Fault Diagnosis and Control-reconfiguration in Large-scale Systems: a Plug-and-Play Approach

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

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

I. INTRODUCTION

Nowadays, several man-made systems are characterized by a large number of states and inputs with a significant spatial distribution. This triggered an increasing interest in the study of Systems-of-Systems [1] and Cyber-Physical Systems [2]. LSSs are often modeled as the interaction of many subsystems coupled through physical variables or communication channels ([3], [4]). Often, LSS are also characterized by compositions of possibly heterogeneous and (semi)autonomous elements, namely, the component subsystems [1].

When dealing with control of LSSs, centralized control architectures can be impractical due to computational, communication and reliability limits, and an alternative is offered by the adoption of decentralized and distributed approaches. In the past, several decentralized (De) and distributed (Di) MPC schemes have been proposed for constrained LSS (see the recent survey[5], and the references cited therein).

In the typical MPC control of the LSS, the prediction of the LSS behavior is carried out through a nominal model of each subsystem and of the local interactions. However, in several applications, faults and malfunctions may occur thus possibly causing critical and unpredictable changes in

the LSS dynamics. Hence, there is a need to devise fault diagnosis schemes (see, for example, [6], [7]) providing on-line the information about the health of the system and to exploit this information to reconfigure the controller so as to guarantee some degree of fault-tolerance (see the seminal paper [?]). Model-based schemes have emerged as prominent approaches to fault diagnosis of continuous and discrete-time systems [8]. As for centralized control, centralized FD architectures suffer of scalability and robustness issues. In this context, decentralized and distributed fault-tolerant control and fault diagnosis algorithms have been proposed (see [9], [10], [11], [12], [13] as examples).

In this paper, the integration of a DiMPC scheme and a distributed FD architecture is proposed for the first time. Specifically, in the off-line control design phase we adopt a decentralized algorithm and we assume that the design of a local controller can use information at most from parents of the corresponding subsystem, i.e., subsystems that influence its dynamics. This implies that the whole model of the LSS is never used in any step of the synthesis process [3]. This approach has several advantages in terms of *scalability*: i) the communication flow at the design phase has the same topology of the coupling graph, usually sparse; ii) the local design of controllers can be parallelized; iii) local design complexity scales with the number of parent subsystems only; iv) if a subsystem joins/leaves an existing network (plug-in/unplugging operation) at most children/parents subsystems can retune their controllers and fault detectors. We refer to this kind of decentralized synthesis as PnP design, if, in addition, the plug-in and unplugging operations can be performed through a procedure for automatically assessing if the operation does not spoil stability and constraint satisfaction for the overall LSS (see [14] and [15]). Different definitions of PnP design are given in [16] and [17].

Novelties: The very significant novelty presented in the paper is the *integration of DiMPC and FD architectures in a PnP framework*. Similarly to the design of local controllers, we propose a PnP design method for local fault detection. Motivations for PnP MPC/FD are the following: i) when the behaviour of a subsystem is corrupted by a fault, we show how the subsystem can be automatically disconnected while preserving stability and constraint satisfaction at each time instant for all other subsystems; ii) when a faulty subsystem is repaired, it can be replugged-in without changing all existing local controllers and fault detectors. We highlight that, differently from [15] and [14], in this paper we design local MPC controllers for a class of nonlinear LSS. As regards FD schemes, to the best of the authors knowledge,

The research leading to these results has received funding from the European Union Seventh Framework Programme [FP7/2007-2013] under grant agreement n° 257462 HYCON2 Network of excellence.

S. Rivero and G. Ferrari-Trecate are with the Dipartimento di Ingegneria Industriale e dell'Informazione, Università degli Studi di Pavia, via Ferrata 1, 27100 Pavia, Italy ({stefano.rivero|giancarlo.ferrari}@unipv.it)

F. Boem is with the University of Trieste, Italy. (francesca.boem@phd.units.it)

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

it is the first time that a PnP FD architecture is proposed.

