A Plug-and-Play Fault Diagnosis Approach for Large-Scale Systems ⋆

Francesca Boem * **Stefano Riverso** **
Giancarlo Ferrari-Trecate *** **Thomas Parisini** ****

* *Dept. of Electrical and Electronic Engineering, Imperial College London, UK,* (f.boem@imperial.ac.uk)
** *United Technologies Research Center Ireland, Penrose Business Center, Penrose Wharf, Cork, Ireland* (riverss@utrc.utc.com)
*** *Dip. di Ingegneria Industriale e dell'Informazione, Università degli Studi di Pavia, Italy* (giancarlo.ferrari@unipv.it)
**** *Dept. of Electrical and Electronic Engineering, Imperial College London, UK, and University of Trieste, Italy* (t.parisini@gmail.com)

Abstract: This paper proposes a novel Plug-and-Play (PnP) dynamic approach for the monitoring of Large-Scale Systems (LSSs). The proposed architecture exploits a distributed Fault Detection and Isolation (FDI) methodology for nonlinear LSS in a PnP framework. The LSS consists of several interconnected subsystems and the designed FDI architecture is able to manage plugging-in of novel subsystems and un-plugging of existing ones. Moreover, the proposed PnP approach performs the unplugging of faulty subsystems in order to avoid the propagation of faults in the interconnected LSS. Analogously, once the issue has been solved, the disconnected subsystem can be re-plugged-in. The reconfiguration processes only involves local operations of neighboring subsystems, thus allowing a distributed architecture.

Keywords: Plug-and-Play, Fault Detection, Fault Isolation, Large-Scale Systems, Networked Systems, Distributed, Monitoring

1. INTRODUCTION

Complex systems such as LSS (Lunze (1992)), Systems-of-Systems (Samad and Parisini (2011)) and Cyber-Physical Systems (Baheti and Gill (2011)) attract a significant and steadily growing interest in academia and industry. These systems are characterized by a large number of states and inputs, are spatially distributed, and are modeled as the interaction of many subsystems coupled through physical or communication relationships. Furthermore, they often can have a dynamic structure that changes along the time. The increased scale and complexity of the considered systems implies a consequent increase in risk: in a networked framework, also small failures can have severe consequences for the entire system, involving individuals, operators, system owners, societies and the environment. Therefore, reliability is a key requirement in systems design and the development of distributed methods for fault diagnosis is an emergent important topic.

When dealing with monitoring of LSSs, centralized architectures (see Blanke et al. (2003) for a survey) can be not adequate due to computational, communication, scalability and reliability limits. An alternative is offered by the adoption of decentralized and distributed approaches (see Li et al. (2009), Zhang and Zhang (2012), Boem et al. (2011), Ferrari et al. (2012) as examples). Moreover, a novel requirement is the design of monitoring architectures able to be robust to the changes that may happen in the dynamic structure of the LSS. This is why, in this paper we develop a distributed Fault Detection and Isolation methodology, properly designed for a Plug-and-Play framework. It is worth noting that the proposed technique is not a data-driven method (see Yin et al. (2014) for a recent survey), but a model-based one (Frank (1996)). To the authors' knowledge, this is the first time that a complete distributed monitoring architecture is designed for LSS in a PnP scenario. Some recent results are presented in Riverso et al. (2014a), integrating distributed model-based fault detection with Model Predictive Control (MPC). Compared with Riverso et al. (2014a), the present paper shows the following significant differences: i) a general class of nonlinear systems is addressed, while in Riverso et al. (2014a) the analysis was limited to a class of nonlinear systems, with matched control input; ii) the fault isolation problem is also considered; iii) we exploit a full PnP framework, where the monitoring architecture is always robust to plug-in and unplugging of subsystems. Instead, in Riverso et al. (2014a) only a reconfiguration process after fault occurrence is considered. Recently, some works have been published dealing with PnP scenarios: Stoustrup (2009); Bendtsen et al. (2013); Riverso et al. (2013) analyze only the control problem; Izadi-Zamanabadi et al. (2012) designs a fault-tolerant control strategy for a centralized system; finally, Bodenburg et al. (2014) presents a fault-tolerant PnP controller, but, differently from the proposed work, it considers linear systems with a centralized approach. The paper is organized as follows. In Section 2, the problem formulation is provided whereas, in Section 3, the PnP distributed FDI scheme is presented. The PnP operations are described in Section 4. Some simulation results on a power systems application are presented in Section 5. Finally, some concluding remarks are given in Section 6.

⋆ The research leading to these results has received partial funding from the European Union Seventh Framework Programme [FP7/2007-2013] under grant agreement n° 257462 HYCON2 Network of excellence and from the EPSRC STABLE-NET grant EP/L014343/1.

Notation. We use $a : b$ for the set of integers $\{a, a+1, \dots, b\}$. Let v, $\bar{v} \in \mathbb{R}^s$, the inequality $|v| \leq \bar{v}$ means that for each component v_k of the vector v, $k = 1 : s$, we have $|v_k| \leq \bar{v}_k$.

