^k(t)$ has all null elements except one equal to 1, the product $W^k(t)W^k(t-1)\dots W^k(0)$ is a stochastic matrix. Hence, since $0 < \lambda < 1$, we have $||\lambda^t(W^k(t)W^k(t-1)\dots W^k(0))|| < 1$ and the hypothesis is satisfied. Finally, since all the uncertain terms are bounded, then the discrete-time system (14) is BIBO stable. ■

VI. Fault Detectability Analysis

In this section, we analyze the fault detectability properties of the proposed FD architecture. In particular, we highlight the effects of the control input on fault detectability conditions. Let us now consider the case of a faulty subsystem, that is, suppose that a fault $\phi(\cdot)$ occurs at an unknown time $t = T_0$ on the k-th state variable. In the general case of a shared variable, $\phi_{k,E} = \phi_{[\cdot,k]}(1, \dots, 1)^T$ denoting the extended fault function vector collecting for the component k the same fault value for each subsystem sharing the k-th variable. After the occurrence of the fault, for $t > T_0$, the state estimation error dynamics is given by:

$$\epsilon^+_{k,E} = W^k \Big[\lambda\epsilon_{k,E} + \tilde{A}_{k,E}\varrho_E + \tilde{B}_{k,E}(\Delta\tilde{g}_E + \Delta\tilde{h}_E) + w_{k,E} - \lambda\varrho_{k,E}] + \lambda\varrho_{k,E} + \varrho^+_{k,E} + \phi_{k,E}.$$

Then, at a time instant $t_1 > T_0$, the estimation error is

$$\begin{aligned} \epsilon_{k,E}(t_1) = \sum_{h=0}^{t_1-1} &(\lambda W^k(h))^{t_1-1-h}[-W^k(h)\tilde{A}_{k,E}\varrho_E(h) \\ &+ \tilde{w}_{k,E}(h) + W^k(h)\tilde{B}_{k,E}(\Delta\tilde{g}_E(h) + \Delta\tilde{h}_E) \\ &- \lambda W^k(h)\varrho_{k,E}(h) + \lambda\varrho_{k,E}(h) + \varrho_{k,E}(h+1) \\ &+ \phi_{k,E}(h)] + \prod_{h=0}^{t_1-1}(\lambda W^k(h))\epsilon_{k,E}(0)\,. \end{aligned}$$

Now, we derive a sufficient condition in order to characterize a class of faults that can be detected by the proposed FD scheme. In order to detect the occurrence of the fault at a certain time t_1, the following inequality has to be satisfied:

$$|\epsilon_{k,E}(t_1)| > \bar{\epsilon}_{k,E}(t_1),$$

for at least one subsystem $i \in \mathbb{S}^k$. When dealing with vectors, in this paper, the inequality operator is applied component-by-component. Using the triangle inequality and the threshold definition (12), the following is implied

$$|\epsilon_{k,E}(t_1)| \geq -\bar{\epsilon}_{k,E}(t_1) + \left|\sum_{h=T_0}^{t_1-1}[\lambda^{t_1-1-h}\phi_{k,E}(h)]\right|.$$

Since $\phi_{k,E}$ is a vector whose components are all equal to $\phi_k = \phi_{i,k_i} = \phi_{j,k_j}$, it is easy to see that the FD condition $\left|\epsilon_{[i,k]}(t_1)\right| > \bar{\epsilon}_{[i,k]}(t_1)$ is satisfied if

$$\exists t_1 > T_0 : \left|\sum_{h=T_0}^{t_1-1}\lambda^{t_1-1-h}\phi_k(h)\right| > 2\bar{\epsilon}_{[i,k]}(t_1) \qquad (15)$$

for at least one component $k \in \{1 \dots, \tilde{n}_i\}$, thus allowing the detection of a fault at time t_1. Condition (15) implicitly characterizes the class of faults that are detectable by the proposed FD architecture at time t_1. Moreover, thanks to the introduction of the time-varying consensus weighting matrix, the threshold on the right-hand-side of (15) is the smallest one in the set of the proposed conservative thresholds of subsystems sharing the same variable, guaranteeing no false alarms. The choice of a smaller threshold makes it easier the detectability at the general time instant t_1, thus we can say intuitively from (15) that the class of detectable faults at time t_1 is enlarged thanks to this choice.

In the case that the fault detection subsystem are input-decoupled as the control ones, $\Delta\bar{g}_E$ can be computed as $\Delta\bar{g}_E\,|u_E(h)|$. It is then worth emphasizing the influence of the control inputs on the fault detectability condition by rewriting (15) as

$$\begin{aligned} &\left|\sum_{h=T_0}^{t_1-1}\lambda^{t_1-1-h}\phi_{k,E}(\tilde{x}_E, \tilde{\psi}_E, u_E, h)\right| > \\ &2\Big(\sum_{h=0}^{t_1-1}(\lambda W^k(h))^{t_1-1-h}[W^k(h)\Big(\left|\tilde{A}_{k,E}\right|\bar{\varrho}_E(h) + \bar{w}_{k,E}(h) \\ &\quad + \left|\tilde{B}_{k,E}\right|(\Delta\bar{g}_E\,|u_E(h)| + \Delta\bar{h}_E) + \lambda\bar{\varrho}_{k,E}(h)\Big) \\ &\quad + \lambda\bar{\varrho}_{k,E}(h) + \bar{\varrho}_{k,E}(h+1)] + \prod_{h=0}^{t_1-1}(\lambda W^k(h))\epsilon_{k,E}(0)\Big)\,. \end{aligned} \qquad (16)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2016.2535724, IEEE Transactions on Automatic Control

Actually, the norm of the control term $u_E(t_1-1)$ affects the threshold on the right side of the inequality and, in particular, it may have a detrimental effect on the fault detectability by increasing the detection threshold. On the other hand, the control influences also the left part of the condition inequality, by acting on the fault function, which depends directly on $u_E(t_1-1)$ and, by means of $\tilde{x}_E$, it depends also on the past history of the control input. In order to analyze this point, it is possible to rewrite (16) as

$$\left|\sum_{h=T_0}^{t_1-1}(\lambda W^k(h))^{t_1-1-h}W^k(h)\phi_{k,E}(\tilde{x}_E,\tilde{\psi}_E,u_E,h)\right| > 2\Big(\sum_{h=0}^{t_1-1}(\lambda W^k(h))^{t_1-1-h}[W^k(h)\left|\tilde{B}_{k,E}\right|(\Delta\bar{g}_E\,|u_E(h)| + \Delta\bar{h}_E)] + \varsigma_E(h)\Big) \quad (17)$$

where

$$\varsigma_E = 2\Big(\sum_{h=0}^{t_1-1}(\lambda W^k(h))^{t_1-1-h}[W^k(h)\Big(\left|\tilde{A}_{k,E}\right|\bar{\varrho}_E(h) + \bar{w}_{k,E}(h) + \Delta\bar{h}_E) + \lambda\bar{\varrho}_{k,E}(h)\Big) + \lambda\bar{\varrho}_{k,E}(h) + \bar{\varrho}_{k,E}(h+1)] + \prod_{h=0}^{t_1-1}(\lambda W^k(h))\epsilon_{k,E}(0)\Big)$$

is the threshold part that does not depend directly on the extended control input. Therefore, it is constant w.r.t. the control input[2]. As a consequence, the contribution of the control input to detectability properties at a certain time t_1 could be highlighted by deriving the vectors of functions $\left|\phi_{k,E}(x_E,\tilde{\psi}_{k,E},u_E,h)\right|$ and $\left|\tilde{B}_{k,E}\right|(\Delta\bar{g}_E\,|u_E(h)| + \Delta\bar{h}_E)$ w.r.t. the vector u_E norm component-by-component. If it is possible to obtain the derivatives vector of the fault function we want to detect (as example, if it is possible to assume that it is a Lipschitz function w.r.t. the control input norm and to know the Lipschitz constant), then, it is possible to compare the two derivatives for each subsystem $i \in \mathbb{S}^k$. In fact, the right side term is linear w.r.t. to the norm of the control input. Intuitively, if the control input norm makes the magnitude of the fault function grow less than the threshold bounds, then the control input has a detrimental effect on detectability at time step t_1, since it increases the uncertainty threshold terms that hide the fault effects. On the other hand, if the control input norm makes the magnitude of the fault function grow much more than the threshold bounds, then it could be possible to take advantage of the control input effect trying to improve detectability. A detailed analysis of this issue is out of the scope of this paper.

VII. Reconfiguration strategy

In the previous sections, we derived suitable control and fault detection architectures for a PnP framework. We now explain how to use them during plugging-in and unplugging operations. In this section, the reconfiguration of the LSS, in case of detection of a fault in one of the subsystems, is addressed (see Fig. 2 for a visual description). We assume that, when the plant is started, all subsystems are healthy, governed by local controllers designed through Algorithm 1 and monitored by local diagnosers proposed in Section V.

