Plug-and-Play Fault Detection and Isolation for Large-Scale Nonlinear Systems with Stochastic Uncertainties

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

***Abstract*—This paper proposes a novel scalable model-based Fault Detection and Isolation approach for the monitoring of nonlinear Large-Scale Systems, consisting of a network of interconnected subsystems. The fault diagnosis architecture is designed to automatically manage the possible plug-in of novel subsystems and unplugging of existing ones. The reconfiguration procedure involves only local operations and communication with neighboring subsystems, thus yielding a *distributed and scalable* architecture. In particular, the proposed fault diagnosis methodology allows the unplugging of faulty subsystems in order to possibly avoid the propagation of faults in the interconnected Large-Scale System. Measurement and process uncertainties are characterized in a probabilistic way leading to the computation, at each time-step, of stochastic time-varying detection thresholds with guaranteed false-alarms probability levels. To achieve this goal, we develop a distributed state estimation scheme, using a consensus-like approach for the estimation of variables shared among more than one subsystem; the time-varying consensus weights are designed to allow plug-in and unplugging operations and to minimize the variance of the uncertainty of the fault diagnosis thresholds. Convergence results of the distributed estimation scheme are provided. A novel fault isolation method is then proposed, based on a Generalized Observer Scheme and providing guaranteed error probabilities of the fault exclusion task. Detectability and isolability conditions are provided. Simulation results on a power network model comprising 15 generation areas show the effectiveness of the proposed methodology.**

I. Introduction

In this paper, a distributed model-based Fault Detection and Isolation (FDI) approach is proposed with stochastic bounds on the measurement noise and modeling uncertainty. The presented architecture is specifically designed for large-scale interconnected systems, typically distributed and characterized by a large number of states, inputs, and constraints. Furthermore, they often have a dynamic structure that changes along the time. Reliability and resilience are therefore key requirements in Large-Scale Systems (LSSs), as their size, complexity and possible evolution over time imply an increased risk of occurrence of faults. The interest towards LSSs [1], Systems-of-Systems (SoS) [2] and Cyber-Physical Systems (CPS) [3] is steadily growing both in industry and academia. When monitoring this kind of systems, distributed or decentralized algorithms are usually necessary due to computational, communication, scalability and reliability limits (see, among others, [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], and the references therein). Moreover, an emerging requirement is the design of monitoring architectures that are robust to changes that may occur in the dynamic topology of the LSS. This is why, in this paper we model LSSs as a network of interacting subsystems and develop a scalable and distributed FDI methodology, properly designed for Plug-and-Play (PnP) scenarios. The words "Plug-and-Play" have been borrowed from computer science to refer to the possibility of adding or removing subsystems with minimal effort or human intervention. More specifically, in the context of control theory, as described in [18], the term PnP denotes a scalable design procedure where a monitoring/control unit for a subsystem can be synthesized using, at most, information from neighboring subsystems, while preserving global properties of interest (such as stability, or convergence of state estimators,...).

Differently from previous works ([8], [19], [20], [21], [22], [17]) where a deterministic approach was adopted, in this paper we consider stochastic models of noises and uncertainties. The aim is to propose a monitoring architecture which is closer to industrial applications, where deterministic bounds on the uncertainties can be difficult to obtain and can produce conservative results. In this connection, in the recent paper [23], a fault detection and isolation method is proposed with probabilistic performance, but considering a centralized architecture. In [24], stochastic uncertainties are considered for a distributed FDI architecture, but in a completely different setting (non-overlapping models, linear dynamics, output measurements only, different assumptions on disturbances which require a distributed Kalman-like filtering scheme).

It is important to note that the proposed technique is not a data-driven statistical method (see [25] for a recent survey). Instead, our approach is model-based [26] as it uses the knowledge of a local and possibly uncertain model of the system in order to compute local state estimates and related detection and isolation thresholds. An integration of data-driven and model-based approaches is proposed in [27], but in a centralized setting, while here the detection and isolation tasks are performed in a distributed way.

To the best of authors' knowledge, this is the first time that a comprehensive model-based distributed fault diagnosis architecture is designed for LSSs in a PnP scenario considering stochastic uncertainties. A preliminary version of this work has been presented in [28] considering only the fault

This work has been partially supported by the European Union's Horizon 2020 Research and Innovation Programme under grant agreement No 739551 (KIOS CoE). This work has also been conducted as part of the research project *Stability and Control of Power Networks with Energy Storage* (STABLE-NET) funded by the RCUK Energy Programme (contract no: EP/L014343/1), and the Swiss National Science Foundation under the COFLEX project (grant number 200021_169906).

F. Boem is with the Dept. of Electronic and Electrical Engineering at University College London, UK. (francesca.l.boem@gmail.com)

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

G. Ferrari-Trecate is with the Automatic Control Laboratory, cole Polytechnique Fdrale de Lausanne (EPFL), Switzerland (giancarlo.ferraritrecate@epfl.ch)

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

detection problem. Some recent results are also presented in [22], integrating distributed fault detection with MPC for nonlinear LSSs. Compared with [22], the present paper shows the following significant differences:

- the fault isolation problem is considered to determine the source/type of the detected fault. This is important because it may allow the reconfiguration of the local controllers to take into account changes in the dynamics of the faulty subsystem;
- a general class of nonlinear uncertain systems is addressed, while in [22] the analysis was limited to a class of nonlinear systems with matched control inputs;
- stochastic uncertainties with known mean and variance are assumed, while in [22] deterministic bounds were considered. This choice allows the design of detection and isolation thresholds that are less conservative (i.e. with less missed detection of faults) than the ones based on the knowledge of upper bounds on the norm of the modeling uncertainty and of the disturbances.

This last point is also the one that mainly describes the novelty with respect to [21]. In the present paper, the main contribution is to define stochastic thresholds for fault detection, able to guarantee a certain false alarms probability and allowing PnP operations.

To this aim, we define a novel time-varying consensus-like approach for the estimation of state variables shared by multiple subsystems, and thus monitored by multiple local diagnosers. Moreover, we propose a method to analytically compute the time-varying consensus weights so as to allow PnP operations and to reduce the amplitude of the thresholds by minimizing the variance of the uncertainty. Convergence of the estimator is studied and fault detectability conditions are provided. Furthermore, we design a novel distributed fault isolation scheme guaranteeing a certain probability error level, and analyze its performance in terms of error probability and fault isolability. The results on fault isolability show the conditions on the local fault function so that the monitoring agent can exclude the faults not occurring in the system.

The contributions mark a substantial difference with respect to [29] (where PnP operations, convergence of the state estimators, computation of the consensus weights, fault detectability, and distributed fault isolation were not considered), [30] (that does not consider PnP operations, consecutive false-alarms analysis, and simulation results) and [28] (where the problems of fault detectability and distributed fault isolation were not addressed).

Recently, some works have been published dealing with scalable and PnP scenarios: [31], [32], [18] analyze only the control problem; [33] designs a fault-tolerant control strategy for a centralized system; [34] presents a fault-tolerant PnP controller, but, differently from the proposed work, it considers linear systems with a centralized approach. [35] focuses on the design process of diagnostic units for interconnected systems, not dealing with a specific FDI method; finally, [36] proposes a passive fault-tolerant control scheme, not involving fault diagnosis methods, for a class of interconnected systems with PnP capabilities of the subsystems in presence of a broadcast network. Structural properties for the reconfiguration of distributed fault-tolerant control architectures are analyzed in [37], while [38] considers the problem of the reconfiguration for fault-tolerant networked control systems using a coordinator agent. [39] proposes a PnP reconfiguration of Intelligent Electronic Devices in substations using event-based Petri Net fault diagnosis methods.

The paper is organized as follows. The problem formulation is presented in Section II; in Section III, the distributed PnP FD scheme is derived, proposing the stochastic detection thresholds in Subsection III-B, the time-varying consensus weights in III-C and the analysis of the estimation convergence and detectability in III-D and V-A, respectively. The distributed fault isolation PnP architecture is presented in IV; then, in V-B, the error probabilities are analyzed, and the isolability conditions are derived in Section V-C. The PnP specific operations are then described in Section VI. Simulation results in the context of a fairly huge power system composed by 15 generation areas are presented in Section VIII. Finally, some concluding remarks are given in Section IX.

A. Notation

We use $a : b$ for the set of integers $\{a, a+1, \dots, b\}$. Given a stochastic variable x, $\mathbb{E}[x]$ denotes its expected value, while $\mathrm{Var}[x]$ its variance; the notation $x \approx (\mu_x, \sigma_x^2)$ denotes that the probability distribution of the stochastic variable x is characterized by mean value μ_x and variance σ_x^2.

II. Problem formulation

Let us consider a LSS which can be modeled as a discrete-time nonlinear system:

$$\tilde{x}^+ = \tilde{f}(\tilde{x}, \tilde{u}), \tag{1}$$

where $\tilde{x} \in \mathbb{R}^n$, $\tilde{u} \in \mathbb{R}^m$ represent the state and the control input, respectively, at time t and $\tilde{x}^+$ denotes the state at time $t+1$. The LSS can be equivalently represented by its directed structural graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ [40], where the nodes $\mathcal{V}$ represent the input and state variables, and the edges in $\mathcal{E}$ show the dynamical relationships between the variables (see Fig. 1 for an example). We assume that the system is decomposed into M (possibly) overlapping subsystems S_i. Please note that non-overlapping decompositions can be considered as well by the proposed monitoring architecture. Formally, for each $i \in \mathcal{M} = 1 : M$, we define S_i as a weakly connected subset of $\mathcal{V}$ that does not contain input nodes only. The elements of S_i form the *local state vector* x_i and the *local input vector* u_i. For each S_i, $i \in \mathcal{M}$, we introduce the set of the *interconnection variables* as $I_i \triangleq \{v \in \mathcal{V} \setminus S_i : (v, s) \in \mathcal{E}, s \in S_i \subset \mathcal{V}, v \textit{ is state variable}\}$. We denote as $\psi_{[i]}$ the vector of the interconnection variables, collecting the elements of I_i. From (1) and using the above definitions, each subsystem dynamics can be described as

$$\Sigma_{[i]} : x_{[i]}^+ = f_i(x_{[i]}, \psi_{[i]}, u_{[i]}), \tag{2}$$

where $x_{[i]} \in \mathbb{R}^{n_i}$, $u_{[i]} \in \mathbb{R}^{m_i}$, $i \in \mathcal{M}$, are the local state and input, respectively, at time t and $x_{[i]}^+$ denotes $x_{[i]}$ at time $t+1$; $f_i(\cdot) : \mathbb{R}^{n_i} \times \mathbb{R}^{p_i} \times \mathbb{R}^{m_i} \to \mathbb{R}^{n_i}$ represents possibly nonlinear local nominal dynamics. The k-th component of vector $x_{[i]}$ is specified by $x_{[i,k]}$. For monitoring purposes, each subsystem $\Sigma_{[i]}$ is equipped with a Local Fault Diagnoser (LFD). To this purpose, we consider the influence of process disturbances and measurement noise on the state dynamics and the possible

presence of faults acting on the subsystem. Therefore, with a little abuse of notation, each subsystem dynamics can be described as

$$\Sigma_{[i]} : x^+_{[i]} = f_i(x_{[i]}, \psi_{[i]}, u_{[i]}) + w_i(t) + \phi_i(x_{[i]}, \psi_{[i]}, u_{[i]}, t), \tag{3}$$

$$y_{[i]} = x_{[i]} + \varrho_{[i]}, \tag{4}$$

where $w_i(\cdot) : \mathbb{N} \to \mathbb{R}^{n_i}$ represents modeling uncertainties, considering unknown possibly nonlinear coupling among subsystems; $y_{[i]} \in \mathbb{R}^{n_i}$ are the local measurements for each subsystem $i \in \mathcal{M}$, $\varrho_{[i]} \in \mathbb{R}^{n_i}$ is the local unknown measurement error at time t, and $\phi_i(\cdot) : \mathbb{R}^{n_i} \times \mathbb{R}^{p_i} \times \mathbb{R}^{m_i} \times \mathbb{R} \to \mathbb{R}^{n_i}$ represents the fault-function, capturing deviations of the dynamics of Σ_i from the nominal healthy dynamics. ϕ_i is assumed null before the (unknown) fault time T_0.

If $S_i \cap S_j \neq 0$, then some variables of the LSS are considered both in the dynamics of $\Sigma_{[i]}$ and of $\Sigma_{[j]}$. If these are state variables, they are named *shared variables*. In particular, from (4) a variable $\tilde{x}^k$ included both in the local state vector x_i and in x_j, is measured by both subsystems $\Sigma_{[i]}$ and $\Sigma_{[j]}$.