2. PROBLEM FORMULATION

Let us consider a LSS, composed, at time t, of M interconnected subsystems. Subsystem dynamics is

$$\Sigma_{[i]} : x^+_{[i]} = f_i(x_{[i]}, \psi_{[i]}, u_{[i]}) + w_i(x_{[i]}, \psi_{[i]}) + \phi_i(x_{[i]}, \psi_{[i]}, u_{[i]}, t) \quad (1)$$

where $x_{[i]} \in \mathbb{R}^{n_i}$, $u_{[i]} \in \mathbb{R}^{m_i}$, $i \in \mathcal{M} = 1 : M$, are the local state and input, respectively, at time t and $x^+_{[i]}$ stands for $x_{[i]}$ at time $t+1$. The vector of interconnection variables $\psi_{[i]} \in \mathbb{R}^{p_i}$ collects components of 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 $\mathcal{N}_i = \{j \in \mathcal{M} : \frac{\partial x^+_{[i]}}{\partial x_{[j]}} \neq 0, i \neq j\}$. We also define $\mathcal{C}_i = \{k : i \in \mathcal{N}_k\}$ as the set of children of $\Sigma_{[i]}$. Finally, we say that $\Sigma_{[i]}$ and $\Sigma_{[j]}$ are neighbors if $j \in \mathcal{N}_i$ or $j \in \mathcal{C}_i$. $f_i(\cdot) : \mathbb{R}^{n_i} \times \mathbb{R}^{p_i} \times \mathbb{R}^{m_i} \to \mathbb{R}^{n_i}$ represents possibly nonlinear nominal dynamics, including also known relationships with parent subsystems by means of the interconnection variables, while $w_i(\cdot) : \mathbb{R}^{n_i} \times \mathbb{R}^{p_i} \to \mathbb{R}^{n_i}$ represents the unknown possibly nonlinear coupling among subsystems and includes also modeling uncertainties. Instead, the function $\phi_i(\cdot) : \mathbb{R}^{n_i} \times \mathbb{R}^{p_i} \times \mathbb{R}^{m_i} \times \mathbb{R} \to \mathbb{R}^{n_i}$ represents the fault-function, capturing deviations of the dynamics of Σ_i from the nominal healthy dynamics: it is null before the unknown fault time T_0. We assume that the nominal model (1) takes already into account the influences due to all the possible subsystems that can be plugged-in to the i-th subsystem, by means of the interconnection variables $\psi_{[i]}$: at a certain time t, some of these variables could be null (or set to a defined value) because the corresponding father subsystem is not connected to $\Sigma_{[i]}$ at that time. The k-th component of vector $x_{[i]}$ is specified by $x_{[i,k]}$. In this paper, we assume that the state vector is fully accessible through noisy measurements $y_{[i]}$:

$$y_{[i]} = x_{[i]} + \varrho_{[i]}, \quad (2)$$

where $\varrho_{[i]} \in \mathbb{R}^{n_i}$, $i \in \mathcal{M}$, is the local unknown measurement error at time t. Similarly, $z_{[i]} = \psi_{[i]} + \theta_{[i]}$ is the vector of measured interconnection variables communicated by father subsystems, with $\theta_{[i]}$ collecting the involved measurement error $\varrho_{[j]}$, $j \in \mathcal{N}_i$. We consider the following

Assumption 1. (I) Subsystems $\Sigma_{[i]}$, $i \in \mathcal{M}$ are subject to the constraints

$$x_{[i]} \in \mathbb{X}_i, \; u_{[i]} \in \mathbb{U}_i, \; \psi_{[i]} \in \Psi_i \,, \quad (3)$$

where $\mathbb{X}_i$, $\mathbb{U}_i$ and Ψ_i are compact sets.

(II) Functions $w_i(\cdot)$ are bounded for all $i \in \mathcal{M}$, i.e. it is possible to define $\forall i$, k at each time step a bound $\bar{w}_{i,k}$, so that $\left|w_{i,k}(x_{[i]}, \psi_{[i]})\right| \leq \bar{w}_{i,k}(y_{[i]}, z_{[i]})$.

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

Some state variables, which we call *shared* variables, are monitored by more than one LFD (see Fig.1). The decomposition of the LSS is then termed *overlapping* (Lunze (1992)). Examples of applications that can be represented in this way are: power networks, water/gas distribution networks and all the facilities networks that are divided into subnetworks.

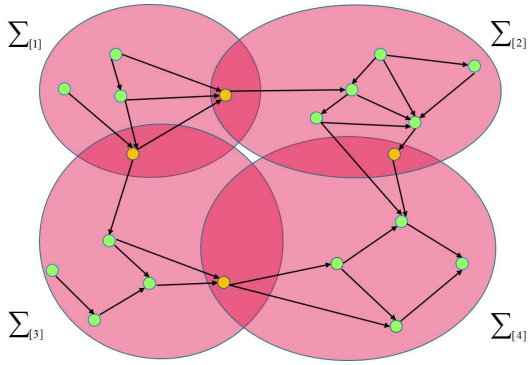

Fig. 1. The possibly overlapping decomposition of the LSS structural graph: the small green circles represent the state and input variables; the yellow ones are the shared state variables.