- At a certain time, in subsystem $\tilde{\Sigma}_{[j]}$, one or more residual components may cross the corresponding threshold. We then have local fault detection (see Fig. 2-a)).
- Depending on the specific application context, two distinct actions may turn out to be feasible: i) immediate "disconnection" of the faulty subsystem or ii) continuation of the system operation in "safety mode". As in this paper we deal with an *active distributed fault-tolerant* control scheme, we consider only the first scenario. Subsystem $\tilde{\Sigma}_{[j]}$ is then disconnected from the networked system. This is the *unplugging* step and is shown in Fig. 2-b) in a pictorial way.
- Due to subsystem $\tilde{\Sigma}_{[j]}$ unplugging, the neighboring subsystems have to reconfigure their local controllers and diagnosers. This is described in Fig. 2-c) and explained in Subsection VII-A.
- When subsystem $\tilde{\Sigma}_{[j]}$ has been repaired or replaced, it can be re-plugged in into the networked system and the neighboring subsystems local controllers and diagnosers are retuned in Fig. 2-d) and Subsection VII-B).

In the following, the *unplugging* after fault-detection and the possible *plug-in* after subsystem repair/replacement are addressed separately.

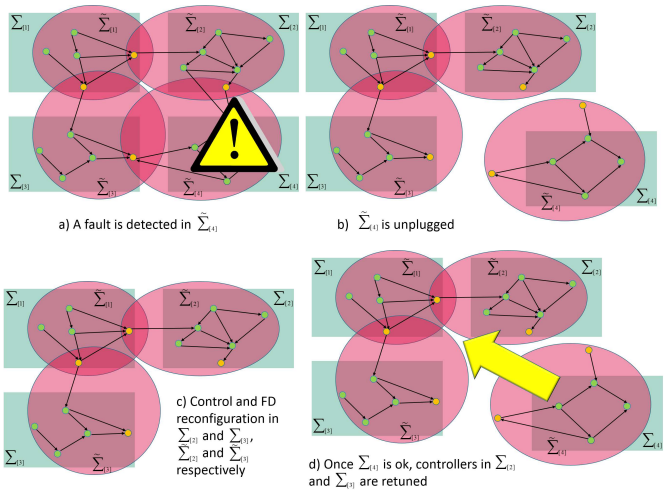


Fig. 2: The reconfiguration process: the a), b), c), d) steps described in Section VII.

A. Subsystem unplugging after fault detection

In this section, we show how to reconfigure local controllers and fault-detectors when a fault is detected in a subsystem. The proposed strategy is based on the isolation of the faulty

[2]This could be not always true since the control input could influence also the bounds of the measurement error and coupling by means of the state dynamics. However in some cases this dependence could be neglected especially when considering conservative bounds.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2016.2535724, IEEE Transactions on Automatic Control

subsystem and on the reconfiguration of controllers and fault-detectors to guarantee closed-loop stability, constraint satisfaction and monitoring of the new network with one less subsystem.

In the following, we describe in depth the needed operations after a fault detection. Let $t = t_1$ the detection time of a fault in the j-th subsystem ($\tilde{\Sigma}_{[j]}$ in the FD architecture and $\Sigma_{[j]}$ in the control architecture), then the faulty subsystem is unplugged and the involved subsystems reconfigured.
As regards the distributed FD, we need to perform the following operations.

- In the children subsystems $i \in \mathcal{F}_j$, for $t \geq t_1$, the components of $\tilde{\psi}_{[i]}$ and $z_{[i]}$ related to subsystem $\tilde{\Sigma}_{[j]}$ become equal to 0. Hence, for $t \geq t_1$, the interconnection variables and measurements related to subsystem $\tilde{\Sigma}_{[j]}$ do not influence the time-behaviour of the state estimation (11) and of the threshold (12) of subsystems $\tilde{\Sigma}_{[i]}$.
- In the children subsystems $i \in \mathcal{F}_j$, the adaptive threshold $\bar{\epsilon}_{[i]}$ is computed through (12) by not considering the coupling terms related to the j-th subsystem when computing $\bar{w}_i$ for $t \geq t_1$.
- In the neighbouring subsystems i, with $i \in \mathcal{F}_j$ or $i \in \mathcal{N}_j$, sharing some variables with $\tilde{\Sigma}_{[j]}$, the weights associated with $\tilde{\Sigma}_{[j]}$ in the consensus matrices W^k computed in (13) are set to zero, that is, $j \notin \mathbb{S}^k$ for $t \geq t_1$ for all the shared variables k. This allows to manage the fact that after unplugging the connected subsystems have not access anymore to the signals from $\tilde{\Sigma}_{[j]}$.

Beyond the above changes in the local estimators embedded in the distributed FD framework as a consequence of the subsystem unplugging after the detection of a fault, the reconfiguration of the control architecture has to be addressed as well. Under Assumption 1-(III), for each $i \in \mathcal{F}_j$, a contraction of the set $\mathcal{N}_i$ takes place, since subsystem $\Sigma_{[i]}$ has one parent less. Then, a contraction takes place also on set $\mathbb{W}_i$ in (10) and the set $\bar{\mathbb{Z}}_i^0$ already computed still verifies the inclusions in Step (III) of Algorithm 1. Therefore, for each $i \in \mathcal{F}_j$, the previous choice of $\bar{\mathbb{Z}}_i^0$ (made before the unplugging) still guarantees the feasibility of the LP problem in Step (IV) of Algorithm 1 which finally implies that there is no need of redesigning the controller $\mathcal{C}_{[i]}$ to keep the overall stability.

In conclusion, thanks to the distributed MPC controllers and distributed fault detectors schemes we designed, the detection of a fault in a subsystem implies the isolation of the faulty subsystem and the reconfiguration of local controllers and fault detectors, at most, of parent and children subsystems. This guarantees that the fault is not propagated in the network.

B. Subsystem plugging-in

The plug-in of a subsystem into the LSS interconnected structure may be needed in case of replacement of a previously unplugged subsystem the fault diagnoser in use before subsystem disconnection can be reused. Since we assumed controllers $\mathcal{C}_{[i]}$ existed for the subsystem and its children when it was connected to the plant, this operation is always feasible as regards the control framework[3]. For what concerns the distributed FD architecture, thanks to the way the time-varying shared variables estimator is defined, the plug-in is always feasible as well.

Remark 6. *Note that, differently from [18], [19], here we do not consider the plugging-in of new subsystems but just the reconnections of subsystems after they have been repaired. Therefore, existence of controllers $\mathcal{C}_{[i]}$ when all subsystems are healthy guarantees that after a plugging-in or unplugging operation in real-time*

- *constraints on the input and states of all subsystems are still fulfilled;*
- *the new mode of operation of the whole plant is asymptotically stable (Theorem 1).*

However, as well known in the hybrid system literature [37], frequent and persistent switching between different modes of operation could compromise asymptotic stability of the whole plant. A remedy could be assuming a minimal dwell-time between consecutive switches [37] although this issue deserves further investigations.

Remark 7. *For what concerns the control, the operations that have to be performed on-line involve the computation of the MPC control input and, in case of reconfiguration operations, the reconfiguration of neighbouring controllers. As regards the fault detection, it is necessary to compute at each sampling time the state estimates and thresholds, including the computation of the time-varying consensus matrix.*

VIII. Examples

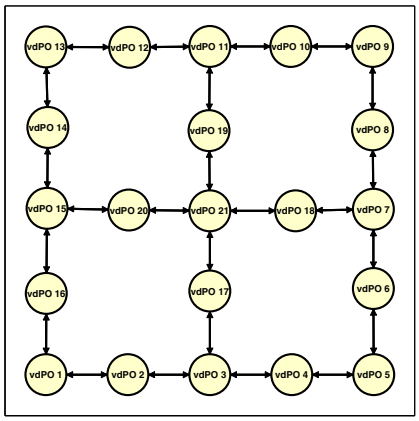


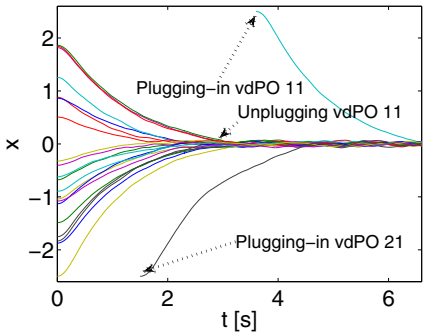
Fig. 3: Matrix composed of coupled van der Pol oscillators.