From the description above, 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 $j \in \mathcal{C}_i$.

As a consequence, the considered decomposition of the LSS is *overlapping* [1], since some of the variables appear in more than one subsystem. Each subsystem is monitored by one LFD. *Shared variables* are monitored by more than one LFD (see Fig.1, as well as [40] and [19]). Examples of applications that can be represented in this way are: power networks, water/gas distribution networks and all facility networks that are naturally split into subnetworks.

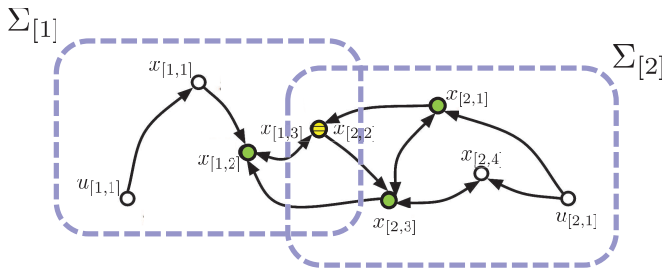


Fig. 1: An example of system structural graph [40], where the nodes of the graph represent the state and input variables, and a possible overlapping decomposition of it in two subsystems; a shared state variable is represented by a yellow circle. Shared variables are monitored and measured by more than one LFD. Interconnection variables are represented by green circles.

Remark 1: Models $\Sigma_{[i]}$, $i \in \mathcal{M}$, provide a possibly non-minimal representation of the LSS. In the sequel, (3) will be the model considered by the corresponding LFD.

In this paper, we assume that the i-th LFD has access to the noisy measurements of the interconnection variables measured by parent subsystems, i.e. the vector

$$z_{[i]} = \psi_{[i]} + \theta_{[i]}$$

where $\theta_{[i]}$ collects the involved measurement error $\varrho_{[j]}$, $j \in \mathcal{N}_i$.

For the sake of notation simplicity, we assume that the vector of the interconnection variables is large enough to embrace coupling terms due to all subsystems that will be possibly plugged-in over the system lifetime. At a certain time t, some of these variables could be null (or set to a defined value) because the corresponding parent subsystem is not connected to $\Sigma_{[i]}$ at that time. This will allow us to avoid using vectors $\psi_{[i]}$ and functions f_i and ϕ_i that change after every plug-in/out event. However, all the results in the paper can be straightforwardly adapted to this case at the price of introducing a more complex notation. We introduce the following assumptions on uncertainties and noises.

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

$$w_i(t) \approx (\mu_{w_i}(t), \sigma^2_{w_i}(t)),$$

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 $i \in \mathcal{M}$:

$$\varrho_{[i]}(t) \approx (\mu_{\varrho_{[i]}}(t), \sigma^2_{\varrho_{[i]}}(t)).$$

The values of mean and variance in Assumptions 1 and 2 are assumed to be computable from the available information on the local models, sensors and possibly on historical data. For approaches based on Monte-Carlo methods, and a discussion about their computational complexity, we refer the reader to [41].

The PnP fault diagnosis framework we are proposing, allows plug-in and unplugging operations of the interconnected subsystems, without any need to reconfigure the entire LSS: only neighboring subsystems have to be updated, continuing to guarantee global convergence properties of the estimators and operational capabilities of the diagnosers, including the guaranteed properties of the proposed thresholds. Therefore, the proposed PnP approach is scalable. More specifically, plug-in and unplugging operations, that we generally call *LSS PnP* operations, could happen due to changes of the dynamic structure of the LSS system or could be the consequence of a decision of the system operators after the detection of a fault. In fact, one of the advantages of the proposed framework is that, after fault detection, the faulty subsystem can be disconnected, when this operation is physically feasible, in order to possibly avoid the propagation of the fault in the LSS system (see Section VII). 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.

Remark 2: A prerequisite of the unplugging operation is that the corresponding subsystem can be physically disconnected from the LSS. This possibility is totally application-dependent. In the rest of the paper, we assume that any subsystem can be physically unplugged, and focus on the impact of this operation on the whole FDI architecture.

III. The PnP 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 componentwise 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 (3). The k_i-th non-shared state variable of $\Sigma_{[i]}$ can be estimated as

$$\hat{x}^+_{[i,k_i]} = \lambda(\hat{x}_{[i,k_i]} - y_{[i,k_i]}) + f_{i,k_i}(y_{[i]}, z_{[i]}, u_{[i]}), \quad (5)$$

where $z_{[i]}$ are the measurements of the interconnection variables communicated by neighboring subsystems and λ is the filter parameter, chosen in the interval $0 < \lambda < 1$ in order to guarantee convergence properties. Note that λ is a design parameter, affecting estimation convergence speed. Let now consider a shared variable $x_{[i,k_i]} = x_{[j,k_j]}$, where k_i and k_j denote the k_i-th and k_j-th components of local vectors $x_{[i]}$ and $x_{[j]}$, respectively. Thanks to overlapping, we use the redundant measurements for implementing a deterministic consensus-like approach (see [21] 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:

$$\hat{x}^+_{[i,k_i]} = \sum_{j \in \mathbb{S}^k} W^k_{i,j} \left[\lambda(\hat{x}_{[j,k_j]} - y_{[j,k_j]}) + f_{j,k_j}(y_{[j]}, z_{[j]}, u_{[j]})\right], \quad (6)$$

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 $j \in \mathbb{S}^k$.

Remark 3: It is worth noting that the proposed deterministic consensus-like approach does not require convergence to a consensus point in order to work. The goal of the consensus step is to take advantage of redundant measurements of shared variables to reduce uncertainty. This is achieved by taking a linear combination of them through the consensus matrix.

We note that (6) can model also the case of estimation of non-shared variables (5), since, in this case, $\mathbb{S}^k = \{i\}$, and $W^k_{i,i} = 1$ by definition and the summation takes into account only local information. 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

$$\epsilon^+_{[i,k]} = \sum_{j \in \mathbb{S}^k} W^k_{i,j} \left[\lambda \epsilon_{[j,k]} + \Delta f_{j,k} + w_{j,k} + \varrho^+_{[i,k]}\right], \quad (7)$$

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:

$$\epsilon^+_{[i,k]} = \lambda \epsilon_{[i,k]} + \Delta f_{i,k} + w_{i,k} + \varrho^+_{[i,k]}. \quad (8)$$

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:

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

The expected value and variance can be computed at each time step, with respect to the stochastic variable $\chi_{[i,k]}$, as

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

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

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 $\Delta f_{i,k} = f_{i,k}(y_{[i]} - \varrho_{[i]}, z_{[i]} - \theta_{[i]}, u_{[i]}) - f_{i,k}(y_{[i]}, z_{[i]}, u_{[i]})$[1].

[1]For example, we can use Monte Carlo methods [41].

In the linear case, the solution of this problem is trivial since $\Delta f_{i,k} = A_{i,k}\varrho_{[i]} + D_{i,k}\theta_{[i]}$, where $A_{i,k}$ is the k-th row of the local state equation matrix A_i, $D_{i,k}$ is the k-th row of the coupling matrix D_i representing relationships with external variables, and we know the mean and variance of $\varrho_{[i]}$ and $\theta_{[i]}$ due to Assumption 2. In the linear case it is therefore 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 $\text{Cov}[\Delta f_{i,k}, \varrho^+_{[i,k]}] = 0$ and (9) can be simplified. Moreover, we consider the following non restrictive assumption, permitting to simplify equation (9).[2]

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, (9) can be rewritten as:

$$\mathbb{E}[\chi^+_{[i,k]}] = \mathbb{E}[\Delta f_{i,k}] \tag{10}$$

$$\text{Var}[\chi^+_{[i,k]}] = \text{Var}[\Delta f_{i,k}] + \sigma^2_{w_{i,k}} + \sigma^2_{\varrho^+_{[i,k]}} + 2\text{Cov}[\Delta f_{i,k}, \varrho^+_{[i,k]}] \tag{11}$$

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 (better results can be found in case of known distribution of the residual process). For a stochastic variable X, with mean $\mu(X)$ and standard deviation $\sigma(X)$, it holds:

$$Pr\big(\mu(X) - \alpha\sigma(X) \leq X \leq \mu(X) + \alpha\sigma(X)\big) \geq 1 - 1/\alpha^2 \tag{12}$$

where $\alpha > 1$ is a tunable real positive valued scalar.

Remark 4: It is important to note that α is a design parameter which is used to determine the maximum accepted false-alarms rate. There is a trade-off between false-alarms rate reduction and detectability maximization, as it will be illustrated in Section V-A.

It follows that:

- at least 75% of the values are between $\mu - 2\sigma$ and $\mu + 2\sigma$;
- at least 88% are between $\mu - 3\sigma$ and $\mu + 3\sigma$;
- at least 93% are between $\mu - 4\sigma$ and $\mu + 4\sigma$;
- at least 96% are between $\mu - 5\sigma$ and $\mu + 5\sigma$;
- at least 99% are between $\mu - 10\sigma$ and $\mu + 10\sigma$.

Therefore, it is possible to obtain a lower and a upper stochastic thresholds for the residual signal, so that at each time t

$$\bar{\epsilon}^{\,low}_{[i]} \leq \epsilon_{[i]} \leq \bar{\epsilon}^{\,upp}_{[i]} \tag{13}$$

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

$$\begin{aligned}\bar{\epsilon}^{+\ upp/low}_{[i,k]} &= \lambda\bar{\epsilon}^{\ upp/low}_{[i,k]} + \mathbb{E}[\chi^+_{[i,k]}] \pm \alpha\left[\text{Var}[\chi^+_{[i,k]}]\right]^{\frac{1}{2}} \\ &= \lambda\bar{\epsilon}^{\ upp/low}_{[i,k]} + \mathbb{E}[\Delta f_{i,k}] \pm \alpha\Big[\text{Var}[\Delta f_{i,k}] \\ &\quad + \sigma^2_{w_{i,k}} + \sigma^2_{\varrho^+_{[i,k]}} + 2\text{Cov}[\Delta f_{i,k}, \varrho^+_{[i,k]}]\Big]^{\frac{1}{2}}. \end{aligned} \tag{14}$$

Let us now analyze the case of variables shared among more than one subsystem. 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:

$$\begin{aligned}\bar{\epsilon}^{+\ upp/low}_{[i,k]} &= \sum_{j\in\mathbb{S}^k} W^k_{i,j}\left[\lambda\bar{\epsilon}^{\ upp/low}_{[j,k]} + \mathbb{E}[\Delta f_{j,k}]\right] \\ &\quad \pm \alpha\Bigg\{\sum_{j\in\mathbb{S}^k}(W^k_{i,j})^2\Big[\text{Var}[\Delta f_{j,k}] + \sigma^2_{w_{j,k}} + \sigma^2_{\varrho^+_{[j,k]}} \\ &\quad + 2\text{Cov}[\Delta f_{j,k}, \varrho^+_{[j,k]}]\Big]\Bigg\}^{\frac{1}{2}}. \end{aligned} \tag{15}$$

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 (15) is lower than in the non-shared case in (14) 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 (in terms of misdetection compared to the case without consensus, see [21]).

Remark 5: For diagnosis purposes, the information exchange between the local diagnosers is limited. It is not necessary that each diagnoser knows the model of neighboring subsystems. In the shared case (6), it is sufficient that each subsystem $\Sigma_{[i]}$ communicates to neighboring subsystems in $\mathbb{S}^k$ only the interconnection variables and the consensus terms for estimates and thresholds, locally computed.

C. The consensus matrix

Now, we design a time–varying consensus matrix in an appropriate way in order to allow PnP operations. Consensus is applied to the shared variables, i.e. state variables representing the interconnection between two or more subsystems. For PnP capabilities, we use a square time-varying weighting matrix W^k. Hereafter we assume to fix the maximum number d_k of subsystems that can be plugged-in sharing that variable. This allows us to keep the dimension of W^k fixed and equal to d_k, irrespectively of the plug-in/out events occurring over the system lifetime. Note, however, that this assumption is made only for simplifying the notation. Moreover, d_k can be chosen arbitrarily large. So, even if the dimension of W^k is fixed, the scalability of our method is not compromised in practice.