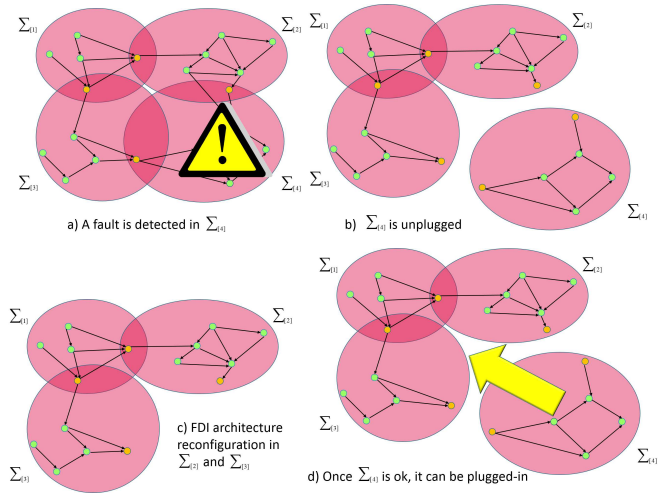

Fig. 2. The reconfiguration option after fault detection.

The PnP framework we are considering, allows the plug-in and unplugging of subsystems, without any need to reconfigure the entire LSS: only neighboring subsystems have to be updated, continuing to guarantee convergence properties of the estimators and operational capabilities of the diagnosers. We assume that only healthy subsystems are connected to the LSS within the plug-in operations. On the other hand, the unplugging process may occur also in faulty conditions. In fact, one of the advantages of the proposed framework is that, after fault detection, the faulty subsystem can be disconnected, in order to avoid the propagation of the fault in the LSS system. More specifically, plug-in and unplugging operations, that we generally call *reconfiguration* operations, could happen due to changes of the dynamic structure of the LSS system or it could be the consequence of the detection of a fault. In this second case, the unplugging could be acted as a consequence of the isolation phase or in alternative to the isolation step. In general, after the detection of a fault (see Section 3.1), depending on the specific application context and criticality, two distinct actions may be feasible: i) immediate "disconnection" of the faulty subsystem after detection (see Fig. 2) or ii) continuation of the system operation in "safety mode" and simultaneously fault isolation, as explained in Section 3.6. After fault isolation, two alternatives are possible: the unplugging of the faulty subsystem or fault accommodation. We do not consider fault accommodation in this paper. All these alternatives are explained in the qualitative flowchart in Fig. 3.

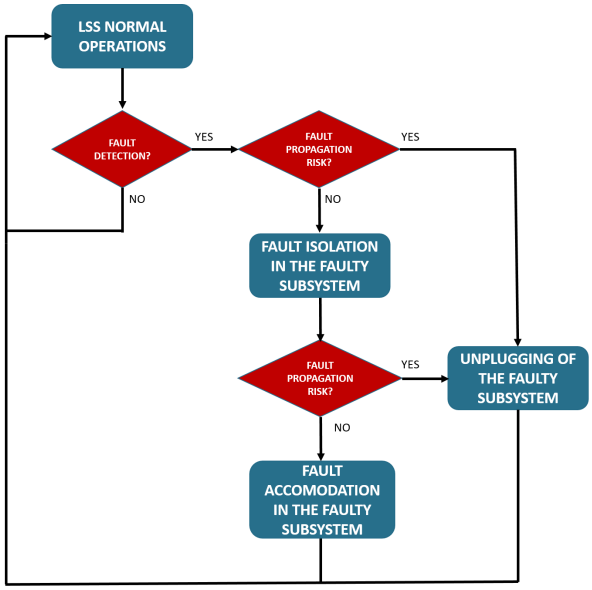

Fig. 3. The proposed FDI architecture in the PnP framework. The LSS normal operations include the plug-in of novel subsystems and unplugging of existent ones.

3. THE FDI ARCHITECTURE

In this section, we design a distributed FDI architecture for the considered PnP framework. Each subsystem is monitored by one Local Fault Diagnoser (LFD).

3.1 Distributed Fault Detection

Let us first consider the fault detection task. We specialize to the PnP framework considered in this paper a typical model-based FD approach: an estimate $\hat{x}_{[i]}$ of the local state variables is defined; the estimation error $\epsilon_{[i]} \triangleq y_{[i]} - \hat{x}_{[i]}$ is compared component-wise with a suitable time-varying detection threshold $\bar{\epsilon}_{[i]} \in \mathbb{R}^{n_i}_{+}$. The condition $|\epsilon_{[i,k]}| \leq \bar{\epsilon}_{[i,k]}, \forall k = 1 : n_i$ is a necessary (but generally not sufficient) condition for the hypothesis $\mathcal{H}_i$: "Subsystem $\Sigma_{[i]}$ is healthy". If the condition is violated at some time instant, then we can conclude that a fault has occurred. 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 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. Furthermore, properties are guaranteed during all the plug-in and unplugging processes in healthy conditions.