A. Coupled van der Pol oscillators

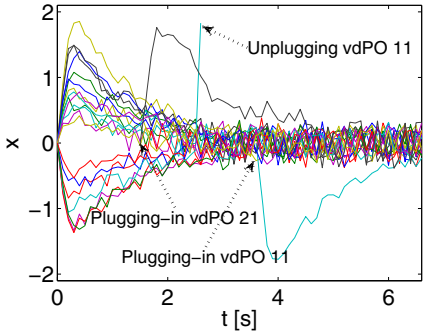
In this example, we apply the proposed methodologies to a matrix of coupled vdPOs as in Figure 3. They can be used to model many oscillating systems in a wide area of applications,

[3]Otherwise, if considering the plug-in of new subsystems, we should check the feasibility of this operation by verifying that the execution of Algorithm 1 for the new subsystem or its children does not stop.

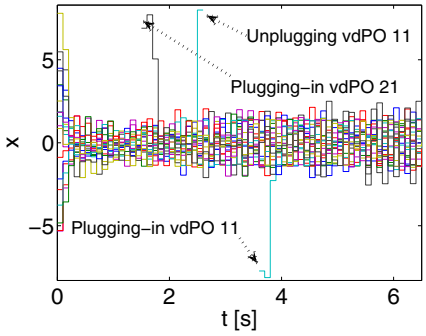
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2016.2535724, IEEE Transactions on Automatic Control



(a) Displacements of the vdPOs, i.e. state $x_{[i,1]}$ for each $i \in \mathcal{M}$.



(b) Velocities of the vdPOs, i.e. state $x_{[i,2]}$ for each $i \in \mathcal{M}$.



(c) Inputs $u_{[i]}$, $i \in \mathcal{M}$.

Fig. 4: Positions, velocities and control inputs for all the vdOPs.

including biological rhythms, heartbeat, chemical oscillations, circadian rhythms [38].

The dynamical model of the i-th coupled vdPO ($\Sigma^C_{[i]}$) is given by

$$\begin{aligned}\dot{x}_{[i,1]} =& x_{[i,2]}\\ \dot{x}_{[i,2]} =& -(1+|\mathcal{N}_i|\bar{\beta})x_{[i,1]} + \bar{\beta}\left(\sum_{j\in\mathcal{N}_i} x_{[j,1]}\right)\\ &-\bar{\alpha}(x^2_{[i,1]}-1)x_{[i,2]} + g^A_i(x_{[i,1]})u_{[i]},\end{aligned} \tag{18}$$

where $g^A_i(x_{[i,1]}) = \frac{1}{0.4+0.1x^2_{[i,1]}}$ is the function describing the nonlinear dynamics of an actuator. Each oscillator $i \in \mathcal{M}$, is a subsystem with state $x_{[i]} = (x_{[i,1]}, x_{[i,2]})$ and input $u_{[i]}$, where $x_{[i,1]}$ is the displacements of oscillator i with respect to a given equilibrium position on the matrix, $x_{[i,2]}$ is the velocity of the oscillator i and $u_{[i]}$ is the force applied to oscillator i. For all vdPOs, we consider $\bar{\alpha} = 0.1$ and $\bar{\beta} = -0.3$. Subsystems are equipped with the state constraints $||x_{[i,1]}||_\infty \leq 3$, $||x_{[i,2]}||_\infty \leq 2$, $i \in \mathcal{M}$ and with the input constraints $||u_{[i]}||_\infty \leq 8$. We obtain models $\Sigma_{[i]}$ by discretizing continuous-time models with $T_s = 0.1$ sec sampling time, using Euler discretization. In this example, the local fault detectors do not share variables, hence $\Sigma_{[i]} = \tilde{\Sigma}_{[i]}$. Moreover the design parameter of fault detectors has been set $\lambda = 0.1$. As regards the control architecture, for each controller, we set

$$\begin{aligned}u_{[i]} = (0.4+0.1x^2_{[i,1]})\Big[&\bar{\alpha}(x^2_{[i,1]}-1)x_{[i,2]} + v_{[i]}\\ &+\bar{\kappa}_i(x_{[i]} - \bar{x}_{[i]})\Big].\end{aligned}$$

Then, we synthesize controllers $\mathcal{C}_{[i]}$, $i \in \mathcal{M}$ using Algorithm 1.

In the following simulation, we consider a matrix composed of $M = 21$ vdPOs (see Figure 3). We also consider the measurement errors bounded in the sets

$$\mathbb{O}_i = \{\varrho_{[i]} \in \mathbb{R}^2 : \ ||\varrho_{[i]}||_\infty \leq 10^{-1}\}.$$

The modelling of the LSS, the design of PnPMPC controllers and the simulations have been performed using the PnPMPC toolbox for MatLab [39]. During the simulation, the control action $u_{[i]}(t)$ computed by the controller $\mathcal{C}_{[i]}$, for all $i \in \mathcal{M}$, is kept constant during the sampling interval and applied to the continuous-time system. In Figure 4a and 4b we show a simulation where at $t = 0$, all vdPOs except $\Sigma_{[21]}$ are connected and placed in a random position around the origin. We consider that the 21-st vdPO is plugged-in at time $t = 1.5s$. For $0 \leq t < 2.5s$, due to the presence of measurements errors, the state is kept around the origin. In particular each controller $\mathcal{C}_{[i]}$ computes the control inputs shown in Figure 4c. At time $t = 1.5s$, oscillator $\Sigma_{[21]}$ is plugged-in connected as in Figure 3, hence $\mathcal{N}_{21} = 17 : 20$. Since all parents of $\Sigma_{[21]}$ have one more child, they receive state constraints from the new oscillator and retune their controllers based on the presence of the new subsystem. The 21-st oscillator is initialized with $x_{[21]}(1.5s) = (-2.5, 0)$ and then the controller steers the state around the origin. At time $\bar{t} = 2.5s$, a fault occurs in the 11-th vdPO: the actuator breaks down and saturates the control input, hence $u_{[11]}(t) = 8$, $\forall t \geq \bar{t}$, and we can also see in Fig. 4b that the velocity of the 11-th vdPO diverges. The next time instant, due to a large error between the state estimates and the measured states, the 11-th FD detects the fault, indeed $|y_{[11,2]}(\bar{t}+T_s) - \hat{\tilde{x}}_{[11,2]}(\bar{t}+T_s)| \geq \bar{\epsilon}_{[11,2]}(\bar{t}+T_s)$ (see Figure 6). At this time instant, the reconfiguration process starts: the faulty subsystem is unplugged and then the neighbouring oscillators ($\Sigma_{[j]}$, $j = \{10, 12, 19\}$) retune their controllers and their fault detectors. At time $t = \bar{t}+10T_s$, the 11-th actuator is fixed, then the vdPO can be plugged in: therefore neighbouring oscillators retune their controllers and fault detectors. The oscillator is initialized with $x_{[11]}(\bar{t}+10T_s) = (2.5, 0)$ and then the controller steers the state around the origin. In Figure 4a and 4b, we can note that for $t \geq \bar{t}+10T_s$, all states are still kept around the origin. In Figure 5, we can see that the estimators

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2016.2535724, IEEE Transactions on Automatic Control

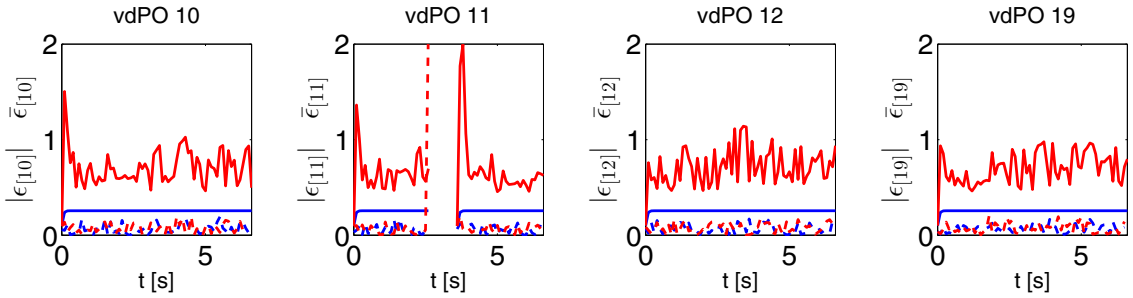


Fig. 5: Simulation of the networked vdPOs in Fig. 3. Dashed lines are the absolute values of errors $\epsilon_{[i]} = |y_{[i]} - \hat{\tilde{x}}_{[i]}|$ (where $|\cdot|$ is used component-wise) and bold lines are the thresholds $\bar{\epsilon}_{[i]}$, for $i = \{10, 11, 12, 19\}$. The same color has been used for each scalar component of the error and the corresponding scalar threshold.