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

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

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 find the weights that allow to minimize the thresholds (15), 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 (15), we decide to minimize those terms. This is obtained by solving the following quadratic optimization problem:

$$\begin{aligned} \min_{W^k_{i,j}} \ & \sum_{j\in\mathbb{S}^k} (W^k_{i,j})^2 \text{Var}[\chi_{[j,k]}] \\ \text{s. t.} \ & \sum_{j\in\mathbb{S}^k} W^k_{i,j} = 1, \\ & \left|W^k_{i,j}\right| \leq 1 \quad \forall j \in \mathbb{S}^k, \end{aligned} \tag{16}$$

remembering that

$$\text{Var}[\chi_{[j,k]}] = \text{Var}[\Delta f_{j,k}] + \sigma^2_{w_{j,k}} + \sigma^2_{\varrho^+_{[j,k]}} + 2\text{Cov}[\Delta f_{j,k}, \varrho^+_{[j,k]}].$$

We have the following result.

Proposition 1: The optimal weights for the minimization problem in (16) are, $\forall j \in \mathbb{S}^k$:

$$W^k_{i,j} = \frac{1}{\text{Var}[\chi_{[j,k]}](\sum_j \frac{1}{\text{Var}[\chi_{[j,k]}]})}. \tag{17}$$

Proof: The problem is convex. Following the results in [42], we formulate the Lagrangian problem:

$$\begin{aligned} L(W^k_{i,j}, \xi, \nu, \lambda) = & \sum_{j\in\mathbb{S}^k} ((W^k_{i,j})^2 \text{Var}[\chi_{[j,k]}]) \\ + \lambda(\sum_{j\in\mathbb{S}^k} W^k_{i,j} - 1) + & \sum_{j\in\mathbb{S}^k} \xi_j(-1 - W^k_{i,j}) + \sum_{j\in\mathbb{S}^k} \nu_j(W^k_{i,j} - 1), \end{aligned} \tag{18}$$

where $\lambda \in \mathbb{R}$, ξ and $\nu \in \mathbb{R}_+^{|\mathbb{S}^k|}$, being $\left|\mathbb{S}^k\right|$ the current cardinality of the time-varying set $\mathbb{S}^k$, are the dual variables. We then derive the following necessary and sufficient optimality conditions using the Karush-Kuhn-Tucker (KKT) conditions:

$$\begin{aligned} & 2\text{Var}[\chi_{[j,k]}] W^{k*}_{i,j} + \lambda^* - \xi^*_j + \nu^*_j = 0 \ , \\ & \xi^*_j(-1 - W^{k*}_{i,j}) = 0 \ , \\ & \nu^*_j(W^{k*}_{i,j} - 1) = 0 \ , \\ & \sum_{j\in\mathbb{S}^k} W^{k*}_{i,j} = 1 \ , \\ & -1 \leq W^{k*}_{i,j} \leq 1 \ , \\ & \lambda^* \in \mathbb{R}, \quad \nu^*_j \in \mathbb{R}^1_+, \quad \xi^*_j \in \mathbb{R}^1_+, \quad \forall j \in \mathbb{S}^k, \end{aligned} \tag{19}$$

denoting with a * the optimal value of the decision variables. It is possible to find the following optimal weights, $\forall j \in \mathbb{S}^k$:

$$\begin{aligned} & W^{k*}_{i,j} = \frac{1}{\text{Var}[\chi_{[j,k]}](\sum_j \frac{1}{\text{Var}[\chi_{[j,k]}]})}, \\ & \lambda^* = -2/\sum_j \frac{1}{\text{Var}[\chi_{[j,k]}]}, \\ & \nu^*_j = 0, \quad \xi^*_j = 0, \quad \forall j \in \mathbb{S}^k, \end{aligned} \tag{20}$$

by noting that they satisfy all the KKT conditions, being $\text{Var}[\chi_{[j,k]}] > 0, \quad \forall j \in \mathbb{S}^k$. ■

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 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, we introduce a vector formulation of the state error equation just for analysis purposes. Specifically, we introduce the extended estimation error vector $\epsilon_{k,E}$, which is a column vector collecting the estimation error vectors of the N_k subsystems sharing the k-th state component: $\epsilon_{k,E} \triangleq \text{col}\left(\epsilon_{[j,k]} : \ j \in \mathbb{S}^k_{all}\right)$, 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:

$$\epsilon^+_{k,E} = W^k \left[\lambda \epsilon_{k,E} + \Delta f_{k,E} + w_{k,E}\right] + \varrho^+_{k,E}, \tag{21}$$

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.

Proposition 2: The mean of the estimation error modeled in (21), where the consensus matrix is row-stochastic and $0 < \lambda < 1$, is BIBO stable.

Proof: The proof is similar to the one provided for the estimation error convergence properties in [22]. Here we consider the mean of the estimation error (21):

$$\mathbb{E}[\epsilon^+_{k,E}] = W^k \Big[\lambda \mathbb{E}[\epsilon_{k,E}] + \mathbb{E}[\Delta f_{k,E}] + \mathbb{E}[w_{k,E}]\Big] + \mathbb{E}[\varrho^+_{k,E}]. \tag{22}$$

By assumption, $\mathbb{E}[w_{k,E}] = 0$, $\mathbb{E}[\varrho^+_{k,E}] = 0$ and it is possible to compute $\mathbb{E}[\Delta f_{k,E}]$, for example with Monte Carlo simulations. We define $\Delta f_{k,E} := \mathbb{E}[\Delta f_{k,E}]$. The rest of the proof is carried out similarly as in [22]. ■

IV. PnP Distributed Fault Isolation

We now propose a novel distributed and scalable fault isolation scheme in a stochastic uncertainty framework. The fault isolation logic is based a Generalized Observer Scheme (GOS, see [43], [44]). Similarly to [19], we assume that each subsystem knows a *local fault set* $\mathcal{F}_i$, collecting all the $N_{\mathcal{F}_i}$ possible nonlinear fault functions. In [19], a more complex approach is introduced, where some approximators are designed to learn also unknown fault functions. Here we assume that the local fault functions are completely known: $\phi^l_i(x_{[i]}, \psi_{[i]}, u_{[i]}, t)$, $l \in \{1, \ldots, N_{\mathcal{F}_i}\}$.

Differently from previous works (see [19], [21]), here the uncertainties are not bounded in a deterministic way, but instead are modeled as stochastic processes. Therefore, in this paper we design novel thresholds for the distributed fault isolation task and we analyze the probability that a certain fault has occurred in the considered subsystem.

Specifically, once a fault is detected at time T_d in the i-th subsystem, each involved diagnoser activates $N_{\mathcal{F}_i}$ estimators, where each filter is sensitive to a specific fault: the generic l–th fault isolation estimator of the i–th LFD is matched to the corresponding fault function ϕ_i^l, belonging to the local fault set $\mathcal{F}_i$. Each l–th estimator provides a local state estimate $\hat{x}_{[i]}^l$ of the local state $x_{[i]}$ affected by the l-th fault. The difference between the estimate $\hat{x}_{[i]}^l$ and the measurements $y_{[i]}$ consists in the fault isolation estimation error $\epsilon_{[i]}^l \triangleq y_{[i]} - \hat{x}_{[i]}^l$, used as a residual and compared, component by component, to some properly designed probabilistic isolation thresholds $\bar{\epsilon}_{[i]}^{\ l\ upp/low} \in \mathbb{R}_+^{n_i}$. We derive a lower and a upper stochastic thresholds for the residual signal, so that, at each time t,

$$\bar{\epsilon}_{[i]}^{\ l\ low} \leq \epsilon^{l}{}_{[i]} \leq \bar{\epsilon}_{[i]}^{\ l\ upp} \tag{23}$$

with a certain probability. The thresholds can be computed at each step t for the following step $t+1$. If the residual crosses one of the two thresholds, that is

$$\epsilon_{[i,k]}^l(t) \notin \left(\bar{\epsilon}_{[i,k]}^{\ l\ low}(t), \bar{\epsilon}_{[i,k]}^{\ l\ upp}(t)\right),$$

we can exclude the occurrence of the considered l-th fault, with a certain guaranteed probability error (see Section V-B for the complete analysis). If we are able to exclude all the faults but one, then we can say that the fault is isolated with a certain probability.

A. 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

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

being $\phi_{i,k} \neq 0$. The l–th estimate for the non–shared case is designed as

$$\hat{x}_{[i,k]}^{+l} = \lambda(\hat{x}_{[i,k]}^l - y_{[i,k]}^l) + f_{i,k}(y_{[i]}, z_{[i]}, u_{[i]}) + \phi_{i,k}^l(y_{[i]}, z_{[i]}, u_{[i]}, t), \tag{24}$$

while it can be computed as follows for the general case of a fault on a variable k shared with the currently connected subsystems $\mathbb{S}^k$:

$$\hat{x}_{[i,k]}^{l+} = \sum_{j\in\mathbb{S}^k} W_{i,j}^{l\ k}\Big[\lambda(\hat{x}_{[j,k]}^l - y_{[j,k]}^l) + f_{j,k}(y_{[j]}, z_{[j]}, u_{[j]}) + \phi_{j,k}^l(y_{[j]}, z_{[j]}, u_{[j]}, t)\Big]. \tag{25}$$

The corresponding estimation error dynamic equation is

$$\epsilon_{[i,k]}^{l+} = \lambda\epsilon_{[i,k]}^l + \Delta f_{i,k} + w_{i,k} + \Delta\phi_{i,k}^l + \varrho_{[i,k]}^+,$$

and

$$\epsilon_{[i,k]}^{l+} = \sum_{j\in\mathbb{S}^k} W_{i,j}^{l\ k}\left[\lambda\epsilon_{[j,k]}^l + \Delta f_{j,k} + w_{j,k} + \Delta\phi_{j,k}^l + \varrho_{[j,k]}^+\right],$$

for the shared case, being

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

B. Fault isolation thresholds

In the matched case, that is, $\phi_{i,k} = \phi_{i,k}^l(x_{[i]}, \psi_{[i]}, u_{[i]}, t)$, we can use a similar logic as in Section III-B and define an upper and a lower isolation thresholds for each l-th residual signal, based on the Chebyshev law:

$$\begin{aligned}\bar{\epsilon}_{[i,k]}^{\ l\ +\ upp/low} &= \lambda\bar{\epsilon}_{[i,k]}^{\ l\ upp/low} + \mathbb{E}[\chi_{[i,k]}^{\phi^l+}] \pm \alpha\left[\mathrm{Var}[\chi_{[i,k]}^{\phi^l+}]\right]^{\frac{1}{2}} \\ &= \lambda\bar{\epsilon}_{[i,k]}^{\ l\ upp/low} + \mathbb{E}[\Delta f_{i,k} + \Delta\phi_{i,k}^l] \pm \alpha\left[\mathrm{Var}[\Delta f_{i,k}]\right. \\ &\quad + \mathrm{Var}[\Delta\phi_{i,k}^l] + \sigma_{w_{i,k}}^2 + \sigma_{\varrho_{[i,k]}^+}^2 + 2\mathrm{Cov}[\Delta f_{i,k}, \varrho_{[i,k]}^+] \\ &\quad \left. + 2\mathrm{Cov}[\Delta\phi_{i,k}^l, \varrho_{[i,k]}^+] + 2\mathrm{Cov}[\Delta f_{i,k}, \Delta\phi_{i,k}^l]\right]^{\frac{1}{2}},\end{aligned} \tag{26}$$

where $\chi_{[i,k]}^{\phi^l+} = \Delta f_{i,k} + w_{i,k} + \Delta\phi_{i,k}^l + \varrho_{[i,k]}^+$.

Assumption 6: 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[3] $\mathbb{E}[\Delta\phi_{i,k}^l]$, $\mathrm{Var}[\Delta\phi_{i,k}^l]$, $\mathrm{Cov}[\Delta\phi_{i,k}^l, \varrho_{[i,k]}^+]$ and $\mathrm{Cov}[\Delta f_{i,k}, \Delta\phi_{i,k}^l]$, where $\Delta\phi_{i,k}^l = \phi_{i,k}^l(y_{[i]} - \varrho_{[i]}, z_{[i]} - \theta_{[i]}, u_{[i]}) - \phi_{i,k}^l(y_{[i]}, z_{[i]}, u_{[i]})$ is stochastic because of the measurement error $\varrho_{[i]}$.

For a shared variable, we have

$$\begin{aligned}\bar{\epsilon}_{[i,k]}^{\ l\ +\ upp/low} &= \sum_{j\in\mathbb{S}^k} W_{i,j}^{l\ k}\left[\lambda\bar{\epsilon}_{[i,k]}^{\ l\ upp/low} + \mathbb{E}[\chi_{[i,k]}^{\phi^l+}]\right] \\ &\quad \pm \alpha\left\{\sum_{j\in\mathbb{S}^k}(W_{i,j}^{l\ k})^2\left[\mathrm{Var}[\chi_{[i,k]}^{\phi^l+}]\right]\right\}^{\frac{1}{2}}.\end{aligned} \tag{27}$$

As for the detection case (see (16) in Section III-C), here for fault isolation estimators we propose to define the time varying consensus matrix elements $W_{i,j}^{l\ k}$, for each l-th isolation estimator, so to minimize the variance terms of the isolation thresholds and allowing PnP operations:

$$W_{i,j}^{l\ k} = \frac{1}{\mathrm{Var}[\chi_{[j,k]}^{\phi^l}](\sum_j \frac{1}{\mathrm{Var}[\chi_{[j,k]}^{\phi^l}]})}, \quad \forall j \in \mathbb{S}^k. \tag{28}$$

The optimization problem and the proof can be derived similarly as in Section III-C.