3.2 The Fault Detection Estimator

For detection purposes, each LFD implements a local nonlinear estimator, based on the local model (1). The k_i-th non-shared state variable of $\Sigma_{[i]}$ can be estimated as

$$\hat{x}^{+}_{[i,k_i]} = \lambda(\hat{x}_{[i,k_i]} - y_{[i,k_i]}) + f_{i,k_i}(y_{[i]}, z_{[i]}, u_{[i]}), \quad (4)$$

where the filter parameter is chosen in the interval $0 < \lambda < 1$, in order to guarantee convergence properties. Let now consider a shared variable $x_{[i,k_i]} = x_{[j,k_j]}$, where k_i and k_j are the k_i-th and k_j-th components of local vectors $x_{[i]}$ and $x_{[j]}$, respectively. We use the redundant measurements due to overlapping for implementing a deterministic consensus approach (see Ferrari et al. (2012)). In fact, as regards shared variables estimation, each subsystem communicates with parents and children subsystems sharing that variable. In the following, $\mathbb{S}^k$ is the time-varying set of subsystems $\Sigma_{[i]}$ sharing a given state variable k of the LSS at the current time step. Let the shared variable be $x_{[i,k_i]}$. The estimates of shared variables are provided by

$$\hat{x}^{+}_{[i,k_i]} = \lambda(\hat{x}_{[i,k_i]} - y_{[i,k_i]}) + \sum_{j \in \mathbb{S}^k} W^k_{i,j} \left[\lambda(\hat{x}_{[j,k_j]} - \hat{x}_{[i,k_i]}) + f_{j,k_j}(y_{[j]}, z_{[j]}, u_{[j]})\right], \quad (5)$$

where $W^k_{i,j}$ are the components of a row-stochastic matrix W^k, which will be defined in Subsection 3.4, designed to allow plugging-in and unplugging operations. By now, notice that W^k collects the consensus weights used by $\Sigma_{[i]}$ to weight the terms communicated by $\Sigma_{[j]}$, with $j \in \mathbb{S}^k$. We note that (5) holds also for the case of non-shared variables (4), 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 omit the subscript of the shared component index k, i.e. we use $x_{[i,k]}$ instead of $x_{[i,k_i]}$ when not strictly necessary.

3.3 The detection threshold

In order to properly define a threshold for FD, we analyze the dynamics of the local estimation error in healthy conditions. Defining W^k such that $\sum_{j \in \mathbb{S}^k} W^k_{i,j} = 1$ and since for shared variables $\forall i, j \in \mathbb{S}^k$ there are k_i and k_j such that it holds $f_{i,k_i}(x_{[i]}, \psi_{[i]}, u_{[i]}) = f_{j,k_j}(x_{[j]}, \psi_{[j]}, u_{[j]})$, the k-th state estimation error dynamics model is given by

$$\epsilon^{+}_{[i,k]} = \sum_{j \in \mathbb{S}^k} W^k_{i,j} \left[\lambda\epsilon_{[j,k]} + \Delta f_{j,k} + w_{j,k}(x_{[j]}, \psi_{[j]}) - \lambda\varrho_{[j,k]}\right] + \lambda\varrho_{[i,k]} + \varrho^{+}_{[i,k]},$$

where $\Delta f_{j,k} \triangleq f_{j,k}(x_{[j]}, \psi_{[j]}, u_{[j]}) - f_{j,k}(y_{[j]}, z_{[j]}, u_{[j]})$ and $\varrho^{+}_{[i,k]}$ is the measurement error at time $t+1$. As in Ferrari et al. (2012), we can bound the estimation error, guaranteeing no false-positive alarms:

$$|\epsilon^{+}_{[i,k]}| \leq \sum_{j \in \mathbb{S}^k} W^k_{i,j} \left[\lambda|\epsilon_{[j,k]}| + |\Delta f_{j,k}| + \lambda|\varrho_{[j,k]}| + |w_{j,k}(x_{[j]}, \psi_{[j]})|\right] + \lambda|\varrho_{[i,k]}| + |\varrho^{+}_{[i,k]}|.$$

We define the following time-varying threshold $\bar{\epsilon}_{[i,k]}$ that *can be computed in a distributed way* by each LFD as

$$\bar{\epsilon}^{+}_{[i,k]} = \sum_{j \in \mathbb{S}^k} W^k_{i,j} \left[\lambda\bar{\epsilon}_{[j,k]} + \Delta\bar{f}_{j,k} + \lambda\bar{\varrho}_{[j,k]} + \bar{w}_{j,k}(y_{[j]}, z_{[j]})\right] + \lambda\bar{\varrho}_{[i,k]} + \bar{\varrho}^{+}_{[i,k]}, \quad (6)$$

where $\Delta\bar{f}_j = \max_{x_{[j]} \in \mathbb{X}_j, \psi_{[j]} \in \Psi_j} |\Delta f_j|$. Assumption 1 implies that state and input variables are bounded; hence all quantities in (6) are bounded as well; $\bar{\varrho}_{[i,k]}$ and $\bar{w}_{i,k}$ are defined in Assumption 1. The threshold dynamics (6) can be initialized with $\bar{\epsilon}_{[i,k]}(0) = \bar{\varrho}_{[i,k]}(0)$. Threshold (6) guarantees the absence of false-alarms caused by the uncertainties. On the other hand, this is a possibly conservative result since, in rough and qualitative terms, it does not allow to detect faults "whose magnitude is lower than the uncertainties magnitude" in the system dynamics [1].

[1] In Riverso et al. (2014b) some detectability results are given.