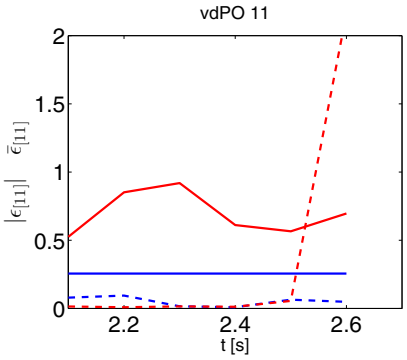


Fig. 6: Dashed lines are the absolute values of errors $\epsilon_{[11]} = |y_{[11]} - \hat{\tilde{x}}_{[11]}|$ and bold lines are the thresholds $\bar{\epsilon}_{[11]}$ during the detection of the fault in the 11-th vdPO.

of the neighboring oscillators $j = \{10, 12, 19\}$ continue to work and thresholds continue to guarantee the absence of false alarms during all the reconfiguration procedures.

B. Power Networks System

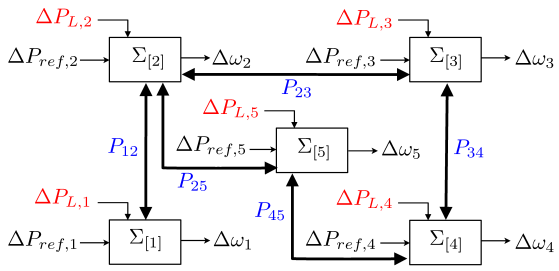


Fig. 7: Power network system of Scenario 2 in Appendix B of [31].

In this example, we apply the proposed state-feedback PnPMPC and FD scheme to the PNS proposed in Appendix B of [31]. In the following we first design the Automatic Generation Control (AGC) layer for the PNS composed of 5 areas as in Figure 7, then we show how, after a fault in area 4, we can disconnect the faulty area (unplugging operation) and redesign the controllers of neighbouring areas (reconfiguration operation). The dynamics of an area equipped with primary control and linearized around the equilibrium value for all variables can be described by the following model [40]

$$\Sigma^C_{[i]}: \quad \dot{x}_{[i]} = A_{ii}x_{[i]} + B_i u_{[i]} + L_i \Delta P_{L_i} + \sum_{j \in \mathcal{N}_i} A_{ij} x_{[j]} \ , \quad (19)$$

where $x_{[i]} = (\Delta\theta_i, \ \Delta\omega_i, \ \Delta P_{m_i}, \ \Delta P_{v_i})$ is the state, $u_{[i]} = \Delta P_{ref_i}$ is the control input of each area, ΔP_L is the local power load and $\mathcal{N}_i$ is the set of neighbouring areas, i.e. areas directly connected to $\Sigma^C_{[i]}$ through tie-lines. The matrices of system (19) are

$$A_{ii}(\{P_{ij}\}_{j\in\mathcal{N}_i}) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -\frac{\sum_{j\in\mathcal{N}_i} P_{ij}}{2H_i} & -\frac{D_i}{2H_i} & \frac{1}{2H_i} & 0 \\ 0 & 0 & -\frac{1}{T_{t_i}} & \frac{1}{T_{t_i}} \\ 0 & -\frac{1}{R_i T_{g_i}} & 0 & -\frac{1}{T_{g_i}} \end{bmatrix}$$

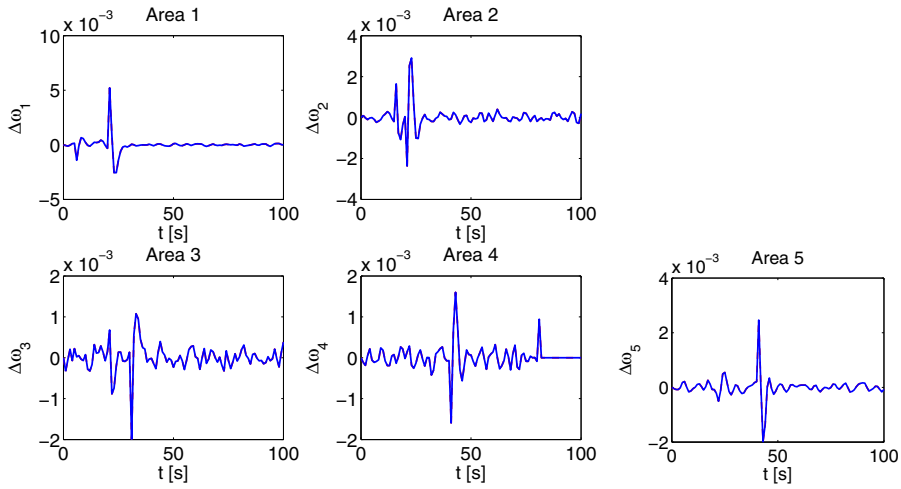
$$B_i = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \frac{1}{T_{g_i}} \end{bmatrix}, \ A_{ij} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ \frac{P_{ij}}{2H_i} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \ L_i = \begin{bmatrix} 0 \\ -\frac{1}{2H_i} \\ 0 \\ 0 \end{bmatrix}$$

For the meaning of constants as well as parameter values we refer the reader to Appendix B of [31]. We highlight that all parameter values are within the range of those used in Chapter 12 of [40]. Model (19) is input decoupled since both ΔP_{ref_i} and ΔP_{L_i} act only on subsystem $\Sigma^C_{[i]}$. Moreover, subsystems $\Sigma^C_{[i]}$ are parameter dependent since the local dynamics depends on the quantities $-\frac{\sum_{j\in\mathcal{N}_i} P_{ij}}{2H_i}$. Each subsystem $\Sigma^C_{[i]}$ is subject to constraints on $\Delta\theta_i$ and on ΔP_{ref_i} in Appendix B of [31]. We obtain models $\Sigma_{[i]}$ by discretizing models $\Sigma^C_{[i]}$ with 1 sec sampling time, using exact discretization and treating $u_{[i]}$, ΔP_{L_i}, $x_{[j]}$, $j \in \mathcal{N}_i$ as exogenous signals. As regards the FD architecture, each area is equipped with a local fault detector $\tilde{\Sigma}_{[i]}$ sharing some state variables. In particular area 1 and 2 share $\Delta\theta_1$, area 2 and 3 share $\Delta\theta_3$, area 2 and 5 share $\Delta\theta_5$ and area 3, 4 and 5 share $\Delta\theta_4$. We note that the choice of shared variables allow each FD to locally consider the effect of coupling terms and hence, from an electrical point of view, to take into account how tie-line powers are exchanged among areas. Moreover we consider the following bounded measurement errors

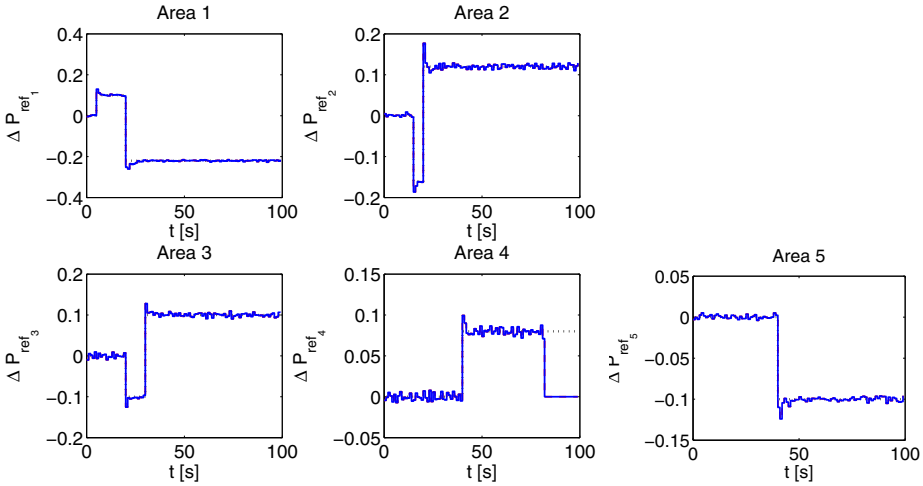
$$\mathbb{O}_i = \{\varrho_{[i]} \in \mathbb{R}^4 : \ ||\varrho_{[i]}||_\infty \leq 10^{-3}\}.$$

The modelling of the LSS, the design of PnPMPC controllers and the simulations have been performed using the PnPMPC

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2016.2535724, IEEE Transactions on Automatic Control



(a) Frequency deviation in each area controlled by PnPMPC controllers. Note that $\Delta\omega_4 = 0$ after unplugging of area 4.



(b) Load reference set-point in each area controlled by PnPMPC controllers. Note that $\Delta P_{ref_4} = 0$ after unplugging of area 4.