V. Analysis of the FDI architecture

In this section we present some theoretical results about the distributed FDI scheme, introduced in Sections III and IV, which is summarized in Algorithms 1 and 2.

A. Fault detectability analysis

We derive some detectability conditions, characterizing the faults that can be detected by the proposed PnP fault detection method described in Section III, depending on the system trajectories and noises features. The detection residual in (8) can be written as:

$$\epsilon_{[i,k]}(t) = \sum_{h=0}^{t-1}\lambda^{t-1-h}(\Delta f_{i,k}(h) + w_{i,k}(h) + \varrho_{[i,k]}(h+1) + \phi_{i,k}(h)) + \lambda^t\epsilon_{[i,k]}(0), \tag{29}$$

[3]For example, Monte Carlo methods can be used.

Algorithm 1 Fault detection for the i-th LFD

Initialize the estimate $\hat{x}_{[i]}(0) = y_{[i]}(0)$
Measurements $z_{[i]}(0)$ are acquired
Compute the estimate $\hat{x}_{[i]}(1)$ (Eq. (6))
Set $t = 1$
while A fault is not detected **do**
  Measurements $y_{[i]}(t)$ are acquired
  Compute $\epsilon_{[i]}(t) = y_{[i]}(t) - \hat{x}_{[i]}(t)$
  Information ($z_{[i]}$, $\bar{\epsilon}^{upp/low}_{[j,k_s]}$, $\mathbb{E}[\chi_{[j,k_s]}]$, $\text{Var}[\chi_{[j,k_s]}]$) from neighbors is acquired, $\forall$ shared variables k_s
  Update consensus weights (Eq. (17))
  Compute the thresholds $\bar{\epsilon}^{upp/low}_{[i]}(t)$ (Eq. (14))
  Compare $\epsilon_{[i]}(t)$ with $\bar{\epsilon}^{upp/low}_{[i]}(t)$
  if $\epsilon_{[i,k]}(t) \notin \left(\bar{\epsilon}^{low}_{[i,k]}(t), \bar{\epsilon}^{upp}_{[i,k]}(t)\right)$ for at least one k **then**
    A fault is detected
    Decision: Unplugging or Fault isolation (Algorithm 2)
  end if
  Compute the novel estimate $\hat{x}_{[i]}(t+1)$ (Eq. (6))
  $t = t + 1$
end while

Algorithm 2 Fault isolation for the i-th LFD

For each $l = 1 : \mathcal{N}_{\mathcal{F}_i}$
Compute estimate $\hat{x}^l_{[i]}(t)$ (Eq. (25))
while A fault is not isolated **do**
  For each $l = 1 : \mathcal{N}_{\mathcal{F}_i}$
  Measurements $y_{[i]}(t)$ are acquired
  Compute $\epsilon^l_{[i]}(t) = y_{[i]}(t) - \hat{x}^l_{[i]}(t)$
  Information from neighbors is acquired
  Update consensus weights (Eq. (28))
  Compute the thresholds $\bar{\epsilon}^{\,l\ \ upp/low}_{[i]}(t)$ (Eq. (27))
  Compare $\epsilon^l_{[i]}(t)$ with $\bar{\epsilon}^{\,l\ \ upp/low}_{[i]}(t)$
  if $\epsilon^l_{[i,k]}(t) \notin \left(\bar{\epsilon}^{l\ \ low}_{[i,k]}(t), \bar{\epsilon}^{l\ \ upp}_{[i,k]}(t)\right)$ for at least one k **then**
    Fault ϕ^l_i is excluded
  end if
  if All faults $\phi^l_i \in \mathcal{F}_i$ excluded but p **then**
    Fault ϕ^p_i is isolated
    Decision: Unplugging or Control reconfiguration
  end if
  Compute estimate $\hat{x}^l_{[i]}(t+1)$ (Eq. (25))
  $t = t + 1$
end while

where $\phi_{i,k}(t) = \phi_{i,k}(x_{[i]}, \psi_{[i]}, u_{[i]}, t)$, with some abuse of notation. As $\phi_{i,k}(t) = 0$ for $t < T_0$, the residual can be rewritten as

$$\epsilon_{[i,k]}(t) = U_{i,k}(t) + \sum_{h=T_0}^{t-1} \lambda^{t-1-h} \phi_{i,k}(h), \tag{30}$$

where $U_{i,k}(t)$ represents the part of the residual collecting all the uncertainty terms, not including fault dynamics, i.e.

$$U_{i,k}(t) = \sum_{h=0}^{t-1} \lambda^{t-1-h} (\chi_{[i,k]}(h+1)) + \lambda^t \epsilon_{[i,k]}(0).$$

Since $\hat{x}_{[i,k]}(0) = y_{[i]}(0)$ and then $\epsilon_{[i,k]}(0) = 0$, one has

$$U_{i,k}(t) = \sum_{h=0}^{t-1} \lambda^{t-1-h} (\chi_{[i,k]}(h+1)).$$

The threshold, as by definition in (13), is designed so that

$$\bar{\epsilon}^{low}_{[i,k]}(t) \leq U_{i,k}(t) \leq \bar{\epsilon}^{upp}_{[i,k]}(t)$$

with a certain probability depending on α. A fault is detected at a certain time instant $t = T_d > T_0$ (detection time) if

$$\epsilon_{[i,k]}(t) \notin \left(\bar{\epsilon}^{low}_{[i,k]}(t), \bar{\epsilon}^{upp}_{[i,k]}(t)\right) \tag{31}$$

for at least one state component $k = 1 : n_i$. Following (30), condition (31) is equivalent to:

$$\sum_{h=T_0}^{t-1} \lambda^{t-1-h} \phi_{i,k}(h) \notin \left(\bar{\epsilon}^{low}_{[i,k]}(t) - U_{i,k}(t), \bar{\epsilon}^{upp}_{[i,k]}(t) - U_{i,k}(t)\right).$$

The uncertainty term $\chi_{[i,k]}(t)$ can be expressed as

$$\chi_{[i,k]}(t) = \mathbb{E}[\chi_{[i,k]}(t)] + \Delta\chi_{[i,k]}(t),$$

where $\Delta\chi_{[i,k]}$ is the deviation of the uncertainty from its mean, and the thresholds defined in (14) can be rewritten as

$$\bar{\epsilon}^{upp/low}_{[i,k]}(t) = \sum_{h=0}^{t-1} \lambda^{t-1-h} \Big\{ \mathbb{E}[\chi_{[i,k]}(h+1)] \pm \alpha \left[\text{Var}[\chi_{[i,k]}(h+1)]\right]^{\frac{1}{2}} \Big\} + \lambda^t \bar{\epsilon}^{upp/low}_{[i,k]}(0), \tag{32}$$

where the thresholds are initialized with $\bar{\epsilon}^{upp/low}_{[i,k]}(0) = 0$. Thanks to these observations, the detectability condition (31) becomes:

$$\sum_{h=T_0}^{t-1} \lambda^{t-1-h} \phi_{i,k}(h) \notin \left(\sum_{h=T_0}^{t-1} \lambda^{t-1-h} \big\{ -\alpha \left[\text{Var}[\chi_{[i,k]}(h+1)]\right]^{\frac{1}{2}} - \Delta\chi_{[i,k]}(h+1) \big\}, \sum_{h=T_0}^{t-1} \lambda^{t-1-h} \big\{ +\alpha \left[\text{Var}[\chi_{[i,k]}(h+1)]\right]^{\frac{1}{2}} - \Delta\chi_{[i,k]}(h+1) \big\} \right).$$

Since $\Delta\chi_{[i,k]}(t)$ is zero–mean, using Chebishev inequalities we obtain

$$-\alpha \left[\text{Var}[\chi_{[i,k]}(t)]\right]^{\frac{1}{2}} \leq \Delta\chi_{[i,k]}(t) \leq \alpha \left[\text{Var}[\chi_{[i,k]}(t)]\right]^{\frac{1}{2}}$$

with a certain probability depending on α. Therefore, the fault detection is guaranteed at time T_d with a certain false–alarms rate depending on α, when the following detectability condition is satisfied:

$$\left| \sum_{h=T_0}^{T_d-1} \lambda^{T_d-1-h} \phi_{i,k}(h) \right| > 2\alpha \sum_{h=T_0}^{T_d-1} \lambda^{T_d-1-h} \left[\text{Var}[\chi_{[i,k]}(h+1)]\right]^{\frac{1}{2}}. \tag{33}$$

In this way, we have derived a characterization in a non-closed form of a class of faults that can be detected given some uncertainty conditions.

Remark 6: It is worth noting that, given a certain fault evolution, bigger values of α make the detection of the fault more difficult.

We can then obtain a detection condition in closed form, as shown in the next proposition.

Proposition 3: Let us assume that a fault $\phi_{i,k}(x_{[i]}, \psi_{[i]}, u_{[i]}, t)$ is occurring on the k-th variable of the i-th subsystem. The fault will be detected at a certain time T_e if

$$\phi_{i,k}(x_{[i]}, \psi_{[i]}, u_{[i]}, T_e - 1) > \lambda r^{upp}_{[i,k]}(T_e - 1) + 2\alpha \text{Var}[\chi_{[i,k]}(T_e)]^{\frac{1}{2}} \quad (34)$$

or

$$\phi_{i,k}(x_{[i]}, \psi_{[i]}, u_{[i]}, T_e - 1) < \lambda r^{low}_{[i,k]}(T_e - 1) - 2\alpha \text{Var}[\chi_{[i,k]}(T_e)]^{\frac{1}{2}} \quad (35)$$

where $r^{upp/low}_{[i,k]} := \bar{\epsilon}^{\ upp/low}_{[i,k]} - \epsilon_{[i,k]}$ is the distance of the residual from the threshold.

Proof: In the case that a fault is occurring in the k-th component of the i-th subsystem, the residual dynamics is

$$\epsilon^{+}{}_{[i,k]} = \lambda \epsilon_{[i,k]} + \Delta f_{i,k} + w_{i,k} + \varrho^{+}_{[i,k]} + \phi_{i,k}(x_{[i]}, \psi_{[i]}, u_{[i]}, t)$$

In order to have that the i-th fault detection estimator detects the fault at a certain time T_e, we need that

$$\epsilon_{[i,k]}(T_e) > \bar{\epsilon}^{\ upp}_{[i,k]}(T_e)$$

or

$$\epsilon_{[i,k]}(T_e) < \bar{\epsilon}^{\ low}_{[i,k]}(T_e).$$

Using the faulty residual dynamics model, this is implied by

$$\phi_{i,k}(T_e - 1) > \bar{\epsilon}^{\ upp}_{[i,k]}(T_e) - (\lambda \epsilon_{[i,k]}(T_e - 1) + \chi_{[i,k]}(T_e))$$

or

$$\phi_{i,k}(T_e - 1) < \bar{\epsilon}^{\ low}_{[i,k]}(T_e) - (\lambda \epsilon_{[i,k]}(T_e - 1) + \chi_{[i,k]}(T_e)).$$

Since we know that $\chi_{[i,k]}$ can be bounded with a certain probability following the same reasoning used for the design of the thresholds, and using the thresholds formulation in (14), we have

$$\phi_{i,k}(T_e - 1) > \lambda \bar{\epsilon}^{\ upp}_{[i,k]}(T_e - 1) + \mathbb{E}[\chi_{[i,k]}(T_e)] + \alpha \text{Var}[\chi_{[i,k]}(T_e)]^{\frac{1}{2}} - \lambda \epsilon_{[i,k]}(T_e - 1) - (\mathbb{E}[\chi_{[i,k]}(T_e)] - \alpha \text{Var}[\chi_{[i,k]}(T_e)]^{\frac{1}{2}})$$

or

$$\phi_{i,k}(T_e - 1) < \lambda \bar{\epsilon}^{\ low}_{[i,k]}(T_e - 1) + \mathbb{E}[\chi_{[i,k]}(T_e)] - \alpha \text{Var}[\chi_{[i,k]}(T_e)]^{\frac{1}{2}} - \lambda \epsilon_{[i,k]}(T_e - 1) - (\mathbb{E}[\chi_{[i,k]}(T_e)] + \alpha \text{Var}[\chi_{[i,k]}(T_e)]^{\frac{1}{2}})$$

