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).  
∗∗ Dip. di Ingegneria Industriale e dell’Informazione, Università degli  
Studi di Pavia, Italy ({stefano.riverso|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 involve only  
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 large-scale systems (see, for example, Lunze (1992)), Systems-of-Systems (SoS) (Samad and Parisini (2011)) and Cyber-Physical Systems (CPS) (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, 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, nowadays, reliability is a key requirement in the 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); Venkatasubramanian 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 Patton et al. (2007), Li et al. (2009), Zhang and Zhang (2012), Boem et al. (2011a), 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. 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 MPC for nonlinear LSS. Compared with Riverso et al. (2014a), the present paper shows the following significant differences:  

1. 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;  
2. the fault isolation problem is also considered;  
3. 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, dealing with just the disconnection of the faulty subsystem and not addressing a possible subsequent plug-in of new subsystem.  

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, Boden-
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 specific operations are then described in Section 4. Some simulation results in the context of a power systems application are presented in Section 5. Finally, some concluding remarks are given in Section 6.

Notation. We use $a : b$ for the set of integers $\{a, a + 1, \ldots, b\}$. The column vector with $s$ components $v_1, \ldots, v_s$ is denoted $v = (v_1, \ldots, v_s)$. Let $v, \bar{v} \in \mathbb{R}^s$, the inequality $|v| \leq \bar{v}$, component-wise means $|v_i| \leq \bar{v}_i$, $i = 1 : s$.

2. PROBLEM FORMULATION

Let us consider a LSS, composed at time $t$ of $M$ interconnected subsystems. Each subsystem dynamics can be described as

$$\dot{x}_{i}^t = f_i(x_{i}^t, \psi_{i}^t, u_{i}^t) + w_i(x_{i}^t, \psi_{i}^t, t)$$

(1)

where $x_{i}^t \in \mathbb{R}^{n_i}$, $u_{i}^t \in \mathbb{R}^{m_i}$, $i \in \mathcal{M} = \{1, \ldots, M\}$, are the local state and input, respectively, at time $t$ and $x_{i}^t$ stands for $x_{i}^t$ at time $t + 1$. The vector of interconnection variables $\psi_{i}^t \in \mathbb{R}^{p_i}$ collects components of the states $\{x_{j}^t\}_{j \in \mathcal{N}_i}$ that influence the dynamics of $x_{i}^t$, where $\mathcal{N}_i$ is the set of parents of subsystem $i$ defined as $\mathcal{N}_i = \{ j \in \mathcal{M} : \frac{\partial x_{i}^t}{\partial x_{j}^t} \neq 0, i \neq j \}$. We also define $\mathcal{C}_i = \{ k : i \in \mathcal{N}_k \}$ as the set of children of $\Sigma_i$. Finally, we say that $\Sigma_{i}[j]$ and $\Sigma_{j}[i]$ are neighbors if $j \in \mathcal{N}_i$ or $j \in \mathcal{C}_i$.

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 diagnosters. 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. Again, after
fault isolation, two alternatives are possible: the unplug-
ing 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
depicted in Fig. 3.

3. THE FAULT DETECTION AND ISOLATION
ARCHITECTURE

In this section, we design a distributed FDI architecture
for the considered PnP framework. Each subsystem is
equipped with a local diagnoser.

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 \( \epsilon[i] = y[i] - \)
\( \hat{x}[i] \) is compared component-wise with a suitable time-
varying detection threshold \( \bar{\epsilon}[i] \in \mathbb{R}^{n_i} \), hence obtaining
a local fault decision about the status of the subsystem,
either as healthy or faulty. If the residual crosses the
threshold, we can conclude that a fault has occurred. 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 \( H_i : 
“Subsystem \Sigma[i] \text{ is healthy}” \). If the condition is violated
at some time instant, then the hypothesis \( H_i \) 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 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 subsystem is monitored by
a local nonlinear estimator, based on the local model \( \Sigma[i] \)
in (1). The $k_i$-th non-shared state variable of $\Sigma_{[i]}$ can be estimated as

$$\hat{x}^+_{i,k_i} = \lambda(\hat{x}_{i,k_i} - y_{i,k_i}) + f_{i,k_i}(y_{i,k_i}, z_{i,k_i}, u_{i,k_i}),$$  \hspace{1cm} (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 $x_{i,k} = x_{i,j,k}$, 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 $x_{i,[k]}$. The estimates of shared variables are provided by the following estimation model:

$$\hat{x}^+_{i,[k]} = \lambda(\hat{x}_{i,[k]} - y_{i,[k]}) + \sum_{j \in \mathbb{S}^k} W^k_{i,j} \left[ \lambda(\hat{x}_{j,[k]} - \hat{x}_{i,[k]}) + f_{j,k_i}(y_{j,[k]}, z_{j,[k]}, u_{j,[k]}) \right], \hspace{1cm} (5)$$

where $W^k_{j,i}$ 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 $\Sigma_{[j]}$ to weight the terms communicated by $\Sigma_{[i]}$, 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 $W^k_{i,j} = 1$ 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 $x_{i,[k]}$ when it is not strictly necessary.