In real application contexts, usually, MPC controllers are designed based on the knowledge of a nominal model of the system. Therefore a FD scheme is needed to monitor the behaviour of the system. The proposed FD architecture is robust w.r.t. modelling and measurement uncertainties. To achieve this goal, it considers local models that are different from those used in local MPC controllers. In fact, another contribution of this paper is the possibility to use different decompositions and different modelling for the control and the diagnosis frameworks. This feature is useful for applications: local controllers must compute local control inputs based on local available measurements only, sometimes with high sampling rates; on the other hand local fault detectors may work at a different rate and can keep advantage of the redundancy given by the shared variables in order to improve estimation performances. It is worth noting that, to the best of the authors knowledge, this is the first contribution addressing distributed schemes for nonlinear LSS integrating model-based fault diagnosis with MPC. For a centralized approach, the interested reader is referred to [18]. Moreover, a centralized reconfiguration process, based on hybrid systems, is proposed in [19].

As application domains, we envisage the following cases as significant examples.

- *Energy efficient buildings.* A distributed control of the heating ventilation and air conditioning systems can increase energy saving, while reducing computational burden. Moreover a FD scheme is needed in order to detect if actuators are damaged and must be replaced.
- *Power network systems.* Each generation area should be locally controlled in order to stabilize the frequency of the power system and to exchange less power as possible with neighbouring areas. Distributed FD architectures allow to detect an electrical fault in an area and then to isolate it while re-dispatching the power flow.
- *Wind farms.* If the wind turbines operate in power tracking mode, a faulty wind turbine can be isolated and power production can be re-dispatched among the healthy wind turbines.
- *Cascade river reaches.* The FD architecture is needed to detect faults in hydropower plants and to redesign local controllers for the new configuration of cascade river reaches.

The paper is organized as follows. In Section II, we define the problem dealt with in the paper and we introduce the decompositions of the LSS. Then, in Section III, we design the nonlinear DiMPC architecture, while in Section IV we derive the PnP distributed FD scheme. The fault detectability analysis is presented in Section V. The re-configuration process after unplugging and the plugging-in process are described in Sections VI and VI-B, respectively. In Section VII, a simple low-order preliminary simulation analysis is reported to show the potentialities of the proposed approach. Finally, some concluding remarks are given in Section VIII.

Fig. 1. The two different decompositions of the LSS structural graph: the non-overlapping subsystems of the control architecture in blue, the overlapping subsystems of the fault diagnosis framework in red. The small circles represent the state and input variables; the yellow one are the shared state variables.

II. SYSTEM DEFINITION

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

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

where $x_{[i]} \in \mathbb{R}^{n_i}$, $u_{[i]} \in \mathbb{R}^{m_i}$, $i \in \mathcal{M} = \{1, \dots, M\}$, are the local state and input, respectively, at time t and $x_{[i]}^+$ stands for $x_{[i]}$ at time $t + 1$. The k -th component of vector $x_{[i]}$ is specified by $x_{[i,k]}$ (similarly for input and output variables). The vector of interconnection variables $\psi_{[i]} \in \mathbb{R}^{p_i}$ collects components of the states $\{x_{[j]}\}_{j \in \mathcal{N}_i}$, where $\mathcal{N}_i$ is the set of parents of subsystem i defined as $\mathcal{N}_i = \{j \in \mathcal{M} : \frac{\partial x_{[i]}^+}{\partial x_{[j]}} \neq \mathbf{0}_{n_i} \text{ or } \frac{\partial x_{[i]}^+}{\partial u_{[j]}} \neq \mathbf{0}_{n_i}, i \neq j\}$. We also define $\mathcal{F}_i = \{k : i \in \mathcal{N}_k\}$ as the set of children of $\Sigma_{[i]}$. $A_{ii} \in \mathbb{R}^{n_i \times n_i}$, $B_i \in \mathbb{R}^{n_i \times m_i}$, $i \in \mathcal{M}$ and $g_i(\cdot) : \mathbb{R}^{n_i} \times \mathbb{R}^{p_i} \rightarrow \mathbb{R}$ represent linear and possibly non-linear nominal dynamics, respectively. Nonlinear dynamics can also include known relationships with neighbouring subsystems by means of the interconnection variables. We assume that the state vector is completely measurable. On the other hand, the distributed FD architecture monitors a state vector $\tilde{x}_{[i]}$ which is extended with respect to the controlled one, since in addition to $x_{[i]}$ it considers some variables $x_{[i,s]}$ that it shares with parents subsystems. We call *shared* variables of subsystem i both the variables belonging to parents subsystems monitored also by subsystem i , and the variables of subsystem i monitored by children subsystems. Moreover, the FD architecture takes into account that the nominal model may be uncertain. Therefore, the system dynamics considered by the i -th local

