Stochastic Fault Detection in a Plug-and-Play Scenario

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

***Abstract*— This paper proposes a novel stochastic Fault Detection (FD) approach for the monitoring of Large-Scale Systems (LSSs) in a Plug-and-Play (PnP) scenario. The proposed architecture considers stochastic bounds on the measurement noises and modeling uncertainties, providing probabilistic time-varying FD thresholds with guaranteed false alarms probability levels. The monitored LSS consists of several interconnected subsystems and the designed FD architecture is able to manage plugging-in of novel subsystems and un-plugging of existing ones. Moreover, the proposed PnP approach can perform 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 scalable architecture. A consensus approach is used for the estimation of variables shared among more than one subsystem; a method is proposed to define the time-varying consensus weights in order to allow PnP operations and to minimize at each step the variance of the uncertainty of the FD thresholds. Simulation results on a Power Network application show the effectiveness of the proposed approach.**

I. Introduction

The interest towards LSS (see, for example, [1]), Systems-of-Systems [2] and Cyber-Physical Systems [3] is steadily growing both in academia and industry. These systems, 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. Reliability is a key requirement especially in these systems, as their increased size and complexity implies an increased risk of faults. When monitoring this kind of systems, the adoption of decentralized and distributed methods is usually necessary due to computational, communication, scalability and reliability limits (see [4], [5], [6], [7], [8] as examples). Moreover, an emerging requirement is the design of monitoring architectures that are robust to changes that may occur in the dynamic structure of the LSS. This is why, in this paper we develop a distributed FD methodology, properly designed for a PnP scenario. Differently from previous works ([7], [8], [9], [10]) where a deterministic approach was adopted, in this paper the novelty is to consider stochastic bounds on the noises and uncertainties, and to derive probabilistic thresholds for fault detection. The aim is to propose a monitoring architecture which is closer to industrial applications, where deterministic bounds on the uncertainties are often difficult to be obtained, producing then conservative results. To the authors' knowledge, this is the first time that a stochastic distributed monitoring architecture is designed for LSS in a PnP scenario. Some recent results are presented in [9], integrating distributed model-based fault detection with MPC for nonlinear LSS, and [10], where a PnP FD and Isolation architecture is designed. Compared with [9], the present paper shows the following significant differences.

- A general class of nonlinear systems is addressed, while in [9] the analysis was limited to a class of nonlinear systems, with matched control inputs.
- We exploit a full PnP framework, where the monitoring architecture is robust to plugging-in and unplugging of subsystems. Instead, in [9] only a reconfiguration process after fault occurrence is considered, dealing with just the disconnection of the faulty subsystem and not addressing a possible plug-in of new subsystems.
- Here a stochastic approach is proposed, while in [9] a deterministic framework was considered.

This last point is also the one that mainly describes the novelty with respect to [10]. In this paper, the main contribution is to define stochastic thresholds for fault detection, able to guarantee a certain false alarms probability and allowing PnP operations. A similar distributed stochastic monitoring architecture has been proposed in [11], but in that paper, the problem of designing an optimal decomposition of the LSS was considered, where the dynamics of the system do not change along the time, while here we consider a PnP scenario. Moreover, in this paper, as a novel contribution, we prove the convergence of the estimation error mean and we define a novel time–varying consensus approach for the estimation of state variables shared among more than one subsystems. We propose a method to analytically compute the consensus weights so as to allow PnP operations and to minimize the magnitude of the thresholds .

Recently, some works have been published dealing with PnP scenarios: [12], [13], [14] analyze only the control problem; [15] designs a fault-tolerant control strategy for a centralized system; [16] presents a fault-tolerant PnP controller, but, differently from the proposed work, it considers linear systems with a centralized approach. [17] proposes a PnP reconfiguration of Intelligent Electronic Devices using event-based Petri Net fault diagnosis methods.