Fig. 8: First simulation example of a fault in area 4 at time $t = 50$ and $t = 80$: frequency deviation (panel 8a) and load reference (panel 8b) in each area.

toolbox for MatLab [39]. For each subsystem $\Sigma_{[i]}$, the controller $\mathcal{C}_{[i]}$, $i \in \mathcal{M}$ is designed by executing Algorithm 1. The aim of the AGC layer is to restore the frequency in each area next to step loads, therefore each controller must be designed in order to stabilize the local area around an equilibria that depends on ΔP_{L_i}. As regards fault diagnosis, for each local FD $\tilde{\Sigma}_{[i]}$, the filter parameter λ is set to 0.4.

In the simulation, step power loads ΔP_{L_i} specified in Table I have been used and they cause the step-like changes of the control variables in Figure 8.

In Figure 8a we show, how in presence of loads, the frequency deviation is steered in a neighbourhood of zero: however, due to the presence of measurement errors $\varrho_{[i]}$ (randomly extracted in the sets $\mathbb{O}_i$), $\Delta\omega_i$ cannot be perfectly zeroed. In Figure 8b we note how the power references ΔP_{ref_i} are changed in order to compensate for local loads.

We consider two simulation examples. In the first, at time instant $t = 50$, the following fault occurs in area 4: the inertia constant H_4 is reduced from 8 to 6. From an electrical point of view, there is a fault in a local generator, hence,

Step time	Area i	ΔP_{L_i}
5	1	+0.10
15	2	-0.16
20	1	-0.22
20	2	+0.12
20	3	-0.10
30	3	+0.10
40	4	+0.08
40	5	-0.10

TABLE I: Load of power ΔP_{L_i} (p.u.) for simulation. $+\Delta P_{L_i}$ means a step of required power, hence a decrease of the frequency deviation $\Delta\omega_i$ and therefore an increase of the power reference ΔP_{ref_i}.

for safety reasons, area 4 must be isolated in order to not propagate faults in the PNS. However, the fault is not detected by the FD $\tilde{\Sigma}_{[4]}$, as it is possible to see in Fig.9 in the initial part of the simulation. This is probably due to the fact that the magnitude of the fault is lower than the measurement and modeling uncertainties and therefore hidden by them. Moreover, we also note that, in absence of disturbances, the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2016.2535724, IEEE Transactions on Automatic Control

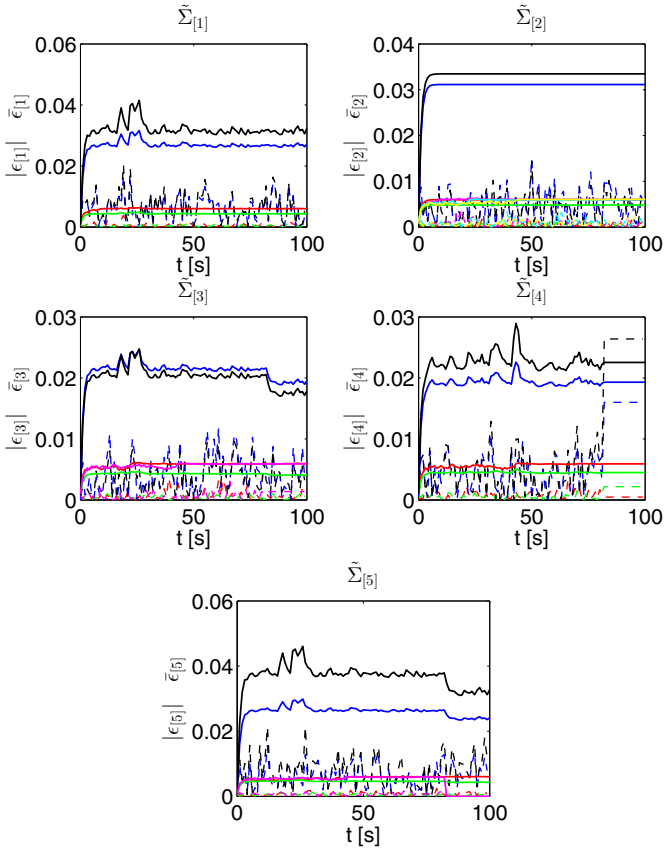


Fig. 9: First simulation example: for each area, for each color, dashed lines are the absolute values of errors $\epsilon_{[i]} = y_{[i]} - \hat{\tilde{x}}_{[i]}$ and bold lines are the corresponding thresholds $\bar{\epsilon}_{[i]}$.

PNS is at steady-state, therefore the states change around the steady-state equilibrium due to the measurement disturbances. In these conditions, then there is no guarantee to detect the fault. At time instant $t = 80$, the inertia constant H_4 is reduced from 6 to 1. In Figure 9, we note that for $t < 82$, the errors $|\epsilon_{[i]}|$ are always upper bounded by the thresholds $\bar{\epsilon}_{[i]}$, hence no faults are detected[3]. At time instant $t = 82$, FD $\tilde{\Sigma}_{[4]}$ detects the fault in area 4, indeed at time $t = 82$, $|\epsilon_{[\Delta P_{v_4}]}| > \bar{\epsilon}_{[\Delta P_{v_4}]}$. Therefore, area 4 is unplugged and controllers $\mathcal{C}_{[i]}$ and FDs $\tilde{\Sigma}_{[i]}$, $i = \{3, 5\}$ are retuned. Note that the reconfiguration operation does not involve areas 1 and 2 since they where not connected with area 4 and they did not share any state variables with it. As a consequence, the reconfiguration process is not propagated in the network. Next to the unplugging of area 4, the new PNS can still compensate power loads and FDs do not detect any fault[3].

We propose a second simulation example (see Figures 10 and 11), where at $t = 50$ we still consider that in area 4 the inertia constant H_4 is reduced from 8 to 6. However in this example we change the power load in area 4 as $\Delta P_{L_4} = 0.15$ at $t = 60$ and $\Delta P_{L_4} = -0.25$ at $t = 70$. In Figures 10 and 11 simulation results are shown. For time instants $50 \leq t \leq 59$, as in the previous example, the fault is not detected by the FD $\tilde{\Sigma}_{[4]}$. At time $t = 60$ the increase of power load in area 4 can be compensated locally even in presence of the fault and the fault is still not detected. This is due to multiple reasons: the magnitude of the fault is lower than the measurement and modeling uncertainties and the controller is robust enough to compensate the increasing of requested power even in presence of the fault. At time $t = 70$ the power load changes from $\Delta P_{L_4} = 0.15$ to $\Delta P_{L_4} = -0.25$ and the fault is detected by FD $\tilde{\Sigma}_{[4]}$. In this case even if the magnitude of the fault is not changed, the power reference ΔP_{ref_4} changes and the fault is not hidden anymore. Summarizing, this second example shows that, as highlighted in Section VI, the detectability of a fault depends on the uncertainty as well as on the trajectories and the excitability of the system.

IX. Concluding Remarks

In this paper, a novel integrated architecture composed of a distributed MPC scheme and of a distributed FD architecture has been proposed in the context of fault-tolerant control for a class of large-scale nonlinear systems. The integrated control scheme guarantees closed-loop asymptotic stability and constraints satisfaction at each time instant, while the FD architecture allows to detect faulty subsystems guaranteeing the absence of false-alarms and the convergence the estimators also during reconfiguration processes. The innovative idea is to combine distributed MPC and distributed FD architectures, where local controllers and state estimators can be designed in a PnP fashion, i.e. the overall model of the LSS is never used in any step of the design phase. The proposed architecture is suitable for several large-scale applications, allowing revamping of actuators and isolating faulty subsystems before the fault is propagate in the network.

Future research efforts will be devoted to generalizing the approach to a larger class of nonlinear systems and to address the important issue of optimal decomposition of the LSS towards better fault detectability properties (preliminary results are given in [41]).

Appendix

A. Proof of Theorem 1

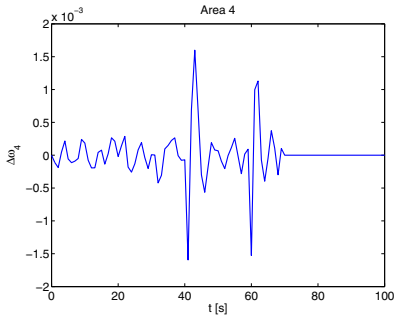
Proof: The proof of Theorem 1 is an adaptation of the proof of Theorem 9 in [19] to the nonlinear case. Due to space limitation in [19], this proof is available in [31] as the proof of Theorem 6.1. First, we can easily show that, if $x_{[i]}(0) \in \mathbb{X}_i^N$, the MPC-$i$ optimization problem defined n (8) is always feasible and its optimizers $\hat{x}_{[i]}(0|t)$ and $v_{[i]}(0|t)$ verify $\hat{x}_{[i]}(0|t) \to \mathbf{0}_{n_i}$ and $v_{[i]}(0|t) \to \mathbf{0}_{m_i}$ as $t \to \infty$.