Remark 2. For diagnosis purposes, the information exchange between the local diagnosers is limited. It is not necessary that each diagnoser knows the model of neighbouring subsystems. In the shared case (5), it is sufficient that each subsystem $\Sigma_{[i]}$ communicates to neighbouring subsystems only the interconnection variables and the local consensus terms for estimates and thresholds.

3.4 The consensus matrix

In this subsection, we explain how to design the consensus matrix in an appropriate way in order to allow PnP operations. For PnP capabilities, we use a square time-varying weighting matrix W^k whose dimension is equal to the maximum number (as large as wanted) of subsystems that can be plugged in sharing that variable. Each row and each column represent a LFD sharing the variable k: the generic element $W^k_{i,j}$ indicates how much the i-th diagnoser weights the consensus terms received by the j-th diagnoser in $\mathbb{S}^k$. Each row can have non null elements only in 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 3.5). Similarly as in Boem et al. (2013) (where it was useful for a delay compensation strategy), here we define the time-varying consensus-weighting matrix W^k:

$$W^k_{i,j} = \begin{cases} 1 & \text{if } j = \arg\min_{j\in\mathbb{S}^k} \lambda(\bar{\epsilon}_{[j,k]} + \bar{\varrho}_{[j,k]}) + \Delta\bar{f}_{j,k} \\ & \quad +\bar{w}_{j,k}(y_{[j]}, z_{[j]}) \\ 0 & \text{otherwise} \end{cases} \tag{7}$$

At each time-step, every LFD receives estimates and consensus terms of variable $x_{[i,k]}$ only from the subsystems sharing it at that specific time. Then, it selects the contribution affected by "smaller uncertainty" in its measurements and in the local model. The introduction of the proposed time-varying consensus matrix allows PnP operations and is advantageous from a second perspective: it allows to obtain the smallest threshold in the set of all the possible conservative thresholds designed in (6).

3.5 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 for analysis purposes a vector formulation of the state error equation. Specifically, the extended estimation error vector $\epsilon_{k,E}$ is a column vector collecting the estimation error vectors of the N_k subsystems sharing the k-th state component: $\epsilon_{k,E} \triangleq \operatorname{col}\left(\epsilon_{[j,k]} : j \in \mathbb{S}^k\right)$. Hence, the dynamics of $\epsilon_{k,E}$ can be described as:

$$\epsilon^+_{k,E} = W^k\left[\lambda\epsilon_{k,E} + \Delta f_{k,E} + w_{k,E} - \lambda\varrho_{k,E}\right] + \lambda\varrho_{k,E} + \varrho^+_{k,E}, \tag{8}$$

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 $j \in \mathbb{S}^k$; $\Delta f_{k,E}$ and $w_{k,E}$ are column vectors collecting the vectors $w_{j,k}$ and $\Delta f_{j,k}$, with $j \in \mathbb{S}^k$, respectively. The following convergence result can now be provided. Due to length constraints, the proof is omitted.

Proposition 3. System (8), where the consensus matrix is given by (7), is BIBO stable.

3.6 Distributed Fault Isolation

For fault isolation, we implement a Generalized Observer Scheme (GOS, see Patton et al. (1989)), following the approach proposed in Ferrari et al. (2012) for distributed systems. We adapt it for the PnP scenario we are considering. We assume that each subsystem knows a *local fault set* $\mathcal{F}_i$, collecting all the $N_{\mathcal{F}_i}$ possible nonlinear fault functions: $\phi^l_i(x_{[i]}, \psi_{[i]}, u_{[i]}, t)$, $l \in \{1, \ldots, N_{\mathcal{F}_i}\}$. After fault detection at time T_d, each interested LFD uses $N_{\mathcal{F}_i}$ nonlinear estimators of the local state $x_{[i]}$, called Fault Isolation Estimators (FIEs), in order to locally determine which of the possible $N_{\mathcal{F}_i}$ faults in the set $\mathcal{F}_i$ has occurred. After the generic l–th FIE estimator is activated, with $l \in \{1, \ldots, N_{\mathcal{F}_i}\}$, it monitors its i-th subsystem, providing a *local state estimate* $\hat{x}^l_{[i]}$ of the local state $x_{[i]}$. The difference between the estimate $\hat{x}^l_{[i]}$ and the measurements $y_{[i]}$ is the *estimation error* $\epsilon^l_{[i]} \triangleq y_{[i]} - \hat{x}^l_{[i]}$ which is used as a residual and compared, component by component, to a suitable *isolation threshold* $\bar{\epsilon}^l_{[i]} \in \mathbb{R}^{n_i}_+$. The condition $|\epsilon^l_{[i,k]}| \le \bar{\epsilon}^l_{[i,k]}\ \forall\, k = 1, \ldots, n_i$ is associated to the l–th fault hypothesis $\mathscr{H}_{i,l}$:"The subsystem $\Sigma_{[i]}$ is affected by the l-th fault", with $l = 1, \ldots, N_{\mathcal{F}_i}$. As soon as the hypothesis $\mathscr{H}_{i,l}$ is falsified, the fault ϕ^l_i is excluded as a possible cause of the fault. The goal of the isolation task is to exclude every but one fault, which is said to be *isolated*.