diagnoser can be described as:

$$\tilde{\Sigma}_{[i]} : \quad \tilde{x}_{[i]}^+ = \tilde{A}_{ii}\tilde{x}_{[i]} + \tilde{B}_i[\tilde{g}_i(\tilde{x}_{[i]}, \tilde{\psi}_{[i]})u_{[i]} \quad (2a)$$

$$+ \Phi_i(\tilde{x}_{[i]}, \tilde{\psi}_{[i]}, u_{[i]}, t) + w_i(\tilde{\psi}_{[i]}) \quad (2b)$$

$$y_{[i]} = \tilde{x}_{[i]} + \varrho_{[i]} \quad (2c)$$

where $\tilde{x}_{[i]} \in \mathbb{R}^{\tilde{n}_i}$, $u_{[i]} \in \mathbb{R}^{m_i}$, $y_{[i]} \in \mathbb{R}^{\tilde{n}_i}$ and $\varrho_{[i]} \in \mathbb{R}^{\tilde{n}_i}$, $i \in \mathcal{M} = \{1 \dots, M\}$, are the local state, input, output and unknown measurement error, respectively, for diagnosis purposes. The vector of interconnection variables $\tilde{\psi}_{[i]} \in \mathbb{R}^{\tilde{p}_i}$ collects the variables $\psi_{[i]}$ except the variables shared with the i -th subsystem. As a consequence the state matrix A_{ii} is extended to $\tilde{A}_{ii}$ to describe the linear dynamics of the state $\tilde{x}_{[i]}$, and similarly B_i and function g_i , $i \in \mathcal{M}$. Instead, $w_i(\cdot) : \mathbb{R}^{\tilde{p}_i} \rightarrow \mathbb{R}^{\tilde{n}_i}$ represents the unknown possibly non-linear coupling among subsystems and includes also modelling uncertainties, while $\Phi_i(\cdot) : \mathbb{R}^{\tilde{n}_i} \times \mathbb{R}^{\tilde{p}_i} \times \mathbb{R}^{m_i} \times \mathbb{R} \rightarrow \mathbb{R}^{\tilde{n}_i}$ represents the fault-function, capturing deviations of the dynamics of $\tilde{\Sigma}_i$ from the nominal healthy dynamics. We consider the following assumptions.

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

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

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

where $\mathbb{X}_i$, $\mathbb{U}_i$ and $\mathbb{O}_i$ are compact, convex and contain the origin in their nonempty interior. Constraints (3) also induce suitable constraints on $\tilde{\Sigma}_{[i]}$, $i \in \mathcal{M}$.

(III) Functions $w_i(\cdot)$ are bounded for all $i \in \mathcal{M}$, i.e. $w_i(\Psi_i) \subseteq \mathbb{W}_i \subset \mathbb{R}^{\tilde{n}_i}$, where $\tilde{\psi}_{[i]} \in \Psi_i$. Moreover if $\Psi_i \subset \tilde{\Psi}_i$ then $\mathbb{W}_i \subset \tilde{\mathbb{W}}_i = w_i(\tilde{\Psi}_i)^1$.

(IV) The measurement error $\varrho_{[i]}$ can be bounded for all $i \in \mathcal{M}$ at each time t so that $|\varrho_{[i]}| \leq \bar{\varrho}_{[i]}$ component-wise.

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

Definition 1 ([3]): A decomposition of the LSS into subsystems $\Sigma_{[i]}$, $i \in \mathcal{M}$ is said *non-overlapping* if no state variables are shared between subsystems, i.e. $x_{[i,k]} \neq x_{[j,l]}$, $\forall i \in \mathcal{M}$, $j \in \mathcal{N}_i$, $k = 1 : n_i$ and $l = 1 : n_j$. Otherwise, the decomposition is termed *overlapping*.

In the following, $\mathbb{S}^k$ will denote the set of subsystems sharing a given state variable k of the LSS.