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

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

S. Riverso is with United Technologies Research Center Ireland, 4th Floor, Penrose Business Center, Penrose Wharf, Cork, Ireland. (riverss@utrc.utc.com)

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

II. Problem formulation

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

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

where $x_{[i]} \in \mathbb{R}^{n_i}$, $u_{[i]} \in \mathbb{R}^{m_i}$, $i \in \mathcal{M} = 1, \ldots, M$, are the local state and input, respectively, at time t and $x_{[i]}^{+}$ denotes $x_{[i]}$ 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 at time t, 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 $j \in \mathcal{C}_i$. $f_i(\cdot) : \mathbb{R}^{n_i} \times \mathbb{R}^{p_i} \times \mathbb{R}^{m_i} \to \mathbb{R}^{n_i}$ represent possibly nonlinear nominal dynamics, including known relationships with parent subsystems by means of the interconnection variables, while $w_i(\cdot) : \mathbb{N} \to \mathbb{R}^{n_i}$ represents modeling uncertainties, considering unknown possibly nonlinear coupling among subsystems. 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 $x_{[i,k]}$. 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.

In this paper, we assume that the state vector is fully accessible (possibly through noisy measurements). Hence, the local output equation is:

$$y_{[i]} = x_{[i]} + \varrho_{[i]}, \tag{2}$$

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 $\varrho_{[j]}$, $j \in \mathcal{N}_i$.

The following assumptions are needed:

Assumption 1: The modeling uncertainty w_i is an unknown function, modeled as a stochastic process of unknown distribution. We know at each time instant t the mean and the variance of the stochastic variables $w_i(t)$, for all $i \in \mathcal{M}$:

$$w_i(t) \approx (\mu_{w_i}(t), \sigma_{w_i}(t)),$$

Assumption 2: The measurement noise $\varrho_{[i]}$ is a stochastic process of known distribution. We assume to know at each time instant t the mean and the variance of the stochastic variables $\varrho_{[i]}(t)$ for all $i \in \mathcal{M}$:

$$\varrho_{[i]}(t) \approx (\mu_{\varrho_{[i]}}(t), \sigma_{\varrho_{[i]}}(t)).$$

The values of mean and variance in Assumptions 1 and 2 are obtained from the knowledge of the system process and sensors methods.

Each subsystem is monitored by one Local Fault Diagnoser (LFD). Some state variables, which we call *shared* variables, are monitored by more than one LFD. These variables represent the coupling variables: by means of them, two (or more) subsystems are connected (see Fig.1). 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. As a consequence, the considered decomposition of the LSS is *overlapping* ([1]), since some of the variables "belong" to more than one subsystem.

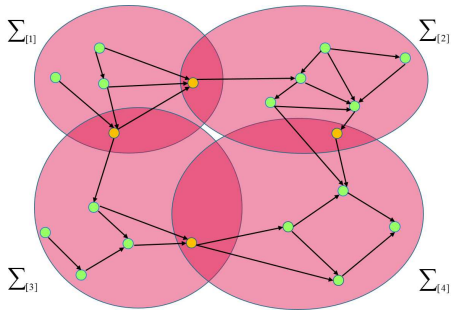

Fig. 1. The possibly overlapping decomposition of the LSS structural graph: the small green circles represent the state and input variables; the yellow ones are the shared state variables.

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 an isolation phase or in alternative to an isolation step. In general, after the detection of a fault, depending on the specific application context and criticality, two distinct actions may be feasible: i) immediate "disconnection" of the faulty subsystem after detection or ii) continuation of the system operation in "safety mode" and simultaneously fault isolation. This second option is not analyzed in this draft.

III. The Fault Detection Architecture

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

An estimate $\hat{x}_{[i]}$ of the local state variables is defined; the estimation error $\epsilon_{[i]} \triangleq y_{[i]} - \hat{x}_{[i]}$ is then compared component-wise with some properly designed time-varying stochastic detection thresholds $\bar{\epsilon}_{[i]}^{upp}$ and $\bar{\epsilon}_{[i]}^{low} \in \mathbb{R}^{n_i}$. If the residual lies in the interval between the thresholds, then the local fault decision about the status of the subsystem is healthy with a certain probability; otherwise, if it crosses one of the two thresholds, we say that a fault has probably occurred. In the PnP framework, the diagnosers are designed so to guarantee the convergence of the mean of the estimation 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.