3.3 The detection threshold

In order to properly define a threshold for FD, we analyze the dynamics of the local diagnoser 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 all $j \in \mathbb{S}^k$ there are $k_i$ and $k_j$ such that it holds $f_{i,k_i}(x_{i,[k]}, y_{i,[k]}, u_{i,[k]}) = f_{j,k_j}(x_{j,[k]}, y_{j,[k]}, u_{j,[k]})$, the $k$-th state estimation error dynamics model is given by

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

where $\epsilon_{j,[k]} = \hat{x}_{j,k} - x_{j,[k]}$, $\lambda \epsilon_{i,[k]} + \Delta f_{i,k} + w_{i,k}(x_{i,[k]}, y_{i,[k]}, u_{i,[k]})$, $w_{i,k}(x_{i,[k]}, y_{i,[k]}, u_{i,[k]})$, $\lambda \theta_{i,[k]}$, $\lambda \bar{\theta}_{i,[k]}$, and $\bar{\theta}^+_{i,[k]}$ are the measurement error at time $t+1$ and $k$-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. (2011a) (where it was useful for a delay compensation strategy), here we define the time-varying consensus-weighting matrix $W^k$ for each $(i,j)$-th component for PuP purposes, by choosing in the consensus sum the lowest threshold term from all the threshold additive terms in (6) available in $\mathbb{S}^k$, i.e., by weighting more the currently connected subsystem that has lower uncertainty in its measurements and in the local model:

$$W^k_{i,j} = \begin{cases} 1 & \text{if } j = \arg\min_{j \in \mathbb{S}^k} \lambda(\epsilon_{j,[k]} + \bar{\theta}_{i,[k]} + \Delta f_{j,k}) + \bar{\theta}^+_{i,[k]} + w_{j,k}(x_{j,[k]}, y_{j,[k]}, u_{j,[k]}) \\ 0 & \text{otherwise} \end{cases}$$ \hspace{1cm} (7)$$

At each time-step, every local fault-diagnoser receives estimates and consensus terms of variable $x_{i,[k]}$ only from the

$$\Delta \bar{f}_j = \max_{y_{j,[k]} \in \mathcal{E}_j} \psi_j(y_j, |\Delta f_j|).$$

It is worth noting that Assumption 1 implies that the state and input variables are bounded; hence all quantities in (6) are bounded as well; $\bar{\theta}_{i,[k]}$ and $\bar{\theta}^+_{i,[k]}$ are defined in Assumption 1. The threshold dynamics (6) can be initialized with $\epsilon_{i,[k]}(0) = \bar{\theta}_{i,[k]}(0)$.

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 in $\mathbb{S}^k$ only the interconnection variables and the consensus terms for estimates and thresholds, locally computed.

The threshold in (6) guarantees the absence of false-positive alarms before the occurrence of the fault 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 (in Rivero et al. (2014b) some detectability results are given).

3.4 The consensus matrix

In this subsection, we explain how to design the consensus matrix in an appropriate way in order to allow PuP operations. Consensus is applied to the shared variables, i.e., state variables representing the interconnection between two or more subsystems. For PuP 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 diagnoser (and so the related subsystem) 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. (2013a) (where it was useful for a delay compensation strategy), here we define the time-varying consensus-weighting matrix $W^k$ for each $(i,j)$-th component for PuP purposes, by choosing in the consensus sum the lowest threshold term from all the threshold additive terms in (6) available in $\mathbb{S}^k$, i.e., by weighting more the currently connected subsystem that has lower uncertainty in its measurements and in the local model:

$$W^k_{i,j} = \begin{cases} 1 & \text{if } j = \arg\min_{j \in \mathbb{S}^k} \lambda(\epsilon_{j,[k]} + \bar{\theta}_{i,[k]} + \Delta f_{j,k}) + \bar{\theta}^+_{i,[k]} + w_{j,k}(x_{j,[k]}, y_{j,[k]}, u_{j,[k]}) \\ 0 & \text{otherwise} \end{cases}$$ \hspace{1cm} (7)$$