III. NONLINEAR TUBE-BASED DISTRIBUTED MPC

In this section, we illustrate the proposed distributed tube-based MPC controller. Concerning the control architecture, we consider a non-overlapping decomposition of the LSS. Note that, in order to design the local controllers, the nominal model in (1) is considered. In the spirit of tube-based MPC, as in [21], we define a nominal model for each subsystem as

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

¹Notice that the second part of this Assumption is needed in order to guarantee that the approximation error of the method does not depend on the sets Ψ_i . For more details, the reader is referred to [20].

where $v_{[i]}$ is the input. As in [21] our goal is to relate inputs $v_{[i]}$ in (4) to $u_{[i]}$ in (1) and compute sets $\mathbb{Z}_i \subseteq \mathbb{R}^{n_i}$, $i \in \mathcal{M}$ such that

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

In other terms, as in [14] and [15], we want to confine $x_{[i]}(t)$ in a tube around $\hat{x}_{[i]}(t)$ of section $\mathbb{Z}_i$. Therefore, if $x_{[i]} \in \mathbb{Z}_i$ there exists $u_{[i]} = \bar{\kappa}_i(x_{[i]}) : \mathbb{Z}_i \rightarrow \mathbb{U}_{z_i}$ such that $x_{[i]}^+ \in \mathbb{Z}_i$, $\forall x_{[j]} \in \mathbb{X}_j$, $j \neq i$. Moreover if $x_{[i]} \in \hat{x}_{[i]} \oplus \mathbb{Z}_i$ and the controller

$$\mathcal{C}_{[i]} : \quad u_{[i]} = g_i(x_{[i]}, \psi_{[i]})^{-1}[v_{[i]} + \bar{\kappa}_i(x_{[i]} - \bar{x}_{[i]})] \quad (5)$$

is used, then, for all $v_{[i]}$, we have $x_{[i]}^+ \in \hat{x}_{[i]}^+ \oplus \mathbb{Z}_i$. Controller $\mathcal{C}_{[i]}$ is based on the well-known idea of “cancelling” the nonlinearities in the state equations. This is possible because in (1) the nonlinear terms are “matched”, i.e. they can be directly modified through the control input $u_{[i]}$. We also note that controller $\mathcal{C}_{[i]}$ is *distributed* since it depends on the state variables of parent subsystems.

Following [21], the next goal is to compute tightened constraints $\hat{\mathbb{X}}_i \subseteq \mathbb{X}_i$ and $\mathbb{V}_i \subseteq \mathbb{U}_i$ in order to guarantee that $\hat{x}_{[i]} \in \hat{\mathbb{X}}_i$ and $v_{[i]} \in \mathbb{V}_i$, at all time instants. Tightened state constraints must satisfy the following inclusions

$$\hat{\mathbb{X}}_i \oplus \mathbb{Z}_i \subseteq \mathbb{X}_i \quad (6a)$$

$$\mathbb{G}_i(\mathbb{V}_i \oplus \mathbb{U}_{z_i}) \subseteq \mathbb{U}_i \quad (6b)$$

where $\mathbb{G}_i = g_i(\mathbb{X}_i, \Psi_i)^{-1}$. Obviously, as in nonlinear tube-based MPC theory, the most difficult step is the evaluation of sets $\mathbb{G}_i$. Estimates of these sets can be obtained using methods of reachability analysis for nonlinear systems, as those discussed in [20] and [22]. Note also that (6a) allows to satisfy state constraints irrespectively of the errors on state measurements. Therefore, since we want to stabilize the nominal subsystems (4) and to guarantee satisfaction of tightened state constraints, we need to solve online the following *local* MPC problem $\mathbb{P}_i^N(x_{[i]}(t))$:

$$\min_{\substack{\hat{x}_{[i]}(0) \\ v_{[i]}(0:N_i-1)}} \sum_{k=0}^{N_i-1} \ell_i(\hat{x}_{[i]}(k), v_{[i]}(k)) + V_{f_i}(\hat{x}_{[i]}(N_i)) \quad (7a)$$

$$x_{[i]}(t) - \hat{x}_{[i]}(0) \in \mathbb{Z}_i \quad (7b)$$

$$\hat{x}_{[i]}(k+1) = A_{ii}\hat{x}_{[i]}(k) + B_iv_{[i]}(k) \quad k \in 0 : N_i - 1 \quad (7c)$$