A. 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

$$\hat{x}^+_{[i,k_i]} = \lambda(\hat{x}_{[i,k_i]} - y_{[i,k_i]}) + f_{i,k_i}(y_{[i]}, z_{[i]}, u_{[i]}) \,, \quad (3)$$

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 thanks to the overlapping for implementing a deterministic consensus approach (see [10] where the effectiveness of this consensus approach is demonstrated for a stochastic framework). 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 t. Let the shared variable be $x_{[i,k_i]}$. The estimates of shared variables are provided by the following estimation model:

$$\hat{x}^+_{[i,k_i]} = \sum_{j \in \mathbb{S}^k} W^k_{i,j} \left[\lambda(\hat{x}_{[j,k_j]} - y_{[j,k_j]}) + f_{j,k_j}(y_{[j]}, z_{[j]}, u_{[j]}) \right] \,, \quad (4)$$

where $W^k_{i,j}$ are the components of a row-stochastic matrix W^k, which will be defined in Subsection III-C, 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 (4) holds also for the case of non-shared variables (3), 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 it is not strictly necessary.

B. The detection thresholds

In order to properly define the stochastic upper and lower thresholds 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 $\forall i, j \in \mathbb{S}^k$ 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

$$\epsilon^+_{[i,k]} = \sum_{j \in \mathbb{S}^k} W^k_{i,j} \left[\lambda \epsilon_{[j,k]} + \Delta f_{j,k} + w_{j,k} + \varrho^+_{[i,k]} \right] \,, \quad (5)$$

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 $t+1$. This is a general formulation, and it holds also in the case of non-shared variables, where it is simply:

$$\epsilon^+_{[i,k]} = \lambda \epsilon_{[i,k]} + \Delta f_{i,k} + w_{i,k} + \varrho^+_{[i,k]} \,, \quad (6)$$

We now analyze the residual, first in the non–shared case and then in the shared one, in order to derive the fault detection thresholds. It is worth noting that at time t, when the thresholds are computed for the step $t+1$, $\epsilon_{[i,k]}$ is not a random variable, since it can be computed as the difference between the measurement $y_{[i,k]}$ and the estimate $\hat{x}_{[j,k_j]}$. We therefore analyze the stochastic part of the residual:

$$\chi^+_{[i,k]} = \Delta f_{i,k} + w_{i,k} + \varrho^+_{[i,k]}.$$

Its mean and variance can be computed as

$$\mathbb{E}[\chi^+_{[i,k]}] = \mathbb{E}[\Delta f_{i,k}] + \mathbb{E}[w_{i,k}] + \mathbb{E}[\varrho^+_{[i,k]}]$$

$$\mathrm{Var}[\chi^+_{[i,k]}] = \mathrm{Var}[\Delta f_{i,k}] + \mathrm{Var}[w_{i,k}] + \mathrm{Var}[\varrho^+_{[i,k]}] + 2\mathrm{Cov}[\Delta f_{i,k}, \varrho^+_{[i,k]}], \quad (7)$$

where the following further assumptions are needed.

Assumption 3: The measurement noise $\varrho_{[i,k]}$ and the modeling uncertainty $w_{i,k}$ are not correlated.

Thanks to this assumption, we can assume also that the covariance between $\Delta f_{i,k}$, which is the error on the nominal model due to the measurement noise, and the modeling uncertainty $w_{i,k}$ is null.

Assumption 4: Given the values of $y_{[i]}$, $z_{[i]}$, $u_{[i]}$ and known the probabilistic distribution of $\varrho_{[i]}$ (and so of $\theta_{[i]}$), it is possible to compute $\mathbb{E}[\Delta f_{i,k}]$ and $\mathrm{Var}[\Delta f_{i,k}]$, where $\Delta f_{i,k} = f_{i,k}(y_{[i]} - \varrho_{[i]}, z_{[i]} - \theta_{[i]}, u_{[i]}) - f_{i,k}(y_{[i]}, z_{[i]}, u_{[i]})$. In the linear case, the solution of this problem is trivial and it is not necessary to know the measurement noise distribution.