At each time-step, every local fault-diagnoser receives estimates and consensus terms of variable $x_{i,[k]}$ only from the
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 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: 
\[
\epsilon_{k,E} := \text{col}(\epsilon_{i,k,j} : j \in \mathcal{S}^k).
\]
Hence, the dynamics of \( \epsilon_{k,E} \) can be described as:
\[
\epsilon_{k,E}(t) = W^k[\lambda_{k,E} + \Delta f_{k,E} + w_{k,E} - \lambda_{k,E} + \lambda_{k,E} + \sum_{j=1}^{t} \lambda_{W}(j)] + \lambda_{k,E}(t) + \epsilon_{k,E}(t + 1). \tag{8}
\]
where \( \epsilon_{k,E} \) is a column vector, collecting the corresponding \( k \)-th vector \( \epsilon_{i,k,j} \), i.e. \( \epsilon_{i,k,j} \), for each \( j \in \mathcal{S}^k \); \( \Delta f_{k,E} \) and \( w_{k,E} \) are column vectors collecting the vectors \( w_{j,k} \) and \( \Delta f_{j,k} \), with \( j \in \mathcal{S}^k \), respectively. The following convergence result can now be provided.

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

Proof. The proof is carried out similarly as in Riverso et al. (2014b). Specifically, since \( W^k \) is a stochastic matrix, its spectral 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:
\[
U_{k,E}(t) = W^k(t)[\Delta f_{k,E}(t) + w_{k,E}(t) - \lambda_{k,E}(t)] + \lambda_{k,E}(t) + \epsilon_{k,E}(t + 1).
\]
We have:
\[
||\epsilon_{k,E}(t + 1)|| \leq ||\lambda W^k(t)\epsilon_{k,E}(t)|| + ||U_{k,E}(t)|| \leq \sum_{j=1}^{t} \lambda W^k(t) |||W^k(t - 1)|| |W^k(0)|| \epsilon_{k,E}(0)|| + \sum_{j=1}^{t} \lambda W^k(t) |||W^k(t - 1)|| |W^k(0)|| \epsilon_{k,E}(j)|| + \lambda_{k,E}(t) ||U_{k,E}(j)||
\]
\[
\leq \gamma \lambda ||\epsilon_{k,E}(0)|| + \sum_{j=1}^{t} \gamma^{t-j} ||U_{k,E}(j)||
\]
\[
\leq \frac{1}{1 - \gamma} \sup_{j \geq 1} ||U_{k,E}(j)||
\]
For \( t \to \infty \), the unforced system converges to zero and the series converges to a bounded value (see results in Michalec and Gerencsér (2002)). Moreover, using results in Sichitiu and Bauer (2003) for unforced systems, we can state that a system \( x(t + 1) = A(t)x(t) \), with \( A(t) \in \text{conv}(A_1, \ldots, A_N) \), it is exponentially stable iff \( \exists \) a sufficiently large integer \( q \) such that \( ||A_1 A_2 \ldots A_q|| \leq \gamma < 1 \), \( \forall (i_1, \ldots, i_q) \in \{1, \ldots, N\}^q \). 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 \( W^k(t)W^k(t - 1) \ldots W^k(0) \) is a stochastic matrix. Hence, since \( 0 < \lambda < 1 \), we have \( ||\lambda^j W^k(t) || W^k(t - 1) \ldots W^k(0)|| < 1 \) and the hypothesis is satisfied. Finally, since all the uncertain terms are bounded, then the discrete-time system (8) is BIBO stable.

3.6 Distributed Fault Isolation

For fault isolation purposes, we implement a Generalized Observer Scheme (GOS, see Frank (1990); Patton et al. (1989)), following the fault isolation approach proposed in Zhang et al. (2002) for centralized architectures and in Ferrari et al. (2012) for distributed ones. We adapt it for the PnP scenario we are considering. We assume that each subsystem knows a local fault set \( F_i \), collecting all the \( N_F \) possible nonlinear fault functions. This could be a limitation: in Ferrari et al. (2012), a more complex approach is introduced, where some approximators are designed to learn also unknown fault functions. Similar methodologies can be implemented also in the PnP architecture proposed in this paper, but for the sake of simplicity, here we assume that the local fault functions are completely known: \( \phi_i(x_i), \psi_i, w_i \) \( \forall \{1, \ldots, N_F \} \). After fault detection, each interested LFD uses \( N_F \) nonlinear estimators of the local state \( x_i \), called Fault Isolation Estimators (FIEs), to order to locally determine which of the possible \( N_F \) faults in the set \( F_i \) has occurred.