$$\hat{x}_{[i]}(k) \in \hat{\mathbb{X}}_i, \quad v_{[i]}(k) \in \mathbb{V}_i \quad k \in 0 : N_i - 1 \quad (7d)$$

$$\hat{x}_{[i]}(N_i) \in \hat{\mathbb{X}}_{f_i} \quad (7e)$$

In (7), $N_i > 0$ is the control horizon, $\ell_i(\cdot) : \mathbb{R}^{n_i \times m_i} \rightarrow \mathbb{R}_{0+}$ is the stage cost, $V_{f_i}(\cdot) : \mathbb{R}^{n_i} \rightarrow \mathbb{R}_{0+}$ is the final cost and $\hat{\mathbb{X}}$ is the terminal set. Furthermore, following [21], in (5) we set

$$v_{[i]}(t) = v_{[i]}(0|t), \quad \bar{x}_{[i]}(t) = \hat{x}_{[i]}(0|t) \quad (8)$$

where $v_{[i]}(0|t)$ and $\hat{x}_{[i]}(0|t)$ are optimal values of the variables $v_{[i]}(0)$ and $\hat{x}_{[i]}(0)$ in the MPC- i problem (7). Note that in (8) we defined the variable $\bar{x}_{[i]}$ depending on the nominal state $\hat{x}_{[i]}$, i.e. the state of the dynamics of the subsystem $\Sigma_{[i]}$

without coupling terms. Note also that the re-definition of $\tilde{x}_{[i]}$ as in (8) is at the core of the tube-MPC scheme proposed in [23] and [21]. Function $\bar{\kappa}_i(\cdot)$ in (5), sets $\mathbb{Z}_i, \mathbb{U}_{z_i}, \hat{\mathbb{X}}_i, \mathbb{V}_i, \hat{\mathbb{X}}_{f_i}$, functions $\ell_i(\cdot)$ and $V_{f_i}(\cdot)$ are computed through Algorithm 1.

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

Input: $A_{ii}, B_i, \mathbb{X}_i, \mathbb{U}_i, g_i(\cdot), w_i(\cdot), \mathcal{N}_i$

Output: controller $\mathcal{C}_{[i]}$

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

$$\mathbb{W}_i = w_i(\Psi_i) \quad (9)$$

and choose $\bar{\mathbb{Z}}_i^0$ such that $\mathbb{X}_i \supseteq \bar{\mathbb{Z}}_i^0 \supseteq \mathbb{W}_i \oplus B_{\omega_i}(0)$ for a sufficiently small $\omega_i > 0$. If $\bar{\mathbb{Z}}_i^0$ does not exist, then **stop** (the controller $\tilde{\mathcal{C}}_{[i]}$ cannot be designed)

- (IV) Check the LP feasibility condition in Step (2) of Algorithm 1 in [15]. If it is not verified, then **stop** (the controller $\tilde{\mathcal{C}}_{[i]}$ cannot be designed)
 - (V) Execute Steps (3)-(6) of Algorithm 1 in [15]. They provide the MPC- i problem and the function $\bar{\kappa}_i(\cdot)$ defined as in (25) in [15]
-

Steps (IV) and (V) of Algorithm 1, that provide constraints in (6), are the most computationally expensive because involve Minkowski sums and differences of polytopic sets. The interested reader is referred to Sections 3.1-3.3 in [15], where we show how to avoid burdensome computations exploiting results from [24] and how to compute a suitable function $\bar{\kappa}_i$ in (5) through LP.

Next we give the main results on stability and constraints satisfaction for the network of subsystems controlled by distributed controllers $\mathcal{C}_{[i]}$. First, we give the following

Definition 2: The feasibility region for the MPC- i problem is

$$\mathbb{X}_i^N = \{s_{[i]} \in \mathbb{X}_i : (7) \text{ is feasible for } x_{[i]}(t) = s_{[i]}\}.$$

The next theorem summarizes the key properties of the closed-loop system (the proof uses similar results as in Chapter 6 and 7 of [25] and is not reported here for the sake of brevity).