Differently from [31], where coupling terms have been defined as linear functions, subsystems $\Sigma_{[i]}$, $i \in \mathcal{M}$ defined in this paper take into account nonlinearities in the coupling among subsystems.

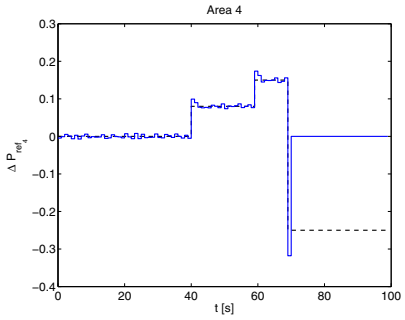
Similarly to Step 1 of the proof of Theorem 6.1 in [31], we aim at showing that if $x_{[i]}(0) \in \mathbb{X}_i^N$ there is $\tilde{T} > 0$ such that

[3]For the convenience of the reader, in Figure 9, after the reconfiguration process, errors and thresholds involving state variables of area 4 are kept constants for display purposes. After fault detection, the local estimator is stopped.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2016.2535724, IEEE Transactions on Automatic Control



(a) Frequency deviation in area 4 controlled by PnPMPC controllers. Note that $\Delta\omega_4 = 0$ after unplugging of area 4.



(b) Load reference set-point in area 4 controlled by PnPMPC controllers. Note that $\Delta P_{ref_4} = 0$ after unplugging of area 4.

Fig. 10: Second simulation of a fault in area 4 at time $t = 50$: frequency deviation (10a) and load reference (10b) in each area.

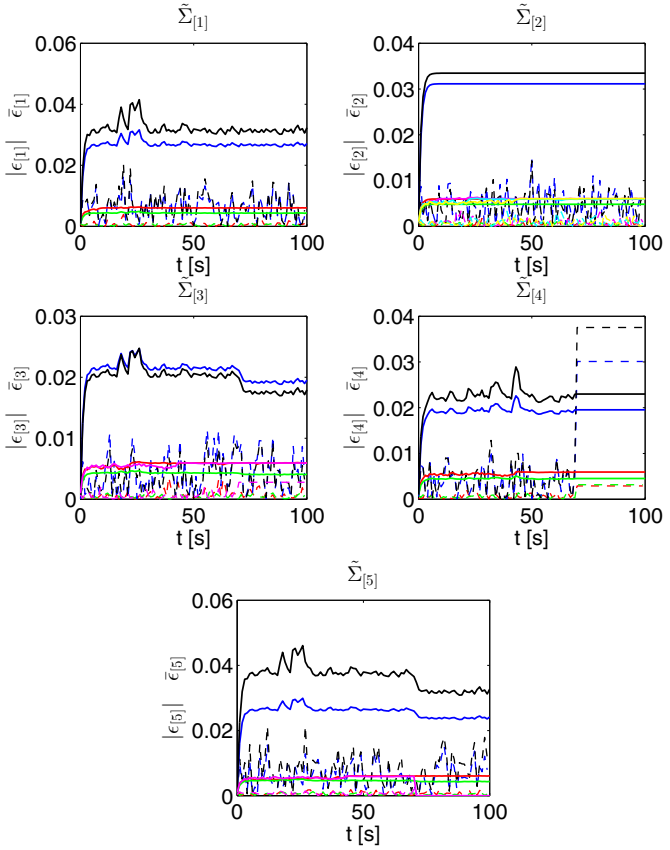


Fig. 11: Second simulation: for each area, for each color, dashed lines are the absolute values of errors $\epsilon_{[i]} = y_{[i]} - \hat{\tilde{x}}_{[i]}$ and bold lines are the corresponding thresholds $\bar{\epsilon}_{[i]}$.

$x_{[i]}(\tilde{T}) \in \mathbb{Z}_i$ and hence $\text{dist}(\mathbb{Z}_i, x_{[i]}(\tilde{T})) = 0$. From (1) and (6), we can write

$$x_{[i]}(t+1) = A_{ii}x_{[i]}(t) + B_i\bar{\kappa}_i(x_{[i]}(t)) + w_i(\psi_{[i]}(t)) + \bar{\eta}_i(t) \tag{20}$$

where

$$\bar{\eta}_i(t) = B_i(v_{[i]}(t) + \bar{\kappa}_i(z_{[i]}(t)) - \bar{\kappa}_i(x_{[i]}(t))) \tag{21}$$

and $z_{[i]}(t) = x_{[i]}(t) - \hat{x}_{[i]}(0|t)$. In particular, if $x_{[i]}(0) \in \mathbb{X}_i^N$, recursive feasibility of the MPC-i problem (8) implies that (20) holds for all $t \geq 0$.

Note that Step (III) of Algorithm 1 guarantees that Assumption 6.3 in [31] is verified and therefore, the LP problem (6.14) in [31] is feasible for all $z_{[i]} \in \mathbb{R}^{n_i}$. This implies that the function $\bar{\kappa}_i(x_{[i]}(t))$ in (20) is always well defined.
From the asymptotic convergence to zero of the nominal state $\hat{x}_{[i]}(0|t)$ and the input signal $v_{[i]}(0|t)$, it holds

$$\forall \delta_i > 0,\ \exists T_{i,1} > 0 :\ ||\hat{x}_{[i]}(0|t)|| \leq \delta_i \text{ and } ||v_{[i]}(0|t)|| \leq \delta_i, \tag{22}$$

$\forall t \geq T_{i,1}$. Moreover, according to [42], we can assume without loss of generality that $\bar{\kappa}_i(\cdot)$ is a continuous piecewise affine map. In view of this, $\bar{\kappa}_i(\cdot)$ is also globally Lipschitz, i.e.

$$\exists\ L_i > 0\ :\ ||\bar{\kappa}_i(x_{[i]} - \hat{x}_{[i]}) - \bar{\kappa}_i(x_{[i]})|| \leq L_i||\hat{x}_{[i]}|| \tag{23}$$

for all $(x_{[i]}, \hat{x}_{[i]})$ such that $x_{[i]} \in \mathbb{X}_i$ and $x_{[i]} - \hat{x}_{[i]} \in \mathbb{Z}_i$. Using (23) one can show that setting $\delta_i = \frac{\epsilon_i}{||B_i||(1+L_i)}$ the following implication holds for all $\epsilon_i > 0$:

$$||\hat{x}_{[i]}(0|t)|| \leq \delta_i \text{ and } ||v_{[i]}(0|t)|| \leq \delta_i \Rightarrow ||\bar{\eta}_i(t)|| \leq \epsilon_i,$$

$\forall x_{[i]}(t) \in \mathbb{X}_i$. Therefore, from (22),

$$\forall \epsilon_i > 0,\ \exists T_{i,1} > 0 :\ ||\bar{\eta}_i(t)|| \leq \epsilon_i,\ \forall t \geq T_{i,1}. \tag{24}$$

Since $\hat{x}_{[i]}(0|t) \to \mathbf{0}_{n_i}$, as $t \to \infty$, and $\mathbb{Z}_i$ contains $B_{\omega_i}(\mathbf{0}_{n_i})$ (see Step (III) of Algorithm 1), then

$$\forall \delta_{z_i} > 0,\ \exists T_{i,2} > 0 :\ \hat{x}_{[i]}(0|t) \in \delta_{z_i}\mathbb{Z}_i,\ \forall t \geq T_{i,2} \tag{25}$$

Hence, from (8b),

$$x_{[i]}(t) = \hat{x}_{[i]}(0|t) + (x_{[i]}(t) - \hat{x}_{[i]}(0|t)) \in (1+\delta_{z_i})\mathbb{Z}_i,\ \forall t \geq T_{i,2}. \tag{26}$$

From (20) we have, for all $i \in \mathcal{M}$,

$$x_{[i]}(t+1) = A_{ii}x_{[i]}(t) + B_i\bar{\kappa}_i(x_{[i]}(t)) + \hat{w}_{[i]}(t) \tag{27}$$

where $\hat{w}_{[i]} = w_i(\psi_{[i]}) + \bar{\eta}_{[i]}$, $\forall i \in \mathcal{M}$. Let $\mathcal{P}_i$ be the map that builds the vector $\psi_{[i]}$ from $\{x_{[j]}\}_{j\in\mathcal{N}_i}$, i.e. $\psi_{[i]} = \mathcal{P}_i(\{x_{[j]}\}_{j\in\mathcal{N}_i})$ and define $\hat{\Psi}_{[i]} = \{\mathcal{P}_i(\{x_{[j]}\}_{j\in\mathcal{N}_i}) :\ x_{[j]} \in (1+\delta_{z_i})\mathbb{Z}_j\}$. Setting $\bar{T} = \max_{i\in\mathcal{M}}\{T_{i,1}, T_{i,2}\}$ and $\delta_z = \max_{i\in\mathcal{M}}\delta_{z_i}$, using (24) and (26), remembering that $\psi_{[i]}$ is the vector of coupling variables, one has, $\forall t \geq \bar{T}$

$$\hat{w}_{[i]} \in w_i(\hat{\Psi}_i) \oplus B_{\epsilon_i}(\mathbf{0}_{n_i}). \tag{28}$$