It is worth noting that, in the case the measurement noise $\varrho_{[i]}$ is a white process, then $\mathrm{Cov}[\Delta f_{i,k}, \varrho^+_{[i,k]}] = 0$ and (7) can be simplified. Moreover, we consider the following additional assumption for the sake of simplicity.[1]

Assumption 5: The measurement noise and the modeling uncertainty are zero-mean: $\mu_{\varrho_{[i]}}(t) = 0$, $\mu_{w_i}(t) = 0$, $\forall t \geq 0$. Then, (7) can be rewritten as:

$$\mathbb{E}[\chi^+_{[i,k]}] = \mathbb{E}[\Delta f_{i,k}] \quad (8)$$

$$\mathrm{Var}[\chi^+_{[i,k]}] = \mathrm{Var}[\Delta f_{i,k}] + \sigma^2_{w_{i,k}} + \sigma^2_{\varrho^+_{[i,k]}} + 2\mathrm{Cov}[\Delta f_{i,k}, \varrho^+_{[i,k]}] \quad (9)$$

[1] In case Assumption 5 is not satisfied, it is sufficient to introduce mean values different from zero in the estimator formulation.

We now derive some time-varying stochastic bounds for $\chi^+_{[i,k]}$. Chebyshev inequalities can be used, without any assumption on the distribution of the residual. For a stochastic variable X, with mean $\mu(X)$ and standard deviation $\sigma(X)$, it holds:

$$Pr\big(\mu(X) - \alpha\sigma(X) \leq X \leq \mu(X) + \alpha\sigma(X)\big) \geq 1 - 1/\alpha^2 \tag{10}$$

where $\alpha > 1$ is a tunable, real positive valued scalar. Therefore, it is possible to obtain a lower and a upper stochastic thresholds for the residual signal, so that at each time t

$$\bar{\epsilon}^{\,low}_{[i]} \leq \epsilon_{[i]} \leq \bar{\epsilon}^{\,upp}_{[i]} \tag{11}$$

with a certain probability. For non-shared variables, the thresholds can be computed at each step t for the following step $t+1$ as:

$$\begin{aligned}\bar{\epsilon}^{+\,upp/low}_{[i,k]} &= \lambda\bar{\epsilon}^{\,upp/low}_{[i,k]} + \mathbb{E}[\chi^+_{[i,k]}] \pm \alpha\left[\text{Var}[\chi^+_{[i,k]}]\right]^{\frac{1}{2}} \\ &= \lambda\bar{\epsilon}^{\,upp/low}_{[i,k]} + \mathbb{E}[\Delta f_{i,k}] \pm \alpha\left[\text{Var}[\Delta f_{i,k}]\right. \\ &\quad \left. +\sigma^2_{w_{i,k}} + \sigma^2_{\varrho^+_{[i,k]}} + 2\text{Cov}[\Delta f_{i,k}, \varrho^+_{[i,k]}]\right]^{\frac{1}{2}}. \end{aligned} \tag{12}$$

The value of α is a tuning parameter by which different values of guaranteed false-alarms rate can be set.

Let us now analyze the case of variables shared among more than one subsystem. As previously mentioned, in the distributed FD architecture considering possibly overlapping decomposition, certain state variables may be measured, estimated and monitored by more than one LFD. In this shared-variable case, the residual is

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

Similarly as before, we obtain the following expressions for the lower and upper thresholds:

$$\begin{aligned}\bar{\epsilon}^{+\,upp/low}_{[i,k]} &= \sum_{j\in\mathbb{S}^k} W^k_{i,j}\left[\lambda\bar{\epsilon}^{\,upp/low}_{[j,k]} + \mathbb{E}[\Delta f_{j,k}]\right] \\ &\pm \alpha\left\{\sum_{j\in\mathbb{S}^k}(W^k_{i,j})^2\left[\text{Var}[\Delta f_{j,k}] + \sigma^2_{w_{j,k}} + \sigma^2_{\varrho^+_{[j,k]}}\right.\right. \\ &\quad \left.\left. +2\text{Cov}[\Delta f_{j,k}, \varrho^+_{[j,k]}]\right]\right\}^{\frac{1}{2}}. \end{aligned} \tag{13}$$

It is worth noting that, since $0 \leq W^k_{i,j} \leq 1$ for every (i,j), then $\sum_{j\in\mathbb{S}^k}(W^k_{i,j})^2 \leq 1$. Therefore, the variance component of the threshold for the shared case in (13) is lower that in the non-shared case in (12) in the case that the variance of the uncertainty terms is equal for all the subsystems. Then, in this case, we are able to show that, sharing some state variables among more than one LFD by means of the proposed consensus method implies the reduction of the variance of the residual signal thus leading to less conservative detection thresholds (see [10]).