Theorem 1: Let Assumption 1 to hold. Assume state-feedback controllers $\mathcal{C}_{[i]}$ are computed using Algorithm 1, $\mathbb{X}^N = \prod_{i \in \mathcal{M}} \mathbb{X}_i^N$ and $\mathbf{x}(t) = (x_{[1]}, \dots, x_{[M]})$. Then, the origin of the closed-loop system is asymptotically stable, i.e. $x_{[i]} \rightarrow \mathbf{0}_{n_i}, i \in \mathcal{M}$; moreover, $\mathbb{X}^N$ is a region of attraction and $\mathbf{x}(0) \in \mathbb{X}^N$ guarantees state and input constraints are fulfilled at all time instants.

Remark 1: Notice that Algorithm 1 provides a decentralized procedure for designing distributed PnP regulators and that it can be executed in parallel for all subsystems. Therefore, as shown in [14], [15] and as we will see jointly with the FD architecture presented in Sections VI and VI-B, plug-in or unplugging operations involve only the update of

a limited number of controllers. Differently from [15] and [14] (where only linear time-invariant subsystems have been considered), we highlight that the proposed regulator allows to control subsystems described by matched nonlinearities and nonlinear couplings with parents.

IV. THE FAULT DETECTION ARCHITECTURE

A. The Fault Detection Estimator

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

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

where the filter parameter is chosen in the interval $0 < \lambda < 1$ in order to guarantee convergence properties, $z_{[i]} = \tilde{\psi}_{[i]} + \theta_{[i]}$ is the vector of measured interconnection variables available for diagnosis, $\theta_{[i]}$ collects the involved $\varrho_{[j]}, j \in \mathcal{N}_i, \tilde{A}_{ii,k}$ and $\tilde{B}_{i,k}$ are the k -th row of matrices $\tilde{A}_{ii}$ and $\tilde{B}_i$, respectively. Using shared variable $\tilde{x}_{[i,k_i]} = \tilde{x}_{[j,k_j]}$, where k_i and k_j are the k_i -th and k_j -th components of vectors $\tilde{x}_{[i]}$ and $\tilde{x}_{[j]}$, respectively, we can take advantage of the redundancy by using a kind of deterministic consensus protocol (see [13], [12]). The estimates of shared variables are provided by

$$\begin{aligned} \hat{\tilde{x}}_{[i,k_i]}^+ &= \lambda(\hat{\tilde{x}}_{[i,k_i]} - y_{[i,k_i]}) + \sum_{j \in \mathbb{S}^k} W_{i,j}^k \left[\hat{\tilde{x}}_{[j,k_j]} - \hat{\tilde{x}}_{[i,k_i]} \right. \\ &\quad \left. + \tilde{A}_{jj,k_j}y_{[j]} + \tilde{B}_{j,k_j}[\tilde{g}_j(y_{[j]}, z_{[j]})u_{[j]}] \right] \end{aligned} \quad (10)$$

where $W_{i,j}^k$ are the components of a row-stochastic matrix W_k , which will be defined in Subsection IV-C. By now, notice that W_k collects the consensus weights used by $\tilde{\Sigma}_{[i]}$ to weight the terms communicated by $\tilde{\Sigma}_{[j]}$, with $j \in \mathbb{S}^k$. We also note that (10) holds also for the case of non-shared variables, since, in this case, $\mathbb{S}^k = \{i\}$, and $W_{i,i}^k = 1$ by definition. In the following, for the sake of simplicity, we omit the subscript of the shared component index k : $\tilde{x}_{[i,k]} = \tilde{x}_{[i,k_i]}$.

B. The detection threshold

According to the usual estimation-based FD approach, the estimation error $\epsilon_{[i]} \triangleq y_{[i]} - \hat{\tilde{x}}_{[i]}$ is compared component-wise with a suitable time-varying detection threshold $\bar{\epsilon}_{[i]} \in \mathbb{R}_{+}^{\tilde{n}_i}$, hence obtaining a local fault decision classifying the status of the subsystem either as healthy or faulty. If the residual crosses the threshold, we can conclude that a fault has occurred. The condition $|\epsilon_{[i,k]}(t)| \leq \bar{\epsilon}_{[i,k]}(t), \forall k = 1 : \tilde{n}_i$ is a necessary (but generally not sufficient) condition for the hypothesis $\mathcal{H}_i$: “Subsystem $\tilde{\Sigma}_{[i]}$ is healthy”. If the condition is violated at some time instant, then the hypothesis $\mathcal{H}_i$ is falsified. In order to define an appropriate threshold for FD, we analyze the dynamics of the local diagnoser estimation error when the subsystem is healthy. Defining W^k such that $\sum_{j \in \mathbb{S}^k} W_{i,j}^k = 1$ and since $\forall i, j \in \mathbb{S}^k$ it holds