In the case that a fault could propagate from the faulty subsystem to the LSS, then we propose a reconfiguration process, by disconnecting the faulty subsystem (see Fig. 2) immediately after fault detection or after fault isolation (depending on the application criticality), in order to avoid fault propagation. In the case that a fault is detected in a shared variable, all the subsystems (two or more) sharing that variable could detect the fault. In this case, the involved subsystems will activate the fault isolation process.

After a fault has been detected at time \( T_d \) in the \( i \)-th subsystem, each LFD enables its bank of \( N_F \) FIEs. After the generic \( i \)-th FIE estimator is activated, with \( i \in \{1, \ldots, N_F \} \), it monitors its \( i \)-th subsystem, providing a local state estimate \( \hat{x}_i \) of the local state \( x_i \). The difference between the estimate \( \hat{x}_i \) and the measurements \( y_i \) will yield the estimation error \( e_i \), which can be used as a residual and compared, component by component, to a suitable isolation threshold \( \varepsilon_i \in \mathbb{R}^n \).

\[
|e_{i,k}| \leq \varepsilon_{i,k} \forall k = 1, \ldots, n_i \tag{10}
\]
is associated to the \( l \)-th fault hypothesis

\[
\mathcal{H}_{i,l} : "The subsystem \{i\} is affected by the \( l \)-th fault",
\]
with \( l = 1, \ldots, N_F \). As soon as the hypothesis \( \mathcal{H}_{i,l} \) is falsified, the fault \( \phi_i \) 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.

Remark 4. If a fault has been locally isolated, we can say that it actually occurred only if we assume that only faults belonging to the set \( F_i \) may occur.
3.7 The Fault Isolation Estimators

After the fault $\phi_i$ has occurred, the dynamics of the $k$-th state component of the $i$-th subsystem becomes

$$x_{i,k}^+ = f_{i,k}(x_{ij}, \psi_{ij}, u_{ij}) + w_{i,k}(x_{ij}, \psi_{ij}) + \phi_{i,k}(x_{ij}, \psi_{ij}, u_{ij}, t),$$

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

$$\dot{x}_{i,k}^+ = \lambda(x_{i,k}^+ - y_{i,k}) + \sum_{j \in S_k} W_{i,j} \left[ \lambda(x_{j,k}^+ - \hat{x}_{i,k}) + f_{j,k}(y_{ij}, z_{ij}, u_{ij}) + \phi_{j,k}(y_{ij}, z_{ij}, u_{ij}, t) \right].$$

The corresponding estimation error dynamic equation is

$$\epsilon_{i,k}^+ = \sum_{j \in S_k} W_{i,j} \left[ \lambda\epsilon_{j,k}^+ + \Delta f_{j,k} + w_{j,k}(x_{ij}, \psi_{ij}) + \Delta \phi_{j,k} - \lambda\theta_{i,k} + \lambda\theta_{i,k} + \phi_{i,k}^+ \right],$$

with

$$\Delta \phi_{j,k} = \phi_{i,k}(x_{ij}, \psi_{ij}, u_{ij}, t) - \phi_{i,k}(y_{ij}, z_{ij}, u_{ij}, t).$$

Now, considering a matched fault (that is, $\phi_{i,k} = \phi_{i,k}(x_{ij}, \psi_{ij}, u_{ij}, t)$, $\forall i \in S_k$), the error equation absolute value can be bounded by a threshold that is solution of the following equation

$$\epsilon_{i,k}^+ = \sum_{j \in S_k} W_{i,j} \left[ \lambda\epsilon_{j,k}^+ + \lambda\theta_{i,k} + \lambda\theta_{i,k} + \lambda\theta_{i,k} + \lambda\theta_{i,k} + \lambda\theta_{i,k} + \lambda\theta_{i,k} + \phi_{i,k}^+ \right]$$

$$+ \Delta \phi_{j,k} - \lambda\theta_{i,k} + \lambda\theta_{i,k} + \phi_{i,k}^+ \right),$$

where $\Delta \phi_{j,k} = \max_{x_{ij} \in X_j, \psi_{ij} \in \psi_j} |\Delta \phi_{j,k}|$. This threshold guarantees by definition that no matched fault will be excluded because of uncertainties. The time varying consensus matrix designed in Section 3.4 is useful also for fault isolation in order to allow Plug-and-Play operations. The derived distributed fault isolation methodology is robust to the PnP considered scenario. In the following section, we will explain how plug-in and unplugging operations are possible.