By the definition of $r^{upp/low}_{[i,k]}$, we obtain the thesis of the proposition. ■

B. False-exclusion error probability analysis

In this subsection we analyze the performance of the PnP Fault isolation method proposed in Section IV. In particular, we consider the false-exclusion error, that is, the probability of mistakenly excluding a fault when it is actually occurring. By the definition of the thresholds in (26), the probability that the residual $\epsilon^{l}_{[i,k]}$ lies inside the thresholds interval at a certain time t, assuming that the fault is matched, that is $\phi_{i,k} = \phi^{l}_{i,k}(x_{[i]}, \psi_{[i]}, u_{[i]}, t)$, is

$$Pr\big(\epsilon^{l}_{[i,k]}(t) \in \left(\bar{\epsilon}^{\ l\ low}_{[i,k]}(t), \bar{\epsilon}^{\ l\ upp}_{[i,k]}(t)\right) | \phi_{i,k} = \phi^{l}_{i,k}\big) \geq 1 - \frac{1}{\alpha^2}.$$

Therefore, the false-exclusion probability can be computed as follows. The probability that the residual $\epsilon^{l}_{[i,k]}$ crosses one of the related thresholds $\bar{\epsilon}^{\ l\ +\ upp/low}_{[i,k]}$, thus excluding the l-th fault in the case that the fault is matched, is lower than $\frac{1}{\alpha^2}$:

$$Pr\big(\epsilon^{l}_{[i,k]}(t) \notin \left(\bar{\epsilon}^{\ l\ low}_{[i,k]}(t), \bar{\epsilon}^{\ l\ upp}_{[i,k]}(t)\right) | \phi_{i,k} = \phi^{l}_{i,k}\big) \leq \frac{1}{\alpha^2}.$$

This is the probability of mistakenly excluding the l-th fault using thresholds $\bar{\epsilon}^{\ l\ +\ upp/low}_{[i,k]}$.

Remark 7: It is worth noting that, given a certain fault evolution, bigger values of α make false-exclusion error less likely. This comes at the cost of making fault isolation more difficult. We can therefore set α depending of the maximum error probability we can accept.

Finally, the proposed monitoring architecture can show better performance if we assume to know for each l-th fault the probability that it occurs at a certain time t: $Pr\big(\phi_{i,k} = \phi^{l}_{i,k}\big)$. The probability to have a correct fault isolation is therefore

$$\begin{aligned} &Pr\big(\epsilon^{l}_{[i,k]}(t) \in \left(\bar{\epsilon}^{\ l\ low}_{[i,k]}(t), \bar{\epsilon}^{\ l\ upp}_{[i,k]}(t)\right) \cap \phi_{i,k} = \phi^{l}_{i,k}\big) \\ &= Pr\big(\epsilon^{l}_{[i,k]}(t) \in \left(\bar{\epsilon}^{\ l\ low}_{[i,k]}(t), \bar{\epsilon}^{\ l\ upp}_{[i,k]}(t)\right) | \phi_{i,k} = \phi^{l}_{i,k}\big) \\ &\quad \cdot Pr\big(\phi_{i,k} = \phi^{l}_{i,k}\big) \geq (1 - \frac{1}{\alpha^2}) Pr\big(\phi_{i,k} = \phi^{l}_{i,k}\big), \end{aligned}$$

thanks to the theorem of compound probability.

Furthermore, it is worth noting that the distance of the residual from the thresholds gives us some useful information. Given the mean and the variance of the theoretical residual at a given time t, we can compute the probability that the current measurement is explained by the considered model. Computing

$$\alpha_l = \frac{\epsilon^{l}_{[i,k]} - (\lambda \bar{\epsilon}^{\ l\ upp/low}_{[i,k]} + \mathbb{E}[\chi^{\phi^l +}_{[i,k]}])}{\left(\text{Var}[\chi^{\phi^l +}_{[i,k]}]\right)^{\frac{1}{2}}},$$

if $\alpha_l > 1$, it follows that

$$Pr\big(\epsilon^{l}_{[i,k]}(t) \notin \left(\bar{\bar{\epsilon}}^{\ l\ low}_{[i,k]}(t), \bar{\bar{\epsilon}}^{\ l\ upp}_{[i,k]}(t)\right) | \phi_{i,k} = \phi^{l}_{i,k}\big) \leq \frac{1}{\alpha_l^2}, \quad (36)$$

where $\bar{\bar{\epsilon}}^{\ l\ low}_{[i,k]}(t)$ and $\bar{\bar{\epsilon}}^{\ l\ upp}_{[i,k]}(t)$ are the lower and upper thresholds computed using α_l. It is therefore possible to define some new thresholds using α_l and compute the error probability that we get by excluding or accepting the l-th fault.

C. Fault isolability analysis

In this subsection, we derive some conditions characterizing the faults that can be isolated by the PnP fault isolation method in Section IV. In particular, we investigate the conditions (in terms of system trajectories and noises features) allowing the proposed architecture to exclude all the possible faults but one. Let us consider the case of a non–matched fault, that is, $\phi_{i,k} = \phi^p_{i,k}(x_{[i]}, \psi_{[i]}, u_{[i]}, t)$, with $p \neq l$. Then, in the case of a non-shared variable k, the dynamics of the estimation error of the l–th fault isolation estimator for each i-th subsystem can be modeled as

$$\epsilon^{l+}_{[i,k]} \;=\; \lambda\epsilon^{l}_{[i,k]} \,+\, \Delta f_{i,k} \,+\, w_{i,k} \,+\, \Delta\phi^{p/l}_{i,k} \,+\, \varrho^{+}_{[i,k]}\,, \quad (37)$$

where

$$\Delta\phi^{p/l}_{i,k} = \phi^p_{i,k}(x_{[i]}, \psi_{[i]}, u_{[i]}, t) - \phi^l_{i,k}(y_{[i]}, z_{[i]}, u_{[i]}, t).$$

Instead, for the shared case we have

$$\epsilon^{l+}_{[i,k]} = \sum_{j\in\mathbb{S}^k} W^{l\ k}_{i,j}\left[\lambda\epsilon^{l}_{[j,k]} + \Delta f_{j,k} + w_{j,k} + \Delta\phi^{p/l}_{j,k} + \varrho^{+}_{[j,k]}\right].$$

For the sake of notational simplicity, we now continue the analysis only for non-shared variables. It is anyway simple to extend in the general case of shared state components. We have the following result:

Proposition 4: Given a fault $\phi^p_{i,k}(x_{[i]}, \psi_{[i]}, u_{[i]}, t)$ occurring on the k-th variable of the i-th subsystem, the l-th fault isolation estimator will exclude the l-th fault function, with $l \in N_{\mathcal{F}_i}$, if at a certain time T_e,

$$\begin{aligned}\phi^p_{i,k}(x_{[i]}, \psi_{[i]}, u_{[i]}, T_e - 1) > \lambda r^l_{[i,k]}(T_e - 1) + \mathbb{E}[\Delta\phi^l_{i,k}] \\ + \alpha(\text{Var}[\chi^{\phi^l}_{[i,k]}(T_e)]^{\frac{1}{2}} + \text{Var}[\chi_{[i,k]}(T_e)]^{\frac{1}{2}}) \\ + \phi^l_{i,k}(y_{[i]}, z_{[i]}, u_{[i]}, T_e - 1) \quad (38)\end{aligned}$$

or

$$\begin{aligned}\phi^p_{i,k}(x_{[i]}, \psi_{[i]}, u_{[i]}, T_e - 1) < \lambda r^l_{[i,k]}(T_e - 1) + \mathbb{E}[\Delta\phi^l_{i,k}] \\ - \alpha(\text{Var}[\chi^{\phi^l}_{[i,k]}(T_e)]^{\frac{1}{2}} + \text{Var}[\chi_{[i,k]}(T_e)]^{\frac{1}{2}}) \\ + \phi^l_{i,k}(y_{[i]}, z_{[i]}, u_{[i]}, T_e - 1) \quad (39)\end{aligned}$$

where $r^l_{[i,k]} := \bar{\epsilon}^{\,l\,+\,upp/low}_{[i,k]} - \epsilon^{l+}_{[i,k]}$ is the distance of the residual from the threshold at the previous step $T_e - 1$.

Proof: In order to have that the l-th fault isolation estimator exclude the l-th fault function at a certain time T_e, we need that

$$\epsilon^{l+}{}_{[i,k]} > \bar{\epsilon}^{\,l+\ upp}_{[i,k]}$$

or

$$\epsilon^{l+}{}_{[i,k]} < \bar{\epsilon}^{\,l+\ low}_{[i,k]}.$$

Basing on these conditions and using the expression for the residual in the non-matched case (Eq.(37)), we have

$$\Delta\phi^{p/l}_{i,k} \;>\; \bar{\epsilon}^{\,l+\ upp}_{[i,k]} \,-\, (\lambda\epsilon^{l}_{[i,k]} \,+\, \Delta f_{i,k} \,+\, w_{i,k} \,+\, \varrho^{+}_{[i,k]}).$$

$$\Delta\phi^{p/l}_{i,k} \;<\; \bar{\epsilon}^{\,l+\ low}_{[i,k]} \,-\, (\lambda\epsilon^{l}_{[i,k]} \,+\, \Delta f_{i,k} \,+\, w_{i,k} \,+\, \varrho^{+}_{[i,k]}).$$

Since we know that $\lambda\epsilon^{l}_{[i,k]} + \Delta f_{i,k} + w_{i,k} + \varrho^{+}_{[i,k]}$ can be bounded with a certain probability following the same reasoning used for the design of the thresholds, and using the isolation thresholds formulation in (26), we obtain

$$\begin{aligned}\Delta\phi^{p/l}_{i,k} > \lambda\bar{\epsilon}^{\,l\ upp}_{[i,k]} + \mathbb{E}[\Delta f_{i,k} + \Delta\phi^l_{i,k}] + \alpha\left[\text{Var}[\chi^{\phi^l+}_{[i,k]}]\right]^{\frac{1}{2}} \\ - (\lambda\epsilon^{l}_{[i,k]} + \mathbb{E}[\Delta f_{i,k}] - \alpha\left[\text{Var}[\chi^{+}_{[i,k]}]\right]^{\frac{1}{2}}).\end{aligned}$$

$$\begin{aligned}\Delta\phi^{p/l}_{i,k} < \lambda\bar{\epsilon}^{\,l\ low}_{[i,k]} + \mathbb{E}[\Delta f_{i,k} + \Delta\phi^l_{i,k}] - \alpha\left[\text{Var}[\chi^{\phi^l+}_{[i,k]}]\right]^{\frac{1}{2}} \\ - (\lambda\epsilon^{l}_{[i,k]} + \mathbb{E}[\Delta f_{i,k}] + \alpha\left[\text{Var}[\chi^{+}_{[i,k]}]\right]^{\frac{1}{2}}).\end{aligned}$$

Finally, by the definition of $\Delta\phi^{p/l}_{i,k}$ and $r^l_{[i,k]}$, we obtain the thesis of the proposition. ∎

Remark 8: It is worth noting that, given a certain fault evolution, bigger values of α make fault exclusion, and therefore fault isolation, more difficult.

VI. LSS PnP operations

In the previous sections, we derived a distributed fault detection and isolation architecture suitable for PnP operations of the interconnected subsystems. We now describe plug-in and unplugging operations. As already explained, these operations could happen due to changes over time of the dynamic structure of the LSS system or could be done on purpose after fault detection (see Section VII). 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 $\psi_{[i]}$ 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 (6) and isolation (25) estimates and related thresholds (14) and (26) .
- 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 (16) 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 (6) and (25), the plug-in is always feasible. More specifically, if a subsystem $\Sigma_{[j]}$ is added to the LSS:

- It receives from parents $i \in \mathcal{N}_j$ the probabilistic distribution of $\varrho_{[i]}$ so as to compute locally the distribution of $\theta_{[j]}$, which is needed for fulfilling Assumption 4.
- In the children subsystems $i \in \mathcal{C}_j$, the vectors $\psi_{[i]}$ and $z_{[i]}$ are expanded to include components related to subsystem $\Sigma_{[j]}$. Moreover, subsystems $i \in \mathcal{C}_j$ receive the distribution of $\varrho_{[i]}$ for computing locally the distribution of $\theta_{[i]}$.
- 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 (16) considering also the components received from $\Sigma_{[j]}$, that is $j \in \mathbb{S}^k$.