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

therefore, the k -th state estimation error can be computed as

$$\epsilon_{[i,k]}^+ = \sum_{j \in \mathbb{S}^k} W_{i,j}^k \left[\lambda \epsilon_{[j,k]}(t) - \tilde{A}_{jj,k} \varrho_{[j]} + w_{j,k}(\tilde{\psi}_{[j]}) + \tilde{B}_{j,k} \Delta g_{j,k} u_{[j]} - \lambda \varrho_{[j,k]} \right] + \lambda \varrho_{[i,k]} + \varrho_{[i,k]}^+,$$

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

As in [13], using the triangular inequality, we can bound the estimation error, guaranteeing no false-positive alarms. By taking the absolute value of $\epsilon_{[i,k]}^+$ component-wise, we get

$$|\epsilon_{[i,k]}^+| \leq \sum_{j \in \mathbb{S}^k} W_{i,j}^k \left[\lambda |\epsilon_{[j,k]}(t)| + |\tilde{A}_{jj,k} \varrho_{[j]}| + \lambda |\varrho_{[j,k]}| + |\tilde{B}_{j,k} \Delta g_{j,k} u_{[j]}| + |w_{j,k}(\tilde{\psi}_{[j]})| \right] + \lambda |\varrho_{[i,k]}| + |\varrho_{[i,k]}^+|.$$

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

$$\bar{\epsilon}_{[i,k]}^+ = \sum_{j \in \mathbb{S}^k} W_{i,j}^k \left[\lambda \bar{\epsilon}_{[j,k]}(t) + |\tilde{A}_{jj,k}| \bar{\varrho}_{[j]} + \bar{w}_{j,k}(\tilde{\psi}_{[j]}) + |\tilde{B}_{j,k}| \Delta \bar{g}_j |u_{[j]}| + \lambda \bar{\varrho}_{[j,k]} \right] + \lambda \bar{\varrho}_{[i,k]} + \bar{\varrho}_{[i,k]}^+ \quad (11)$$

where $\Delta \bar{g}_j(t) = \max_{\tilde{x}_{[j]}, \tilde{\psi}_{[j]}} |\Delta \tilde{g}_j(t)|$. It is worth noting that Assumption 1 implies that the state and input variables are bounded; hence all quantities in (11) are bounded as well. The threshold dynamics (11) can be initialized with $\bar{\epsilon}_{[i,k]}(0) = \bar{\varrho}_{[i,k]}(0)$.

Remark 2: For FD purposes, the communication between subsystems is limited. It is not necessary that each diagnoser knows the model of neighbouring subsystems. Instead, in the shared case (10), it is sufficient that each subsystem $\tilde{\Sigma}_{[i]}$ sends to neighbouring subsystems in $\mathbb{S}^k$ only a limited number of variables (the interconnection variables and the consensus terms for estimates and thresholds), locally computed.

The threshold in (11) guarantees the absence of false-positive alarms before the occurrence of the fault caused by the uncertainties. On the other hand, this is a conservative result since it does not allow to detect faults whose magnitude is lower than the uncertainties magnitude in the system dynamics. This issue is formalized in the fault detectability section (Section V), where we consider also the issue that the fault may be hidden by the control action.

C. The consensus matrix

In this subsection we explain how to properly define the consensus matrix in order to allow a PnP architecture. 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 time-varying weighting matrix W^k whose dimension is equal to the maximum number of subsystems that can be plugged in sharing that variable. In the case that, at a given time, the variable is not shared (and hence at most one subsystem is using it) the only non-null weight is the one corresponding to the

considered subsystem (this does not affect the convergence of the FD estimator as illustrated in Subsection IV-D).