From Steps (III)-(V) of Algorithm 1, since $\Psi_i = \{\mathcal{P}_i(\{x_{[j]}\}_{j\in\mathcal{N}_i}) : \ x_{[j]} \in \mathbb{X}_j\}$, using (7), we can deduce that $\hat{\Psi}_i \subset \dot{\Psi}_i$. Under Assumption 1-(III), we have

$$w_i(\hat{\Psi}_i) \subset \mathbb{W}_i = w_i(\Psi_i) \tag{29a}$$

Therefore, there is $\xi_i \in [0, 1)$ (that does not depend on ϵ_i) such that

$$w_i(\hat{\Psi}_i) \subseteq \xi_i \mathbb{W}_i, \tag{30}$$

and then, from (28),

$$\hat{w}_{[i]} \in (1+\delta_z)\xi_i \mathbb{W}_i \oplus B_{\epsilon_i}(\mathbf{0}_{n_i}), \ \forall t \geq \bar{T}.$$

Note that in (24) the parameter $\epsilon_i > 0$ can be chosen arbitrarily small. Assume that it verifies $\epsilon_i < (1+\delta_z)\xi_i\bar{\omega}_i, \forall i \in \mathcal{M}$ where $\bar{\omega}_i$ are the radii of the balls in Assumption 6.3 in [31]. Then, using Assumption 6.3 in [31] we get for $t \geq \bar{T}$

$$\hat{w}_{[i]}(t) \in (1+\delta_z)\xi_i(\mathbb{W}_i \oplus B_{\bar{\omega}_i}(\mathbf{0}_{n_i})) \subseteq (1+\delta_z)\xi_i \bar{\mathbb{Z}}_i^0. \tag{31}$$

In view of (26) and (31), Lemma 6.2 in [31] guarantees that

$$x_{[i]}^+ \in (1+\delta_z)(\mathbb{Z}_i \ominus (1-\xi_i)\bar{\mathbb{Z}}_i^0) \tag{32}$$

From Assumption 6.3 in [31], one has $\mathbb{Z}_i \ominus (1-\xi_i)\bar{\mathbb{Z}}_i^0 \subset \mathbb{Z}_i \ominus B_{(1-\xi_i)\omega_i}(\mathbf{0}_{n_i})$ and hence, since $\mathbb{Z}_i$ contains the origin in its interior, there is $\mu_i \in [0, 1)$ such that $\mathbb{Z}_i \ominus (1-\xi_i)\mathbb{Z}_i^0 \subset \mu_i \mathbb{Z}_i$. From (32) we get $x_{[i]}^+ \in (1+\delta_z)\mu_i \mathbb{Z}_i$. If in (25) we set δ_z such that $(1+\delta_z)\mu_i < 1$, we have shown that for $t = \bar{T}$ it holds $x_{[i]}(\bar{T}+1) \in \mathbb{Z}_i$ and Step 1 of the proof is concluded setting $\bar{T} = \bar{T} + 1$.

The proof of Theorem 1 can be concluded using Steps 2 and 3 of the proof of Theorem 6.1 in [31]. In particular in Step 2 we prove the convergence of the overall state to the origin and in Step 3 we prove stability of the closed-loop overall system. We note that Steps 2 and 3 use the fact that set $\mathbb{Z} = \prod_{i\in\mathcal{M}} \mathbb{Z}_i$ is an RCI set for the overall closed-loop system. ■

REFERENCES

[1] T. Samad and T. Parisini, "Systems of Systems," in *The Impact of Control Technology*, T. Samad and A. M. Annaswamy, Eds. IEEE Control Systems Society, pp. 175–183, 2011. [Online]. Available: ieeecss.org/general/impact-control-technology

[2] K. Baheti and H. Gill, "Cyber-physical Systems," in *The Impact of Control Technology*, T. Samad and A. M. Annaswamy, Eds. IEEE Control Systems Society, pp. 161–166, 2011. [Online]. Available: http://ieeecss.org/general/impact-control-technology

[3] J. Lunze, *Feedback control of large scale systems*. Upper Saddle River, NJ, USA: Prentice Hall, Systems and Control Engineering, 1992.

[4] P. D. Christofides, R. Scattolini, D. Muñoz de la Peña, and J. Liu, "Distributed model predictive control: A tutorial review and future research directions," *Computers and Chemical Engineering*, vol. 51, pp. 21–41, 2013.

[5] J. Liu, X. Chen, D. Muñoz de la Peña, and P. D. Christofides, "Sequential and iterative architectures for distributed model predictive control of nonlinear process systems," *AIChE Journal*, vol. 56, no. 8, pp. 2137–2149, 2010.

[6] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and Fault Tolerant Control*. Berlin, Germany: Springer, 2003.

[7] R. Isermann, *Fault-Diagnosis Systems: An Introduction from Fault Detection to Fault Tolerance*. Springer-Verlag, 2006.

[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, no. 8, pp. 1259–1274, 2004.

[9] V. Venkatasubramanian, R. Rengaswamy, S. N. Kavuri, and K. Yin, "A review of process fault detection and diagnosis: Part I: Quantitative model-based methods," *Computers and Chemical Engineering*, vol. 27, pp. 293–311, 2003.

[10] 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.

[11] W. Li, W. Gui, Y. Xie, and S. Ding, "Decentralized fault detection system design for large-scale interconnected systems," in *Proc. of the 7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, pp. 816–821, 2009.

[12] X. Zhang and Q. Zhang, "Distributed fault diagnosis in a class of interconnected nonlinear uncertain systems," *International Journal of Control*, vol. 85, no. 11, pp. 1644–1662, 2012.

[13] F. Boem, R. M. G. Ferrari, T. Parisini, and M. M. Polycarpou, "A distributed fault detection methodology for a class of large-scale uncertain input-output discrete-time nonlinear systems," in *Proc. of the 50th IEEE Conference on Decision and Control, and European Control Conference*, pp. 897–902, 2011.

[14] F. Boem, R. M. G. Ferrari, and T. Parisini, "Distributed Fault Detection and Isolation of Continuous-Time Non-Linear Systems," *European Journal of Control*, vol. 17, no. 5-6, pp. 603–620, 2011.

[15] R. M. G. Ferrari, T. Parisini, and M. M. Polycarpou, "Distributed Fault Detection and Isolation of Large-Scale Discrete-Time Nonlinear Systems: An Adaptive Approximation Approach," *IEEE Transactions on Automatic Control*, vol. 57, no. 2, pp. 275–290, 2012.

[16] C. Keliris, M. M. Polycarpou, and T. Parisini, "A Distributed Fault Detection Filtering Approach for a Class of Interconnected Continuous-Time Nonlinear Systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 8, pp. 2032–2047, 2013.

[17] V. Reppa, M. M. Polycarpou, and C. Panayiotou, "Distributed Sensor Fault Diagnosis for a Network of Interconnected Cyber-Physical Systems," *IEEE Transactions on Control of Network Systems*, vol. 2, no. 1, pp. 11–23, 2015.

[18] 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.

[19] ——, "Plug-and-Play Model Predictive Control based on robust control invariant sets," *Automatica*, vol. 50, no. 8, pp. 2179–2186, 2014.

[20] J. Stoustrup, "Plug & Play Control: Control Technology towards new Challenges," in *Proc. of the 10th European Control Conference*, pp. 1668–1683, 2009.

[21] J. Bendtsen, K. Trangbaek, and J. Stoustrup, "Plug-and-Play Control Modifying Control Systems Online," *IEEE Transactions on Control Systems Technology*, vol. 21, no. 1, pp. 79–93, 2013.

[22] S. Bodenburg, S. Niemann, and J. Lunze, "Experimental evaluation of a fault-tolerant plug-and-play controller," in *Proc. of the 13th European Control Conference*, pp. 1945–1950, 2014.

[23] S. Riverso, F. Boem, G. Ferrari-Trecate, and T. Parisini, "Fault Diagnosis and Control-reconfiguration in Large-scale Systems: a Plug-and-Play Approach," in *Proc. of the 53rd IEEE Conference on Decision and Control*, pp. 4977–4982, 2014.

[24] 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.

[25] P. Mhaskar, J. Liu, and P. D. Christofides, *Fault-tolerant process control: methods and applications*. Springer Science & Business Media, 2012.