Remark 1: 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 (4), 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.

C. The consensus matrix

In this subsection, we explain how to design a time–varying consensus matrix in a proper 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 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 a single subsystem is monitoring 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 III-D). We define the time-varying consensus-weighting matrix W^k for each (i,j)-th component for PnP purposes. The objective is to obtain the most reliable local state estimation by using only the terms available in $\mathbb{S}^k$ at the current time step. To do that, we want to use the weights that allow to minimize the thresholds (13), by weighting more the currently connected subsystems that have lower uncertainty in its measurements and in the local model. Since the amplitude of the thresholds is mainly due to the variance terms in (13), we decide to minimize those terms. This is obtained by solving the following quadratic optimization problem:

$$\begin{aligned}&\min_{W^k_{i,j}} \sum_{j\in\mathbb{S}^k}(W^k_{i,j})^2\text{Var}[\chi_{[j,k]}] \\ &\text{s. t.} \sum_{j\in\mathbb{S}^k} W^k_{i,j} = 1, \\ &\quad \left|W^k_{i,j}\right| \leq 1 \quad \forall j \in \mathbb{S}^k. \end{aligned} \tag{14}$$

We have the following result. The proof is omitted due to space constraints.

Proposition 1: The optimal weights for the minimization problem in (14) are, $\forall j \in \mathbb{S}^k$:

$$W^k_{i,j} = \frac{1}{\text{Var}[\chi_{[j,k]}](\sum_j \frac{1}{\text{Var}[\chi_{[j,k]}]})}. \tag{15}$$

At each time-step, every local fault-diagnoser receives estimates and consensus terms of variable $x_{[i,k]}$ only from the subsystems sharing it at that specific time, thus allowing PnP operations. Then, it selects and weights more the contributions affected by "smaller uncertainty".

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, for sake of compacting the notation, 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: $\epsilon_{k,E} \triangleq \text{col}\left(\epsilon_{[j,k]} : \ j \in \mathbb{S}^k_{all}\right)$, where $\mathbb{S}^k_{all}$ collects all the indices of the subsystems that can share variable k, also the ones not currently connected. Hence, the dynamics of $\epsilon_{k,E}$ can be described as:

$$\epsilon^+_{k,E} = W^k \left[\lambda \epsilon_{k,E} + \Delta f_{k,E} + w_{k,E}\right] + \varrho^+_{k,E}, \tag{16}$$

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. The proof is omitted due to space constraints.

Proposition 2: System (16), describing the dynamics of the mean of the estimation error, where the consensus matrix is row-stochastic and $0 < \lambda < 1$, is Bounded Input Bounded Output stable.

IV. Reconfiguration strategy

In the previous sections, we derived a suitable fault detection architecture for a PnP framework. We now explain how to use it during plug-in and unplugging 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. In both cases (healthy and faulty conditions), subsystems plug-in and unplugging are designed as follows.

A. Subsystem unplugging

In this paragraph, we show how to reconfigure local diagnosers 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. We need to retune fault diagnosers for children subsystems $\Sigma_{[i]}$, $i \in \mathcal{C}_j$, since they do not receive anymore the interconnection variables values from the parent subsystem $\Sigma_{[j]}$. Moreover if the unplugged subsystem was sharing variable k, its consensus contribution will not be received by neighboring subsystems sharing k. More specifically:

- In the children subsystems $i \in \mathcal{C}_j$, the components of $\tilde{\psi}_{[i]}$ and $z_{[i]}$ related to subsystem $\Sigma_{[j]}$ 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 estimates (4) and related thresholds (12).
- In the neighboring subsystems i, with $i \in \mathcal{C}_j$ or $i \in \mathcal{N}_j$, sharing some variables with $\Sigma_{[j]}$, the weights associated with $\Sigma_{[j]}$ in the consensus matrices W^k computed in (14) are set to zero and $j \notin \mathbb{S}^k$.

B. Subsystem plugging-in

The plugging-in of a subsystem into the LSS 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 FD architecture, thanks to the way the time-varying shared variables estimator is defined in (4), 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 the computation of detection estimates (4) and related thresholds (12).
- In the neighboring subsystems i, with $i \in \mathcal{C}_j$ or $i \in \mathcal{N}_j$, sharing some variables k with $\Sigma_{[j]}$, the consensus matrices W^k are computed as in (14) considering also the components received from $\Sigma_{[j]}$, that is $j \in \mathbb{S}^k$.