3.7 The Fault Isolation Estimators

After the fault ϕ_i has occurred, the dynamics of the k–th state component of the i–th subsystem becomes

$$x^+_{[i,k]} = f_{i,k}(x_{[i]}, \psi_{[i]}, u_{[i]}) + w_{i,k}(x_{[i]}, \psi_{[i]}) + \phi_{i,k}(x_{[i]}, \psi_{[i]}, u_{[i]}, t),$$

being $\phi_{i,k} \neq 0$. The l–th FIE estimate for the general case of a fault on a shared variable, can be computed as

$$\hat{x}^{+l}_{[i,k]} = \lambda(\hat{x}^l_{[i,k]} - y_{[i,k]}) + \sum_{j\in\mathbb{S}^k} W^k_{i,j}\left[\lambda(\hat{x}^l_{[j,k]} - \hat{x}^l_{[i,k]}) + f_{j,k}(y_{[j]}, z_{[j]}, u_{[j]}) + \phi^l_{j,k}(y_{[j]}, z_{[j]}, u_{[j]}, t)\right]. \tag{9}$$

The corresponding estimation error dynamic equation is

$$\epsilon^{+l}_{[i,k]} = \sum_{j\in\mathbb{S}^k} W^k_{i,j}\left[\lambda\epsilon^l_{[j,k]} + \Delta f_{j,k} + w_{j,k}(x_{[j]}, \psi_{[j]}) + \Delta\phi^l_{j,k} - \lambda\varrho_{[j,k]}\right] + \lambda\varrho_{[i,k]} + \varrho^+_{[i,k]},$$

with

$$\Delta\phi^l_{j,k} = \phi_{i,k}(x_{[i]}, \psi_{[i]}, u_{[i]}, t) - \phi^l_{j,k}(y_{[j]}, z_{[j]}, u_{[j]}, t).$$

Now, considering a matched fault (that is, $\phi_{i,k} = \phi^l_{i,k}(x_{[i]}, \psi_{[i]}, u_{[i]}, t)$, $\forall\, i \in \mathbb{S}^k$), the error equation absolute value can be bounded by a threshold:

$$\bar{\epsilon}^{+l}_{[i,k]} = \sum_{j\in\mathbb{S}^k} W^k_{i,j}\left[\lambda\bar{\epsilon}^l_{[j,k]} + \bar{w}_{j,k}(z_{[j]}) + \Delta\bar{f}_{j,k} + \Delta\bar{\phi}_{j,k} + \lambda\bar{\varrho}_{[j,k]}\right] + \lambda\bar{\varrho}_{[i,k]} + \bar{\varrho}^+_{[i,k]} \tag{10}$$

where $\Delta\bar{\phi}_j = \max_{x_{[j]}\in\mathbb{X}_j, \psi_{[j]}\in\Psi_j} |\Delta\phi_j|$. This threshold guarantees by definition that no matched fault will be excluded because of uncertainties [2]. The time-varying consensus matrix designed in Section 3.4 is useful also for fault

[2] Isolability conditions can be derived (Ferrari et al. (2012)).

isolation in order to allow PnP operations. The derived distributed fault isolation methodology is robust to the PnP considered scenario.

4. RECONFIGURATION STRATEGY

In the previous sections, we derived suitable fault detection and isolation architectures for a PnP framework. We now explain how to use them during PnP operations. As already explained, system reconfiguration could happen due to changes over time of the dynamic structure of the LSS system or it could be the consequence of the decision of the monitoring architecture after fault detection (see Fig. 2). In both cases (healthy and faulty conditions), subsystems plug-in and unplugging are designed as follows.

4.1 Subsystem unplugging

In this paragraph, we show how to reconfigure LFDs in the LSS when a subsystem $\Sigma_{[j]}$ is disconnected from the LSS, guaranteeing estimators convergence and monitoring of the new network with one less subsystem. The following operations are needed:

- In the children subsystems $i \in \mathcal{C}_j$, the components of the interconnection variables $\tilde{\psi}_{[i]}$ and $z_{[i]}$ related to parent subsystem $\Sigma_{[j]}$ are not received anymore and so become equal to 0 or set to defined values. This is needed for computation of detection (5) and isolation (9) estimates and related thresholds (6)-(10) .
- If the unplugged subsystem was sharing variable k, its consensus contribution will not be received by neighboring subsystems i, with $i \in \mathcal{C}_j$ or $i \in \mathcal{N}_j$, sharing some variables with $\tilde{\Sigma}_{[j]}$; then the weights associated with $\tilde{\Sigma}_{[j]}$ in the consensus matrices W^k computed in (7) are set to zero.

4.2 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 or if a novel subsystem has to be added to the LSS. For what concerns the distributed FDI architecture, thanks to the way the time-varying shared variables estimators are defined in (5) and (9), the plug-in is always feasible. More specifically, if a subsystem $\Sigma_{[j]}$ is added to the LSS:

- In the children subsystems $i \in \mathcal{C}_j$, the components of $\tilde{\psi}_{[i]}$ and $z_{[i]}$ related to subsystem $\Sigma_{[j]}$ are received and used for computation of detection (5) and isolation (9) estimates and related thresholds (6)-(10) .
- In the neighboring subsystems i, with $i \in \mathcal{C}_j$ or $i \in \mathcal{N}_j$, sharing some variables k with $\tilde{\Sigma}_{[j]}$, the consensus matrices W^k are computed as in (7) considering also the components received from $\Sigma_{[j]}$.