4. RECONFIGURATION STRATEGY

In the case of a non-matched fault (that is, $\phi_{i,k} \neq \phi_{i,k}(x_{ij}, \psi_{ij}, u_{ij}, t)$ for some $i \in S_k$, with $p \neq l$), then the dynamics of the estimation error of the $l$-th FIE in $\Sigma_{ij}$ can be written as

$$\epsilon_{i,k}^+ = \sum_{j \in S_k} W_{i,j} \left[ \lambda\epsilon_{j,k}^+ + \lambda\theta_{i,k} + \lambda\theta_{i,k} + \lambda\theta_{i,k} + \lambda\theta_{i,k} + \lambda\theta_{i,k} + \lambda\theta_{i,k} + \phi_{i,k}^+ \right],$$

with

$$\Delta \phi_{j,k} = \phi_{i,k}(x_{ij}, \psi_{ij}, u_{ij}, t) - \phi_{i,k}(y_{ij}, z_{ij}, u_{ij}, t).$$

With a similar procedure as the one followed in Boem et al. (2011a); Ferrari et al. (2012), some fault isolability conditions can be derived, in order to define some class of faults that cannot be isolated by the conservative derived thresholds, due to the presence of uncertainties (due to lack of space, is not included in the present paper).

4.1 Subsystem unplugging

In this paragraph, we show how to reconfigure local diagnosers in the LSS when a subsystem $\Sigma_{ij}$ is disconnected from the LSS, guaranteeing estimators convergence and monitoring of the new network with one less subsystem. We need to reconfigure fault diagnosers for children subsystems $\Sigma_{ij}$, $i \in C_j$, since they do not receive anymore the interconnection variables values from the parent subsystem $\Sigma_{ij}$. Moreover if the unplugged subsystem was sharing variable $k$, its consensus contribution will not be received by neighboring subsystems sharing $k$; hence, the weights associated to $\Sigma_{ij}$ in the consensus matrices $W^k$ of subsystems in $S_k$ are set to zero (see (7)). More specifically:

- In the children subsystems $i \in C_j$, the components of $\hat{\psi}_{ij}$ and $z_{ij}$ related to subsystem $\Sigma_{ij}$ become equal to 0 or set to defined values (in the case 0 is a not appropriate value for the considered variable). This is needed for the computation of detection (5) and isolation (12) estimates and related thresholds (6) and (13).

- In the neighboring subsystems $i$, with $i \in C_j$ or $i \in N_j$, sharing some variables with $\Sigma_{ij}$, the weights associated with $\Sigma_{ij}$ 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 (12), the plug-in is always feasible. More specifically, if a subsystem $\Sigma_{ij}$ is added to the LSS:

- In the children subsystems $i \in C_j$, the components of $\hat{\psi}_{ij}$ and $z_{ij}$ related to subsystem $\Sigma_{ij}$ are received and used for the computation of detection (5) and isolation (12) estimates and related thresholds (6) and (13).

- In the neighboring subsystems $i$, with $i \in C_j$ or $i \in N_j$, sharing some variables $k$ with $\Sigma_{ij}$, the consensus matrices $W^k$ are computed as in (7) considering also the components received from $\Sigma_{ij}$.

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 Rivero 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 Figure 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.

At time $t = 60s$, 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 Figure 5 we show that the fault is detected a time $t = 68s$ 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 Figure 5 at time $t = 68s$, the state estimations and the thresholds are changed in accordance with the new state estimator.

In Figure 6 and 7 we show problems that can occur without a suitable reconfiguration. In the simulation, in Figure 6, we assume that at time $t = 68s$ neither the isolation procedure is executed nor the faulty area is unplugged (indeed we can notice that for $t > 68s$ the fault is still detected). Moreover, in Figure 7 we also note that without the reconfiguration process, hence 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.

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 the case it is necessary to avoid the risk of propagation of faults in the interconnected LSS. Simulation results show the potential of the proposed approach in a power networks application.

Future research efforts will be devoted to provide the detectability and isolability analysis and to extend the PnP methodology to the case in which the state variables are not fully accessible.

REFERENCES