V. Example: Power Networks

In this section, we apply the proposed FD architecture to the Power Network System (PNS) described in [9], that is composed by five generation areas connected through tie-lines (see Fig. 2). The LFDs share some state variables[2]. In

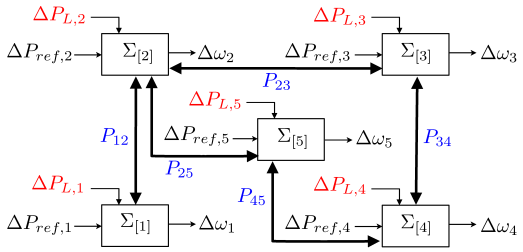

Fig. 2. Power network system.

[18], we shown how to reconfigure LFDs in a deterministic framework. In order to test the proposed stochastic PnP FD architecture, we use the scenario in Fig. 2 and same parameters and PnP model predictive controllers as in Section 7.2 in [18]. However, differently from [18], in this paper at time $t = 35$s, a fault occurs in the speed governor in area 4: in particular, its time constant increases from 0.1s to 10s, which corresponds to a slower frequency regulation, both in the primary and secondary control layers. The measurement errors $\varrho_{[i]}$, $i = 1, \ldots, 5$ and the modeling uncertainties $w_i(\cdot)$ are zero-mean white Gaussian noise processes and their variances are $\sigma^2_{w_{i,\cdot}} = 0.001$ and $\sigma^2_{\varrho_{[i,\cdot]}} = 0.001$, respectively. Since the local models of each area and their interactions are linear, we can easily compute $\text{Var}[\Delta f_{i,\cdot}]$ for each variable. For all LFDs we use $\lambda = 0.3$ and $\alpha = 2$, thus dealing with a maximum false alarm probability equal to 15%. We have performed 20 simulations using different sets of uncertainties and measurement errors.

In Fig. 4, due to the fault, in all simulations we note an increasing of the input $u_{[4]}$ (power reference ΔP_{ref_4}) and hence a diverging behavior of the frequency deviation. Therefore, the error $\epsilon_{[4,2]} = y_{[4,2]} - \hat{x}_{[4,2]}$ (red dashed lines in Fig. 3) diverges[3]: for all simulations, at time $t \geq 42$s, the LFD for area 4 is able to detect the fault. As in [18], we unplug area 4 and reconfigure local controllers and the LFDs for areas 3 and 5, that were directly connected with

[2]Area 1 and 2 share the angular deviation $\Delta\theta_1$, area 2 and 3 share $\Delta\theta_3$, area 2 and 5 share $\Delta\theta_5$ and area 3, 4 and 5 share $\Delta\theta_4$.

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

the faulty area. As shown in Fig. 4, we note the benefits of the reconfiguration, since, after a short transient, all local power references can still compensate local power loads and the fault is not propagated in the network.

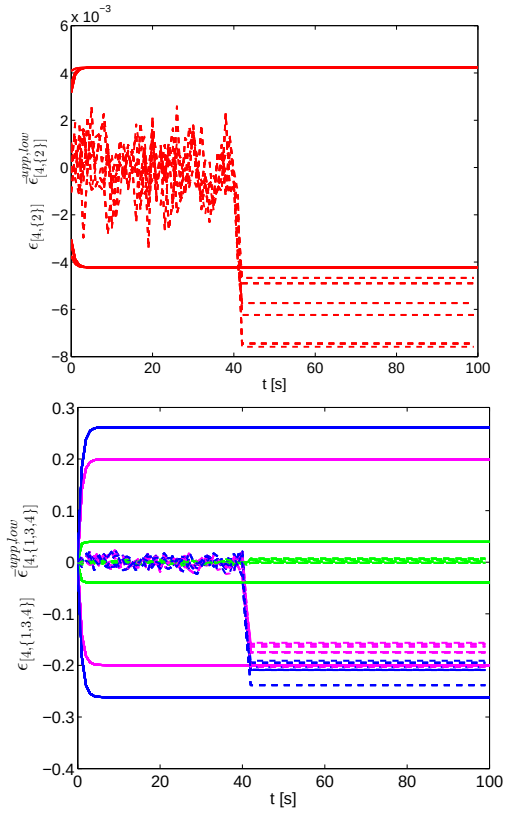

Fig. 3. Simulation: for area 4, dashed lines are the errors $\epsilon_{[4]} = y_{[4]} - \hat{x}_{[4]}$ and bold lines are the thresholds $\bar{\epsilon}_{[4]}^{upp/low}$, for faulty and non-faulty state components. Fault time $t = 35$; detection time $t = 42$.