We highlight that when subsystem j is added or removed, neighboring subsystems have to modify the local FDI algorithm but the FDI units of all other subsystems are unaffected. Furthermore, by performing the updates described above, stability of state estimators (see Proposition 2) and fault detectability/isolability properties (see Section V) are preserved for the whole system. The scalability of the design procedure, accompanied by formal guarantees about global properties, allows us to qualify the architecture as PnP [18].

VII. Reconfiguration options

In this section we describe the reconfiguration actions that can be implemented thanks to the proposed PnP fault diagnosis architecture. In fact, one of the advantages of the proposed framework is that, after fault detection, the faulty subsystem can be disconnected (when this operation is physically feasible), in order to avoid or reduce the propagation of the fault in the network of the LSS system. After the detection of a fault, depending on the specific application context and criticality, two distinct actions may be feasible: i)"disconnection" of the faulty subsystem after fault detection or ii) activation of the fault isolation procedure explained in Section IV. Again, after fault isolation, two alternatives are possible depending on the additional available information: the unplugging of the faulty subsystem or fault accommodation. We do not consider the control reconfiguration problem in this paper.

A. Reduction of false-alarms and false-exclusion errors

In order to improve the reliability of the proposed decision system strategy, to reduce the number of false-alarms and false-exclusion errors and so to avoid unnecessary subsystems unpluggings or wrong decisions, we propose the following approach. In the case of fault detection, after the first alarm, we do not disconnect immediately the alleged faulty subsystem, but, depending on the desired reliability, we wait for q time steps confirming the same decision in order to reduce the probability of false alarms. We have the following theoretical result.

Proposition 5: The probability of $q > 1$ consecutive false-alarms is lower than $(\frac{1}{\alpha^2})^q$.

Proof: Since the probability of false-alarm, as explained in Section V-B, is lower than $\frac{1}{\alpha^2}$, the probability of $q > 1$ consecutive false-alarms is lower than $(\frac{1}{\alpha^2})^q$. In fact,as shown next, consecutive detection events can be considered independent since the value of the thresholds are computed at each time step independently, considering the residual as an independent stochastic variable at each time step. Let us define

$$T^l_{i,k} = \left(\bar{\epsilon}^{\,l\ low}_{[i,k]}, \bar{\epsilon}^{\,l\ upp}_{[i,k]}\right).$$

We have that

$$Pr\big(\epsilon^{l\ +}_{[i,k]} \notin T^{l+}_{i,k} | \epsilon^l_{[i,k]} \notin T^l_{i,k}\big)$$

is equivalent to

$$Pr\big(\chi^{l\ +}_{i,k} \notin \Big(\lambda(\bar{\epsilon}^{l\ low}_{[i,k]} - \epsilon^l_{[i,k]}) + \mathbb{E}[\chi^{l\ +}_{[i,k]}] - \alpha\left[\text{Var}[\chi^{l\ +}_{[i,k]}]\right]^{\frac{1}{2}},$$
$$\lambda(\bar{\epsilon}^{l\ upp}_{[i,k]} - \epsilon^l_{[i,k]}) + \mathbb{E}[\chi^{l\ +}_{[i,k]}] + \alpha\left[\text{Var}[\chi^{l\ +}_{[i,k]}]\right]^{\frac{1}{2}}\Big) |$$
$$\epsilon^l_{[i,k]} \notin \left(\bar{\epsilon}^{\,l\ low}_{[i,k]}, \bar{\epsilon}^{\,l\ upp}_{[i,k]}\right)\big). \quad (40)$$

At time $t+1$, $\bar{\epsilon}^{l\ low/upp}_{[i,k]} - \epsilon^l_{[i,k]}$ is a deterministic value. It results that

$$Pr\big(\epsilon^{l\ +}_{[i,k]} \notin T^{+}_{i,k} | \epsilon^l_{[i,k]} \notin T_{i,k}\big) = Pr\big(\epsilon^{l\ +}_{[i,k]} \notin T^{+}_{i,k}\big),$$

thus proving that consecutive detection events are independent. ■

The faulty subsystem can be disconnected after q consecutive alarms, depending on the specific risks and required reliability. In the case that after fault detection we want to go on with the fault isolation, on the other hand, we can activate the fault isolation estimators immediately after the first fault detection alarm.

Similarly to the approach proposed for fault detection, also for the fault exclusion, it is possible to implement such a procedure. The faults are not excluded at the first alarm, but we wait for $p > 1$ consecutive alarms before taking a decision.

VIII. Application Use Case: Power Networks

In this section, we apply the proposed FDI architecture to a Power Network System (PNS) composed of 15 generation areas connected through tie-lines (see Figure 2). The model of each area is described in [45], parameters and constraints are listed in Table I. For each area the local model is composed of 4 states ($x_{[i]} = (\Delta\theta_i,\ \Delta\omega i,\ \Delta P_{m_i},\ \Delta P_{v_i})$, respectively angular deviation, speed deviation, mechanical power deviation and steam valve deviation), 1 control input ($u_{[i]} = \Delta P_{ref_i}$, reference set power deviation) and 1 exogenous input ($d_{[i]} = \Delta P_{L_i}$ load power deviation). This LSS is composed of 60 state variables, 15 control inputs, 15 exogenous disturbances. In this scenario we consider that the shared variables are $\Delta\theta_i$, $i = 1:15$ meaning that if an area i is coupled with area j then $\Delta\theta_i$ is an overlapped state used by LFD-i and LFD-j. Based on this overlapping decomposition the overall FD architecture is composed of 94 states. The measurement errors $\varrho_{[i]}$, $i = 1:15$ and the modeling uncertainties $w_i(\cdot)$ are zero-mean white Gaussian noise processes and their variances are $\sigma^2_{w_{i,\cdot}} = 0.0001$ and $\sigma^2_{\varrho_{[i,\cdot]}} = 0.0001$ for noises associated with states ΔP_{m_i} and ΔP_{v_i}, and $\sigma^2_{\varrho_{[i,\cdot]}} = 0.00001$ for noises associated with states $\Delta\theta_i$ and $\Delta\omega i$, respectively.

In [22], we shown how to reconfigure LFDs in a deterministic framework. In order to test the proposed stochastic PnP FDI architecture, we use the PNS example in Fig. 2 and similar PnP Model Predictive Controllers (MPC) as in Section 7.2 in

TABLE I: Model parameters and constraints for systems $\Sigma_{[i]}$, $i \in 1:15$.

	$\Sigma_{[1]}$	$\Sigma_{[2]}$	$\Sigma_{[3]}$	$\Sigma_{[4]}$	$\Sigma_{[5]}$	$\Sigma_{[6]}$	$\Sigma_{[7]}$	$\Sigma_{[8]}$	$\Sigma_{[9]}$	$\Sigma_{[10]}$	$\Sigma_{[11]}$	$\Sigma_{[12]}$	$\Sigma_{[13]}$	$\Sigma_{[14]}$	$\Sigma_{[15]}$
H_i	12	10	8	8	10	7	7	11	8	9	10	11	12	7	9
R_i	0.05	0.0625	0.08	0.08	0.05	0.05	0.05	0.08	0.08	0.05	0.05	0.0625	0.05	0.08	0.05
D_i	0.7	0.9	0.9	0.7	0.86	0.7	0.9	0.9	0.7	0.86	0.7	0.9	0.7	0.7	0.86
T_{t_i}	0.65	0.4	0.3	0.6	0.5	0.65	0.6	0.6	0.6	0.8	0.65	0.6	0.65	0.6	0.8
T_{g_i}	0.1	0.1	0.1	0.1	0.15	0.1	0.1	0.1	0.1	0.15	0.1	0.1	0.1	0.1	0.15
$\lvert\Delta\theta_i\rvert \leq$	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
$\lvert\Delta P_{ref_i}\rvert \leq$	0.5	0.65	0.65	0.55	0.5	0.5	0.65	0.65	0.55	0.5	0.5	0.65	0.65	0.55	0.5

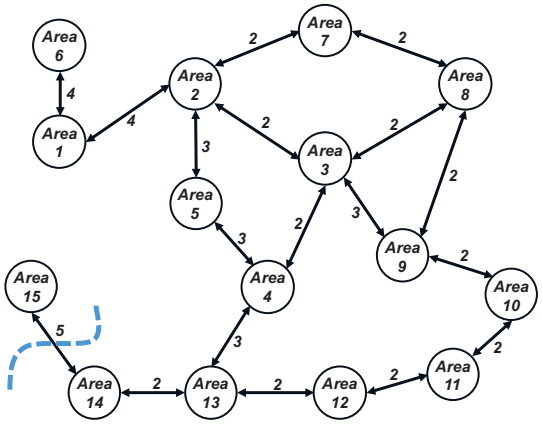


Fig. 2: Power network system composed of 15 generation areas. For each area the local model [45] is composed of 4 states $x_{[i]} = (\Delta\theta_i,\ \Delta\omega i,\ \Delta P_{m_i},\ \Delta P_{v_i})$, 1 control input $u_{[i]} = \Delta P_{ref_i}$ and 1 exogenous input $d_{[i]} = \Delta P_{L_i}$. The weights on the edges represent P_{ij}, the slope of the power angle curve at the initial operating angle between area i and area j. In Scenario 1, area 15 is initially disconnected and plugged-in at time 70s. The overlapping decomposition is not shown in this figure.

[22]. Moreover since the local models of each area and their interactions are linear, we can easily compute $\mathrm{Var}[\Delta f_{i,.}]$ for each variable. For all LFDs we use $\lambda = 0.3$ and $\alpha = 2$. Two different scenarios are considered. To simulate each scenario we used Matlab 2014a, PnPMPC toolbox [46] and CPLEX on an Intel Core TM i7 2.20GHz. To run 1 step of the detection Algorithm 1, in the worst case, the computational time is 4.1ms.

Remark 9: It is worth noting that since the proposed architecture is distributed and scalable, and both the design and on-line operations only rely on local information, models and communication, and can be parallelized, the complexity of the problem is not increasing with the total number of subsystems.

A. Scenario 1: change of the governor time constant

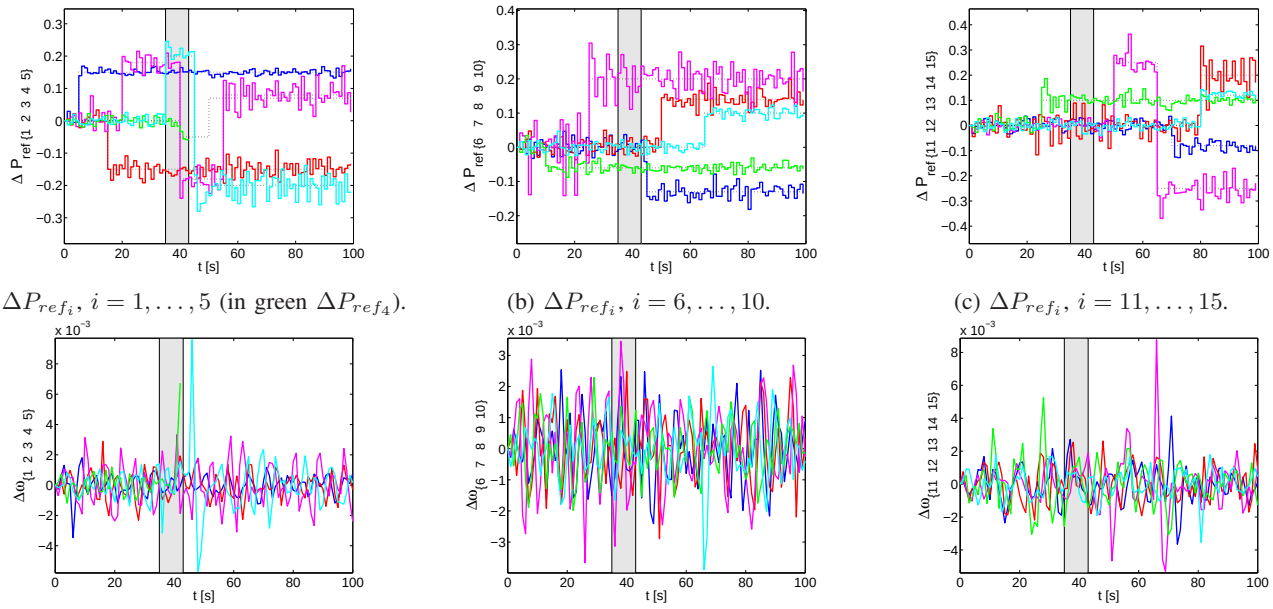
At time $t = 0$s area 15 is disconnected and working autonomously. At time $t = 35$s, a fault occurs in the speed governor in area 4: in particular, its time constant T_g increases from 0.1s to 1000s, which corresponds to a slower frequency regulation, both in the primary and secondary control layers. At time 70s area 15 is plugged in. In order to test robustness of the proposed architecture, we have performed multiple simulations using different sets of uncertainties and measurement errors. For the sake of clarity only one simulation is shown in the figures.