5. A POWER NETWORKS APPLICATION

In this section, we show features brought about by the proposed PnP architecture using models of Power Network Systems (PNS) described in Riverso et al. (2014a), that are composed by five generation areas connected through tie–lines (see Fig. 4). In Riverso et al. (2014b), we shown how to reconfigure controllers and LFDs when a fault is detected in a generation area and the faulty area is unplugged. In the following we propose a fault isolation scheme. Indeed, when a fault occurs in a generation area, we should not unplug the faulty area, until it can still contribute to the frequency regulation. Therefore, electrical or mechanical faults, that reduce capabilities of a generation area, must be detected and then isolated. In the following, for the PNS in Fig. 4, we use the same parameters as in Section 7.2 in Riverso et al. (2014b). Due to faults, we consider that a generation area may lose local generators: this corresponds to reducing the inertia parameter for that area. In particular, we consider that the inertia can decrease of 30%, 60% and 90% from the nominal value. This defines local fault sets for each area.

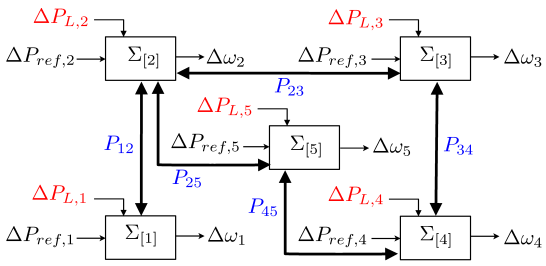

Fig. 4. Power network system.

At time $t = 60$s, a fault occurs in area 4 and the inertia parameter is reduced of 90%. Therefore, the area can still contribute to the frequency regulation. In Fig. 5 we show that the fault is detected a time $t = 68$s when $\epsilon_{[4]}(68) > \bar{\epsilon}_{[4]}(68)$. At this time, we run three different state estimators by varying the inertia parameter. Since only the state estimator designed using 90% of the nominal inertia guarantees $\epsilon_{[4]}(68) < \bar{\epsilon}_{[4]}(68)$, we are able to isolate the fault. Therefore we do not need to unplug the faulty area, but we reconfigure the local controller and the local fault detector. Moreover, in Fig. 5 at time $t = 68$s, the state estimations and the thresholds are changed in accordance with the new state estimator.

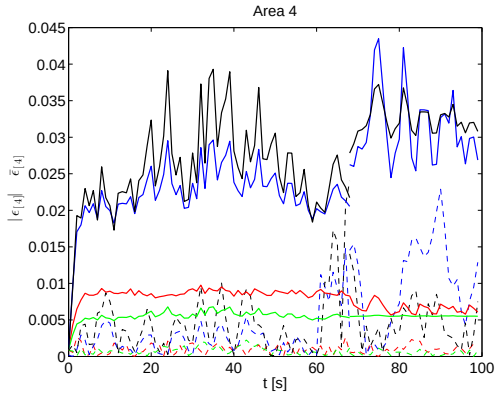

Fig. 5. Simulation for area 4 with isolation and reconfiguration: dashed lines are the absolute values of errors $\epsilon_{[4]}$ and bold lines are the thresholds $\bar{\epsilon}_{[4]}$.

In Fig. 6 and 7 we show problems that can occur without a suitable reconfiguration. In the simulation, in Fig. 6, we assume that at time $t = 68$s neither the isolation procedure is executed nor the faulty area is unplugged (indeed we can notice that for $t > 68$s the fault is still detected). Moreover, in Fig. 7 we also note that without a suitable reconfiguration of the local controller, the stability of the closed-loop system can not be guaranteed. The reason is that, as in Riverso et al. (2014a), we use local controllers

based on MPC and, without reconfiguration, predictions made by MPC over the control horizon are based on the incorrect model of the generation area.

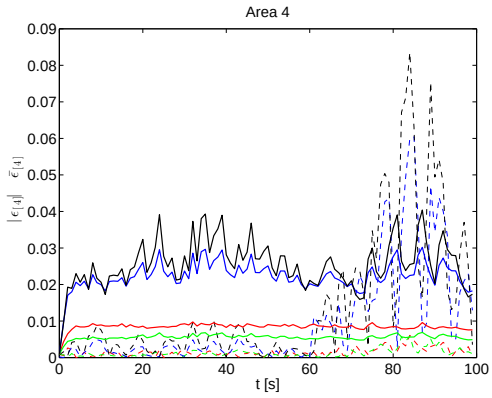

Fig. 6. Simulation for area 4 without isolation and reconfiguration: dashed lines are the absolute values of errors $\epsilon_{[4]}$ and bold lines are the thresholds $\bar{\epsilon}_{[4]}$.