[26] D. M. Raimondo, G. R. Marseglia, R. D. Braatz, and J. K. Scott, "Fault-tolerant model predictive control with active fault isolation," in *Proc. of 2nd International Conference on Control and Fault-Tolerant Systems*, pp. 444–449, 2013.

[27] 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.

[28] K. Tsudal, D. Mignone, G. Ferrari-Trecate, and M. Morari, "Reconfiguration Strategies for Hybrid Systems," in *Proc. of American Control Conference*, pp. 868–873, 2001.

[29] S. V. Raković, A. R. Teel, D. Q. Mayne, and A. Astolfi, "Simple Robust Control Invariant Tubes for Some Classes of Nonlinear Discrete Time Systems," in *Proc. of the 45th IEEE Conference on Decision and Control*, pp. 6397–6402, 2006.

[30] G. J. Pappas, J. Lygeros, and D. N. Godbole, "Stabilization and tracking of feedback linearizable systems under input constraints," in *Proc. of the 34th IEEE Conference on Decision and Control*, pp. 596–601, 1995.

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

2014. [Online]. Available: http://sisdin.unipv.it/pnpmpc/phpinclude/papers/phd_thesis_riverso.pdf

[32] D. M. Raimondo, S. Riverso, S. Summers, C. N. Jones, J. Lygeros, and M. Morari, "A set theoretic method for verifying feasibility of a fast explicit nonlinear Model Predictive Controller," in *Distributed Decision Making and Control*, R. Johansson and A. Rantzer, Eds. Springer, Lecture Notes in Control and Information Sciences vol. 417, ch. 13, pp. 289–311, 2012.

[33] S. V. Raković and M. Baric, "Parameterized Robust Control Invariant Sets for Linear Systems: Theoretical Advances and Computational Remarks," *IEEE Transactions on Automatic Control*, vol. 55, no. 7, pp. 1599–1614, 2010.

[34] F. Boem, R. M. G. Ferrari, T. Parisini, and M. M. Polycarpou, "Distributed Fault Detection for Uncertain Nonlinear Systems: a Network Delay Compensation Strategy," in *Proc. of American Control Conference*, pp. 3549–3554, 2013.

[35] G. Michaletzky and L. Gerencsér, "Bibo stability of linear switching systems," *IEEE transactions on automatic control*, vol. 47, no. 11, pp. 1895–1898, 2002.

[36] M. L. Sichitiu and P. H. Bauer, "Stability of Discrete Time-Varying Linear Delay Systems and Applications to Network Control," in *Stability and Control of Dynamical Systems with Applications*, D. Liu and P. J. Antsaklis, Eds. New York, NY, USA: Springer, Control Engineering, pp. 117–130, 2003.

[37] J. P. Hespanha and A. S. Morse, "Stability of Switched Systems with Avarage Dwell-Time," in *Proc. of the 38th IEEE Conference on Decision and Control*, pp. 2655–2660, 1999.

[38] M. A. Barrón and M. Sen, "Synchronization of four coupled van der Pol oscillators," *Nonlinear Dynamics*, vol. 56, no. 4, pp. 357–367, 2008.

[39] S. Riverso, A. Battocchio, and G. Ferrari-Trecate, "PnPMPC: a toolbox for MatLab," 2012. [Online]. Available: http://sisdin.unipv.it/pnpmpc/pnpmpc.php

[40] H. Saadat, *Power System Analysis*, 2nd ed. New York. NY, USA: McGraw-Hill Series in Electrical and Computer Engineering, 2002.

[41] F. Boem, R. Ferrari, T. Parisini, and M. Polycarpou, "Optimal Topology for Distributed Fault Detection of Large-scale Systems," in *Proc. of the 9th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, pp. 60–65, 2015.

[42] T. Gal, *Postoptimal Analyses, Parametric Programming and Related Topics*, 2nd ed. Berlin, Germany: de Gruyter, 1995.

PLACE PHOTO HERE

Stefano Riverso (M14) received the M.Sc. degree in computer engineering from the Dipartimento di Informatica e Sistemistica, Universita? degli Studi di Pavia, Pavia, Italy, and the Ph.D. degree in electronic, computer, and electrical engineering from the Dipartimento di Ingegneria Industriale e dellInformazione, Universita? degli Studi di Pavia, in 2010 and 2014, respectively. In 2010, he was a Visiting Student at the Institut Automatik, ETH Zurich, Zurich, Switzerland. From September 2012 to March 2013, he was a Visiting PhD Student at the University of WisconsinMadison, Madison, WI, USA. In 2014, he was a Visiting Post-Doctoral Researcher at Microgrids Group, Aalborg University, Aalborg, Denmark. Since December 2014, he is with the control group at United Technologies Research Center Ireland (UTRC-I), Cork, Republic of Ireland. His current research interests include decentralized/distributed control, state estimation and fault detection for large-scale systems, model predictive control, robust control, demand response, control of microgrids, smart-grids and HVAC systems.

PLACE PHOTO HERE

Francesca Boem received the M.Sc. degree (cum laude) in Management Engineering in 2009 and the Ph.D. degree in Information Engineering in 2013 from the University of Trieste, Italy. She was Post-Doc at the Department of Engineering and Architecture at the University of Trieste from 2013 to 2014 with the Automation Group and with the Machine Learning Group. Since 2014, she is Research Associate at the Department of Electrical and Electronic Engineering, Imperial College London, UK, with the Control and Power Research Group. She visited the Institute for Human-Machine Communication at the Technical University of Munich, Germany, in 2010, and the ACCESS Linnaeus Center, KTH Royal Institute of Technology, Sweden, in 2013. She cooperated with the R&D department of Danieli Automation SpA, Buttrio (UD), Italy. She has authored and co-authored several papers published in international journals and conference proceedings. Her current research interests include distributed fault diagnosis methods for large-scale networked systems and distributed estimation methods for sensor networks.

PLACE PHOTO HERE

Giancarlo Ferrari-Trecate (SM12) received the Ph.D. degree in Electronic and Computer Engineering from the Universita degli Studi di Pavia in 1999. Since November 2005, he has been Associate Professor at the Dipartimento di Ingegneria Industriale e dellInformazione of the same university. In spring 1998, he was a Visiting Researcher at the Neural Computing Research Group, University of Birmingham, UK. In fall 1998, he joined as a Postdoctoral Fellow the Automatic Control Laboratory, ETH, Zurich, Switzerland. He was appointed Oberassistent at ETH, in 2000. In 2002, he joined INRIA, Rocquencourt, France, as a Research Fellow. From March to October 2005, he worked at the Politecnico di Milano, Italy. His research interests include distributed and decentralised control, scalable control of microgrids, modelling and analysis of biochemical networks, hybrid systems and Bayesian learning. Prof. Ferrari-Trecate was the recipient of the assegno di ricerca Grant from the University of Pavia in 1999 and the Researcher Mobility Grant from the Italian Ministry of Education, University and Research in 2005. He is currently a member of the IFAC Technical Committee on Control Design and he is on the editorial board of Automatica and Nonlinear Analysis: Hybrid Systems.

PLACE PHOTO HERE

Thomas Parisini received the Ph.D. degree in Electronic Engineering and Computer Science in 1993 from the University of Genoa. He holds the Chair of Industrial Control at Imperial College London. Since 2001 he is also Danieli Endowed Chair of Automation Engineering with University of Trieste. He authored or co-authored more than 250 research papers in archival journals, book chapters, and international conference proceedings. His research interests include neural-network approximations for optimal control problems, fault diagnosis for nonlinear and distributed systems, nonlinear model predictive control systems and nonlinear estimation. He is a co-recipient of the 2011-2013 IFAC Best Application Paper Prize of the Journal of Process Control, Elsevier, and of the 2004 Outstanding Paper Award of the IEEE Trans. on Neural Networks. He is also a recipient of the 2007 IEEE Distinguished Member Award. In 2012 he was awarded a prestigious ABB Research Grant dealing with energy-autonomous sensor networks for self-monitoring industrial environments. Thomas Parisini is the Editor-in-Chief of the IEEE Trans. on Control Systems Technology. He is also the Chair of the IFAC Techn. Comm. on Fault Detection, Supervision & Safety of Technical Processes. He was the Chair of the IEEE CSS Conference Editorial Board and a Distinguished Lecturer of the IEEE. He is currently serving as an Associate Editor of the Int. J. of Control and served as Associate Editor of the IEEE Trans. on Automatic Control, of the IEEE Trans. on Neural Networks, of Automatica, and of the Int. J. of Robust and Nonlinear Control. Among other activities, he was the Program Chair of the 2008 IEEE CDC and a General Co-Chair of the 2013 IEEE CDC.