In Figure 3, due to the fault, we note a decrease of the input $u_{[4]}$ (power reference ΔP_{ref_4}, green line in the Figure 3a) and hence a diverging behavior of the frequency deviation. Therefore, the error $\epsilon_{[4,\{3,4\}]} = y_{[4,\{3,4\}]} - \hat{x}_{[4,\{3,4\}]}$ (blue and red dashed lines in Figure 4) crosses the threshold: for the simulation in figure, after 3 consecutively alarms, at time $t = 43$s the LFD for area 4 is finally able to detect the fault. After fault detection, similarly as in [22], we unplug area 4 and reconfigure local MPC controllers and the LFDs for areas 3, 5 and 13, that were directly connected with the faulty area. The accommodation of faults is out of the scope of the present paper and thus for area 4 we do not show the frequency deviation and power reference when the area is disconnected (see Figures 3a and 3d). As showed in Figure 3, we note the benefits of the unplugging operation, since, after a short transient, all local power references can still compensate local power loads and the fault is not propagated in the network. Finally at time 70s a plug-in operation is performed, where area 15 joins the PNS connected to area 14: retuning operations of LFDs and MPC controllers are not propagated in the network and overall stability is guaranteed (see Figures 3c and 3f specifically for area 14 in green and 15 in cyan).

In Figure 4 we also compare the proposed stochastic FD architecture and the deterministic FD architecture proposed in [22]: for this case deterministic bounds are set as upper bounds of the same measurements errors and modeling uncertainties values used for the stochastic example. Since real noises are stochastic and unbounded, it is not easy to define deterministic bounds guaranteeing the absence of false-alarms, as required in [22]. Heuristic criteria can be used, possibly resulting in conservative thresholds. Specifically, we generated 10 time series with mean and variance specified above and bounded the maximum absolute value of all samples. The chosen upper bound is 0.0427. Figure 4 shows that the proposed stochastic approach is able to detect faults when the deterministic approach can not: this guarantees that the faulty area 4 can be disconnected and faults are not propagated in the network. This shows that in general the proposed stochastic approach allows to obtain less conservative (in terms of missed detection of faults) and more easily settable thresholds, relating the thresholds with the false-alarm rate.

B. Scenario 2: sign change of the input signal

We then consider a second simulation scenario. At time $t = 45$s a different fault occurs in area 5: an attacker is able to change the sign bit of the digital input signal, so that the applied control input is $-u_{[5]}$. In few time instants at time $t = 62$s the fault is detected. After fault detection, in this case, we do not disconnect the faulty subsystem, but we proceed with fault isolation. We consider three different



(a) ΔP_{ref_i}, $i = 1, \ldots, 5$ (in green ΔP_{ref_4}). (b) ΔP_{ref_i}, $i = 6, \ldots, 10$. (c) ΔP_{ref_i}, $i = 11, \ldots, 15$.

(d) $\Delta\omega_i$, $i = 1, \ldots, 5$ (in green $\Delta\omega_4$). (e) $\Delta\omega_i$, $i = 6, \ldots, 10$. (f) $\Delta\omega_i$, $i = 11, \ldots, 15$.

Fig. 3: Scenario 1. Figures 3a, 3b and 3c: for each area, the time-behaviors of the power reference set-points (solid lines) – computed by PnPMPC controllers designed as in [22] – and of the local loads (dashed lines) are shown, respectively. Figures 3d, 3e and 3f: for each area, the time-behaviors of the frequencies are shown, respectively. Each color in the figures is associated with the index i according to the following order: blue, red, magenta, green and cyan. The grey-shaded sections highlight the time-interval between the occurrence of the fault and its detection.

attack control strategies: $-u_{[5]}$, $2u_{[5]}$ and $10u_{[5]}$. The proposed fault isolation method is able to exclude all the attacks but the correct one: $-u_{[5]}$. It is therefore possible to reconfigure the attacked controller. As it is possible to see in Figures 5, 6 and 7, after the attack starts to have effect at time $t = 45$s the local power reference in area 5 (cyan line) is not able to compensate the local power load and starts diverging. After fault detection at $t = 48$s (after 3 alarms), isolation and reconfiguration (at $t = 61$s and $t = 67$s respectively), all local power references can still compensate local power loads after a short transient and the attack effect is not propagated in the network. This is an example of CPS, where the attack, detection, isolation and reconfiguration are all performed in an automatic way in a PnP fashion.

IX. Concluding Remarks

In this paper, a model-based distributed fault detection and isolation architecture for nonlinear interconnected systems is designed in a PnP scenario. A stochastic characterization of the process disturbances and measurement noise is considered. The proposed fault diagnosis 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 large-scale systems. Fault detection and isolation probabilistic thresholds are designed, guaranteeing maximum error levels set by the designer. Fault detectability and isolability analysis are provided. Simulation results show the potential of the proposed approach in a power networks application. Future research efforts will be devoted to extend the proposed methodology to the case in which the state variables are not fully accessible and to consider real applications.

References

[1] J. Lunze, *Feedback control of large scale systems*. Upper Saddle River, NJ, USA: Prentice Hall, Systems and Control Engineering, 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. [Online]. Available: ieeecss.org/general/impact-control-technology

[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. [Online]. Available: http://ieeecss.org/general/impact-control-technology

[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.

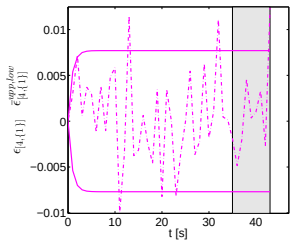
[6] S. Stankovic, N. Ilic, Z. Djurovic, M. Stankovic, and K. Johansson, "Consensus based overlapping decentralized fault detection and isolation," *Control and Fault-Tolerant Systems Conference*, pp. 570–575, 2010.

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

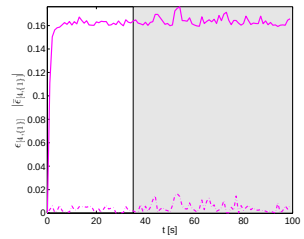
[8] F. Boem, R. M. G. Ferrari, and T. Parisini, "Distributed fault detection and isolation of continuous-time nonlinear systems," *European Journal of Control*, no. 5-6, pp. 603–620, 2011.

[9] 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.

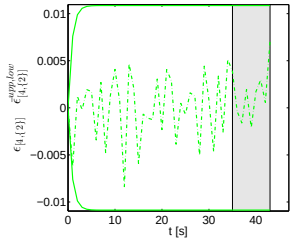
[10] M. Staroswiecki and A. M. Amani, "Fault-tolerant control of distributed systems by information pattern reconfiguration," *International Journal of Adaptive Control and Signal Processing*, 2014.



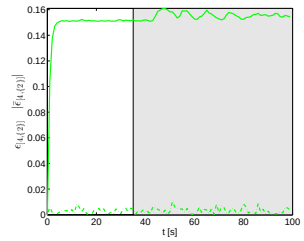
(a) $\epsilon_{[4,\{1\}]}$ (dashed line) and $\bar{\epsilon}^{upp,low}_{[4,\{1\}]}$ (solid lines) for Stochastic-based LFD.



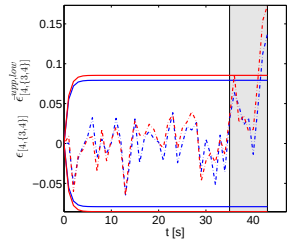
(b) $\epsilon_{[4,\{1\}]}$ (dashed line) and $\bar{\epsilon}_{[4,\{1\}]}$ (solid lines) for Deterministic-based LFD.



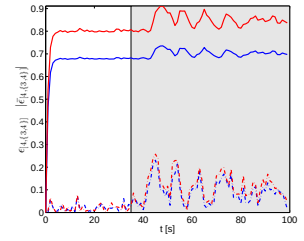
(c) $\epsilon_{[4,\{2\}]}$ (dashed line) and $\bar{\epsilon}^{upp,low}_{[4,\{2\}]}$ (solid lines) for Stochastic-based LFD.



(d) $\epsilon_{[4,\{2\}]}$ (dashed line) and $\bar{\epsilon}_{[4,\{2\}]}$ (solid lines) for Deterministic-based LFD.

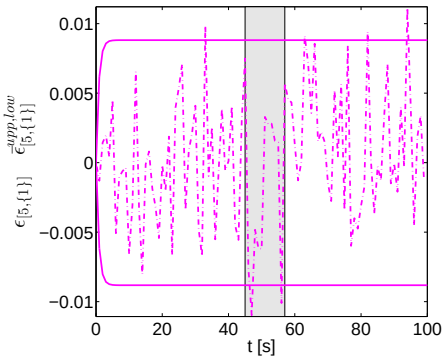


(e) $\epsilon_{[4,\{3,4\}]}$ (dashed line) and $\bar{\epsilon}^{upp,low}_{[4,\{3,4\}]}$ (solid lines) for Stochastic-based LFD.

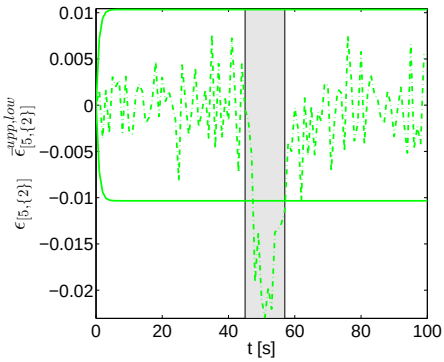


(f) $\epsilon_{[4,\{3,4\}]}$ (dashed line) and $\bar{\epsilon}_{[4,\{3,4\}]}$ (solid lines) for Deterministic-based LFD.

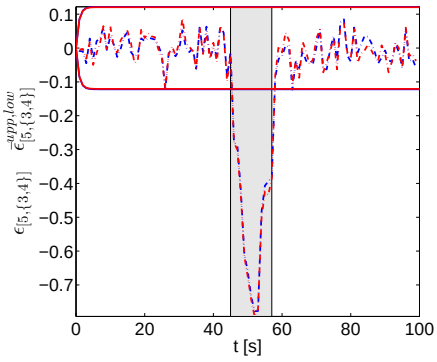
Fig. 4: Scenario 1. In Figures 4a, 4c and 4e, for area 4, for each component (in curly brackets in the subscript), dashed lines are the errors $\epsilon_{[4]} = y_{[4]} - \hat{x}_{[4]}$ and bold lines are the thresholds $\bar{\epsilon}^{upp/low}_{[4]}$ computed using the proposed stochastic FD architecture. In Figures 4b, 4d and 4f, for area 4, dashed lines are the absolute errors $\epsilon_{[4]} = |y_{[4]} - \hat{x}_{[4]}|$ and solid lines are the thresholds $\bar{\epsilon}_{[4]}$ for each component computed using the deterministic FD architecture proposed in [22]. The grey-shaded sections highlight the time-interval between the occurrence of the fault and its detection. In the deterministic case the fault is not detected. In the stochastic case, after detection, area 4 is disconnected.



(a) $\epsilon_{[5,\{1\}]}$ (dashed line) and $\bar{\epsilon}^{upp,low}_{[5,\{1\}]}$ (solid lines) for Stochastic-based LFD.



(b) $\epsilon_{[5,\{2\}]}$ (dashed line) and $\bar{\epsilon}^{upp,low}_{[5,\{2\}]}$ (solid lines) for Stochastic-based LFD.



(c) $\epsilon_{[5,\{3,4\}]}$ (dashed line) and $\bar{\epsilon}^{upp,low}_{[5,\{3,4\}]}$ (solid lines) for Stochastic-based LFD.

Fig. 5: Scenario 2. For area 5, for each component (in curly brackets in the subscript), dashed lines are the errors $\epsilon_{[5]} = y_{[5]} - \hat{x}_{[5]}$ and bold lines are the thresholds $\bar{\epsilon}^{upp/low}_{[5]}$ computed using the proposed stochastic FD architecture. The grey-shaded sections highlight the time-interval between the occurrence of the fault and its detection.

[11] V. Reppa, M. M. Polycarpou, and C. G. Panayiotou, "Decentralized isolation of multiple sensor faults in large-scale interconnected nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 60, no. 6, pp. 1582–1596, 2015.

[12] C. Keliris, M. M. Polycarpou, and T. Parisini, "Distributed fault diagnosis for process and sensor faults in a class of interconnected input–output nonlinear discrete-time systems," *International Journal of Control*, vol. 88, no. 8, pp. 1472–1489, 2015.