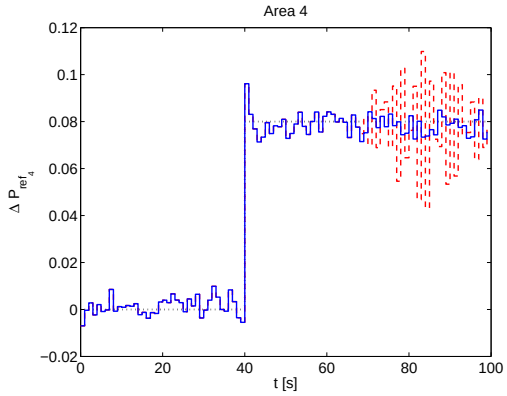

Fig. 7. Control input for area 4: dashed line is the set-point, bold blue line is the input with reconfiguration and dashed red line is the input without reconfiguration.

6. CONCLUDING REMARKS

In this paper, a distributed fault detection and isolation architecture for nonlinear LSS is designed in a PnP scenario. The proposed FDI architecture is able to manage plugging-in of novel subsystems and un-plugging of existent ones, requiring reconfiguration operations only in the neighboring subsystems. Moreover, the proposed PnP monitoring framework allows the unplugging of faulty subsystems in case it is necessary to avoid the risk of fault propagation. Simulation results show the potential of the proposed approach in power networks applications. Future research efforts will be devoted to provide detectability and isolability analysis and to extend the PnP methodology to the non completely measurable state case.

REFERENCES

Baheti, K. and Gill, H. (2011). Cyber-physical Systems. In T. Samad and A.M. Annaswamy (eds.), *The Impact of Control Technology*, 161–166. IEEE Control Systems Society.

Bendtsen, J., Trangbaek, K., and Stoustrup, J. (2013). Plug-and-Play Control Modifying Control Systems Online. *IEEE Trans. on Control Systems Technology*, 21(1), 79–93.

Blanke, M., Kinnaert, M., Lunze, J., and Staroswiecki, M. (2003). *Diagnosis and Fault Tolerant Control*. Springer, Berlin, Germany.

Bodenburg, S., Niemann, S., and Lunze, J. (2014). Experimental evaluation of a fault-tolerant plug-and-play controller. In *Proc. of European Control Conf.*, 1945–1950.

Boem, F., Ferrari, R.M.G., and Parisini, T. (2011). Distributed fault detection and isolation of continuous-time nonlinear systems. *Europ. J. of Control*, (5-6), 603–620.

Boem, F., Ferrari, R.M.G., Parisini, T., and Polycarpou, M.M. (2013). Distributed Fault Detection for Uncertain Nonlinear Systems: a Network Delay Compensation Strategy. In *Proc. of American Control Conf.*, 3549–3554.

Ferrari, R.M.G., Parisini, T., and Polycarpou, M.M. (2012). Distributed Fault Detection and Isolation of Large-Scale Discrete-Time Nonlinear Systems: An Adaptive Approximation Approach. *IEEE Trans. on Automatic Control*, 57(2), 275–290.

Frank, P.M. (1996). Analytical and qualitative model-based fault diagnosis–a survey and some new results. *European Journal of control*, 2(1), 6–28.

Izadi-Zamanabadi, R., Vinther, K., Mojallali, H., Rasmussen, H., and Stoustrup, J. (2012). Evaporator unit as a benchmark for plug and play and fault tolerant control. In *8th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, 701–706.

Li, W., Gui, W., Xie, Y., and Ding, S. (2009). 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*, 816–821.

Lunze, J. (1992). *Feedback control of large scale systems*. Prentice Hall, Systems and Control Engineering, Upper Saddle River, NJ, USA.

Patton, R., Frank, P., and Clark, D. (1989). *Fault Diagnosis in Dynamic Systems: Theory and Application*. Prentice Hall, Upper Saddle River, NJ, USA.

Riverso, S., Boem, F., Ferrari-Trecate, G., and Parisini, T. (2014a). Fault Diagnosis and Control-reconfiguration in Large-scale Systems: a Plug-and-Play Approach. In *Proc. of the 53rd IEEE Conf. on Decision and Control*, 4977–4982.

Riverso, S., Boem, F., Ferrari-Trecate, G., and Parisini, T. (2014b). Plug-and-play fault diagnosis and control-reconfiguration for a class of nonlinear large-scale constrained systems. Technical report. URL `http://arxiv.org/abs/1409.5224`.

Riverso, S., Farina, M., and Ferrari-Trecate, G. (2013). Plug-and-Play Decentralized Model Predictive Control for Linear Systems. *IEEE Trans. on Automatic Control*, 58(10), 2608–2614.

Samad, T. and Parisini, T. (2011). Systems of Systems. In T. Samad and A.M. Annaswamy (eds.), *The Impact of Control Technology*, 175–183. IEEE Control Systems Society.

Stoustrup, J. (2009). Plug & Play Control: Control Technology towards new Challenges. In *Proc. of the 10th European Control Conference*, 1668–1683.

Yin, S., Ding, S.X., Xie, X., and Luo, H. (2014). A review on basic data-driven approaches for industrial process monitoring. *Industrial Electronics, IEEE Trans. on*, 61(11), 6418–6428.

Zhang, X. and Zhang, Q. (2012). Distributed fault diagnosis in a class of interconnected nonlinear uncertain systems. *Int. Journal of Control*, 85(11), 1644–1662.