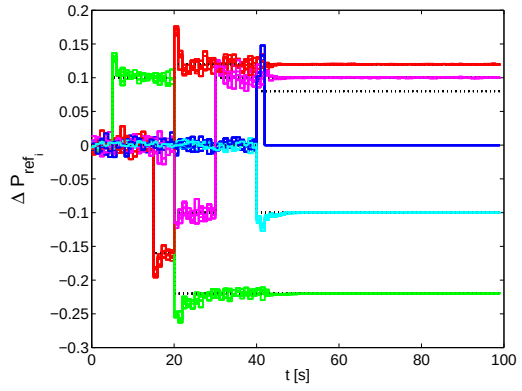

Fig. 4. Simulation: for each area, power reference set-points (bold lines), computed by PnPMPC controllers designed as in [9], and loads (dashed lines). Note that $u_{[4]} = \Delta P_{ref_4} = 0$ (blue line) after unplugging area 4.

VI. Concluding Remarks

In this paper, a stochastic distributed fault detection architecture for nonlinear LSS is designed in a PnP scenario. The proposed FD architecture is able to manage plugging-in of novel subsystems and un-plugging of existent ones, requiring reconfiguration operations only for 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 detectability analysis and to extend the PnP methodology to the case in which the state variables are not fully accessible.

References

[1] J. Lunze, *Feedback control of large scale systems*. Prentice Hall PTR, 1992.

[2] 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, 2011, pp. 175–183.

[3] 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, 2011, pp. 161–166.

[4] 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.

[5] 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*, 2009, pp. 816–821.

[6] 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.

[7] F. Boem, R. M. G. Ferrari, and T. Parisini, "Distributed fault detection and isolation of continuous-time nonlinear systems," *Europ. J. of Control*, no. 5-6, pp. 603–620, 2011.

[8] 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 Trans. on Automatic Control*, vol. 57, no. 2, pp. 275–290, 2012.

[9] 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 Conf. on Decision and Control*, Los Angeles, CA, USA, December 15-17, 2014, pp. 4977–4982.

[10] F. Boem, S. Riverso, G. Ferrari-Trecate, and T. Parisini, "A Plug-and-Play Fault Diagnosis Approach for Large-Scale Systems," in *IFAC Safeprocess Conf.*, 2015.

[11] F. Boem, R. Ferrari, T. Parisini, and M. Polycarpou, "Optimal Topology for Distributed Fault Detection of Large-scale Systems," in *IFAC Safeprocess Conf.*, 2015.

[12] J. Stoustrup, "Plug & Play Control: Control Technology towards new Challenges," in *Proc. of the 10th European Control Conference*, Budapest, Hungary, August 23-26, 2009, pp. 1668–1683.

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

[14] S. Riverso, M. Farina, and G. Ferrari-Trecate, "Plug-and-Play Decentralized Model Predictive Control for Linear Systems," *IEEE Trans. on Automatic Control*, vol. 58, no. 10, pp. 2608–2614, 2013.

[15] R. Izadi-Zamanabadi, K. Vinther, H. Mojallali, H. Rasmussen, and J. Stoustrup, "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*, 2012, pp. 701–706.

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

[17] A. Chen, H. Zhang, Q. Yang, H. Ren, M. Geng, and Y. Jiang, "Dynamic reconfiguration of intelligent electronic devices for substation automation system," in *Power System Technology, Int. Conf. on*, Oct 2014, pp. 1696–1700.

[18] S. Riverso, F. Boem, G. Ferrari-Trecate, and T. Parisini, "Plug-and-play fault diagnosis and control-reconfiguration for a class of nonlinear large-scale constrained systems," Tech. Rep., 2014. [Online]. Available: http://arxiv.org/abs/1409.5224