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

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

[15] V. Gupta and V. Puig, "Distributed fault diagnosis using minimal structurally over-determined sets: Application to a water distribution net-

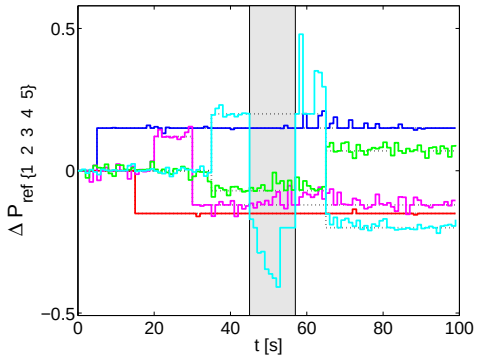


Fig. 6: Scenario 2. ΔP_{ref_i}, $i = 1, \ldots, 5$: the time-behaviors of the power reference set-points (solid lines) – computed by PnPMPC controllers designed as in [22] – and of the local loads (dashed lines) are shown, respectively. Each color in the figure is associated with the index i according to the following order: blue, red, magenta, green and cyan. The grey-shaded sections highlight the time-interval between the occurrence of the fault and the start of the reconfiguration in area 5. Note that, even in presence of the cyber-attack, in the stochastic case ΔP_{ref_5} (solid line, in cyan) allows balancing the load thanks to the reconfiguration.

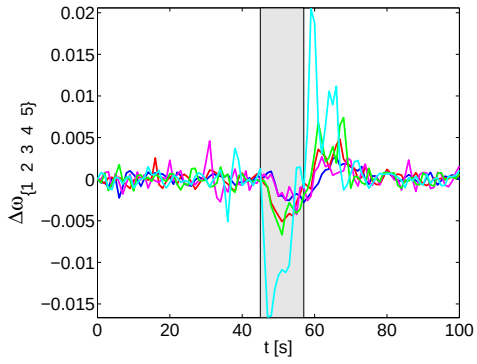


Fig. 7: Scenario 2. $\Delta\omega_{ref_i}$, $i = 1 \ldots, 5$, frequency deviations. Each color in the figure is associated with the index i according to the following order: blue, red, magenta, green and cyan. The grey-shaded sections highlight the time-interval between the occurrence of the fault and the start of the reconfiguration in area 5. Note that, even in presence of the cyber-attack, in the stochastic case $\Delta\omega_{ref_5}$ (solid line, in cyan) allows balancing the load thanks to the reconfiguration.

work," in *Proc. 3rd Conference on Control and Fault-Tolerant Systems (SysTol)*. IEEE, 2016, pp. 811–818.

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

[17] F. Boem, R. M. G. Ferrari, C. Keliris, T. Parisini, and M. M. Polycarpou, "A distributed networked approach for fault detection of large-scale systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 1, pp. 18–33, 2017.

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

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

[20] 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*, 2014, pp. 4977–4982.

[21] F. Boem, S. Riverso, G. Ferrari-Trecate, and T. Parisini, "A Plug-and-Play Fault Diagnosis Approach for Large-Scale Systems," in *Proc. 9th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, vol. 48, no. 21, 2015, pp. 601–606.

[22] S. Riverso, F. Boem, G. Ferrari-Trecate, and T. Parisini, "Plug-and-play fault detection and control-reconfiguration for a class of nonlinear large-scale constrained systems," *IEEE Transactions on Automatic Control*, vol. 61, no. 12, pp. 3963–3978, 2016.

[23] P. M. Esfahani and J. Lygeros, "A tractable fault detection and isolation approach for nonlinear systems with probabilistic performance," *IEEE Transactions on Automatic Control*, vol. 61, no. 3, pp. 633–647, 2016.

[24] F. Boem, R. Carli, M. Farina, G. Ferrari-Trecate, and T. Parisini, "Scalable monitoring of interconnected stochastic systems," in *IEEE 55th Conference on Decision and Control*. IEEE, 2016, pp. 1285–1290.

[25] S. Yin, S. X. Ding, X. Xie, and H. Luo, "A review on basic data-driven approaches for industrial process monitoring," *IEEE Transactions on Industrial Electronics*, vol. 61, no. 11, pp. 6418–6428, 2014.

[26] P. M. Frank, "Analytical and qualitative model-based fault diagnosis–a survey and some new results," *European Journal of Control*, vol. 2, no. 1, pp. 6–28, 1996.

[27] S. Yin, X. Yang, and H. R. Karimi, "Data-driven adaptive observer for fault diagnosis," *Mathematical Problems in Engineering*, vol. 2012, 2012.

[28] F. Boem, S. Riverso, G. Ferrari-Trecate, and T. Parisini, "Stochastic fault detection in a plug and play scenario," in *Proc. 54th IEEE Conference on Decision and Control*, 2015, pp. 3137–3142.

[29] F. Boem, R. Ferrari, T. Parisini, and M. Polycarpou, "Optimal Topology for Distributed Fault Detection of Large-scale Systems," in *9th IFAC Symposium on Fault Detection,Supervision and Safety of Technical Processes*, vol. 48, no. 21, 2015, pp. 60–65.

[30] F. Boem and T. Parisini, "Distributed model-based fault diagnosis with stochastic uncertainties," in *54th IEEE Conference on Decision and Control*, 2015, pp. 4474–4479.

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

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

[33] 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 *Proc. 8th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, 2012, pp. 701–706.

[34] 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.

[35] S. Bodenburg and J. Lunze, "Plug-and-play diagnosis of locally interconnected systems with limited model information," in *Proc. 3rd Conf. on Control and Fault-Tolerant Systems (SysTol)*. IEEE, 2016, pp. 735–742.

[36] H. Yang, B. Jiang, and M. Staroswiecki, "Fault tolerant control for plug-and-play interconnected nonlinear systems," *Journal of the Franklin Institute*, 2016.

[37] M. Staroswiecki and A. M. Amani, "Fault-tolerant control of distributed systems by information pattern reconfiguration," *International Journal of Adaptive Control and Signal Processing*, vol. 29, no. 6, pp. 671–684, 2015.

[38] C. Kambhampati, R. Patton, and F. Uppal, "Reconfiguration in networked control systems: Fault tolerant control and plug-and-play," *IFAC Proceedings Volumes*, vol. 39, no. 13, pp. 126–131, 2006.

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

[40] D. Šiljak, *Large-Scale Dynamic Systems: Stability and Structure*. New York: North Holland, 1978.

[41] C. P. Robert and G. Casella, "Monte carlo statistical methods," 1998.

[42] S. M. Stefanov, "Convex quadratic minimization subject to a linear constraint and box constraints," *Applied Mathematics Research eXpress*, vol. 2004, no. 1, pp. 17–42, 2004. [Online]. Available: http://amrx.oxfordjournals.org/content/2004/1/17.abstract

[43] P. M. Frank, "Fault diagnosis in dynamic systems using analytical and knowledge–based redundancy – A survey and some new results," *Automatica*, vol. 26, no. 3, pp. 459–474, 1990.

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

[45] S. Riverso, "Distributed and plug-and-play control for constrained systems," Ph.D. dissertation, Università degli Studi di Pavia, 2014. [Online]. Available: http://sisdin.unipv.it/pnpmpc/phpinclude/papers/phd_thesis_riverso.pdf
[46] S. Riverso, A. Battocchio, and G. Ferrari-Trecate, "PnPMPC: a toolbox for MatLab," 2012. [Online]. Available: http://sisdin.unipv.it/pnpmpc/pnpmpc.php

PLACE PHOTO HERE

Francesca Boem received the M.Sc. degree (cum laude) in Management Engineering in 2009 and the Ph.D. degree in Information Engineering in 2013, both from the University of Trieste, Italy. She was Post-Doc at the University of Trieste with the Machine Learning Group from 2013 to 2014. From 2014 to 2018, she was Research Associate at the Department of Electrical and Electronic Engineering, Imperial College London, with the Control and Power Research Group. Since 2015 she has been part of the team at Imperial College working on the flagship EU H2020-WIDESPREAD-TEAMING project for the development of the EU KIOS Research and Innovation Centre of Excellence, a strategic partnership between University of Cyprus and Imperial College London. In 2018 Dr. Boem has been appointed as a Lecturer in the Department of Electronic and Electrical Engineering at University College London. Her current research interests include distributed fault diagnosis and fault-tolerant control methods for large-scale networked systems and distributed estimation methods for sensor networks. Dr. Boem is member of the IFAC Technical Committee 6.4 ("Fault Detection, Supervision & Safety of Technical Processes - SAFEPROCESS") and Associate Editor for the IEEE Control System Society Conference Editorial Board and for the EUCA Conference Editorial Board.

PLACE PHOTO HERE

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

PLACE PHOTO HERE

Giancarlo Ferrari-Trecate Giancarlo Ferrari-Trecate (SM12) received the Ph.D. degree in Electronic and Computer Engineering from the Università degli Studi di Pavia in 1999. Since September 2016 he is Professor at EPFL, Lausanne, Switzerland. In spring 1998, he was a Visiting Researcher at the Neural Computing Research Group, University of Birmingham, UK. In fall 1998, he joined as a Postdoctoral Fellow the Automatic Control Laboratory, ETH, Zurich, Switzerland. He was appointed Oberassistent at ETH, in 2000. In 2002, he joined INRIA, Rocquencourt, France, as a Research Fellow. From March to October 2005, he worked at the Politecnico di Milano, Italy. From 2005 to August 2016, he has been Associate Professor at the Dipartimento di Ingegneria Industriale e dell'Informazione of the Universita degli Studi di Pavia. His research interests include decentralised and networked control, plug-and-play control, scalable control of microgrids, modelling and analysis of biochemical networks, hybrid systems and Bayesian learning. Prof. Ferrari-Trecate was awarded the "assegno di ricerca" grant from the University of Pavia in 1999 and the Researcher Mobility Grant from the Italian Ministry of Education, University and Research in 2005. He is currently a member of the IFAC Technical Committee on Control Design and he is on the editorial board of Automatica and Nonlinear Analysis: Hybrid Systems.

PLACE PHOTO HERE

Thomas Parisini received the Ph.D. degree in Electronic Engineering and Computer Science in 1993 from the University of Genoa. He was with Politecnico di Milano and since 2010 he holds the Chair of Industrial Control and is Director of Research at Imperial College London. He is a Deputy Director of the KIOS Research and Innovation Centre of Excellence, University of Cyprus. Since 2001 he is also Danieli Endowed Chair of Automation Engineering with University of Trieste. In 2009-2012 he was Deputy Rector of University of Trieste. He authored or co-authored more than 280 research papers in archival journals, book chapters, and international conference proceedings. His research interests include neural-network approximations for optimal control problems, fault diagnosis for nonlinear and distributed systems, nonlinear model predictive control systems and nonlinear estimation. He is a co-recipient of the IFAC Best Application Paper Prize of the Journal of Process Control, Elsevier, for the three-year period 2011-2013 and of the 2004 Outstanding Paper Award of the IEEE Trans. on Neural Networks. He is also a recipient of the 2007 IEEE Distinguished Member Award. In 2016 he was awarded as Principal Investigator at Imperial of the H2020 European Union flagship Teaming Project *KIOS Research and Innovation Centre of Excellence* led by University of Cyprus. In 2012 he was awarded an ABB Research Grant dealing with energy-autonomous sensor networks for self-monitoring industrial environments. Thomas Parisini currently serves as Vice-President for Publications Activities of the IEEE Control Systems Society and during 2009-2016 he was the Editor-in-Chief of the IEEE Trans. on Control Systems Technology. Since 2017, he is Editor for Control Applications of *Automatica* and since 2018 he is the Editor in Chief of the *European Journal of Control*. He is also the Chair of the IFAC Technical Committee on Fault Detection, Supervision & Safety of Technical Processes - SAFEPROCESS. He was the Chair of the IEEE Control Systems Society Conference Editorial Board and a Distinguished Lecturer of the IEEE Control Systems Society . He was an elected member of the Board of Governors of the IEEE Control Systems Society and of the European Control Association (EUCA) and a member of the board of evaluators of the 7th Framework ICT Research Program of the European Union. Thomas Parisini is currently serving as an Associate Editor of the Int. J. of Control and served as Associate Editor of the IEEE Trans. on Automatic Control, of the IEEE Trans. on Neural Networks, of Automatica, and of the Int. J. of Robust and Nonlinear Control. Among other activities, he was the Program Chair of the 2008 IEEE Conference on Decision and Control andGeneral Co-Chair of the 2013 IEEE Conference on Decision and Control. Prof. Parisini is a Fellow of the IEEE and of the IFAC.