Indeed, the introduction of the proposed time-varying consensus matrix is advantageous from a second perspective. Since the proposed threshold is conservative, an important topic is to reduce it. Therefore, in the case of shared variables, similarly as in [26], we design a time-varying consensus-weighting matrix W^k able to minimize the adaptive threshold with respect to the consensus weights, by choosing the smallest threshold term from all the threshold additive terms in (11). In this consensus protocol, it is convenient to weight more the subsystem which has got the lowest threshold component, hence the subsystem that has lower uncertainty in its measurements and in the local model. These aims can be achieved by defining the following consensus matrix, where each (i, j) -th component is computed as:

$$W_{i,j}^k = \begin{cases} 1 & \text{if } j = \arg \min_{j \in \mathbb{S}^k} \lambda (\bar{\epsilon}_{[j,k]} + \bar{\varrho}_{[j,k]}) \\ & + |\tilde{A}_{jj,k}| \bar{\varrho}_{[j]} + |\tilde{B}_{j,k}| \Delta \bar{g}_j |u_{[j]}| + \bar{w}_{j,k}(\tilde{\psi}_{[j]}) \\ 0 & \text{otherwise} \end{cases} \quad (12)$$

At each time-step each local fault-diagnoser receives estimates and consensus terms of variable $\tilde{x}_{[i,k]}$ only from the subsystems sharing it at that specific time. Then, it selects the contribution affected by “smaller uncertainty”. As briefly discussed in Section V, fault-detectability may be improved by this approach.

D. Estimator convergence

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

$$\epsilon_{k,E}^+ = W^k \left[\lambda \epsilon_{k,E} + \tilde{A}_{k,E} \varrho_E + \tilde{B}_{k,E} \Delta g_E u_E + w_{k,E} - \lambda \varrho_{k,E} \right] + \lambda \varrho_{k,E} + \varrho_{k,E}^+, \quad (13)$$

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

Proposition 1: The dynamics defined in (13), where the consensus matrix is given by (12), converges to a neighbourhood of the origin.

Proof: The proof is carried out exploiting the one reported in [26] in a purely distributed fault-diagnosis framework. Specifically, since W^k is a stochastic matrix, its norm is always equal to 1. Therefore, since $0 < \lambda < 1$, then also $\|\lambda W^k(t)\| \leq \gamma < 1$, with $0 < \gamma < 1$.

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

For $t \rightarrow \infty$, the series converges to zero. Moreover, using results in [27], we can state that a system $x(t+1) = A(t)x(t)$, with $A(t) \in \text{convh}(A_1, \dots, A_N)$, it is exponentially stable iff $\exists$ a sufficiently large integer q such that $\|A_{i_1} A_{i_2} \dots A_{i_q}\| \leq \gamma < 1$, $\forall (i_1, \dots, i_q) \in \{1, \dots, N\}^q$. In our case, therefore, we only need to analyze matrix $W^k(t)$. Since each row of $W^k(t)$ has all null elements except one equal to 1, the product $W^k(t)W^k(t-1) \dots W^k(0)$ is a stochastic matrix. Hence, since $0 < \lambda < 1$, we have $\|\lambda^t(W^k(t)W^k(t-1) \dots W^k(0))\| < 1$ and the hypothesis is satisfied. Finally, since all the uncertain terms are bounded, then the discrete-time system described in (13) converges to a neighbourhood of the origin. ■

V. FAULT DETECTABILITY ANALYSIS

Consider the case of a faulty subsystem, that is, suppose that a fault $\phi(\cdot)$ occurs at an unknown time $t = T_0$. We address the general case of a shared variable, with $\phi_{k,E} = \phi^{(k)} \cdot (1, \dots, 1)^T$ denoting the extended fault function vector collecting the fault functions of the subsystems sharing the k -th variable. After the occurrence of the fault, for $t > T_0$, the state estimation error dynamics is given by

$$\begin{aligned} \epsilon_{k,E}^+ &= W^k \left[\lambda \epsilon_{k,E} + \tilde{A}_{k,E} \varrho_E + \tilde{B}_{k,E} \Delta g_E u_E + w_{k,E} \right. \\ &\quad \left. - \lambda \varrho_{k,E} \right] + \lambda \varrho_{k,E} + \varrho_{k,E}^+ + \phi_{k,E}. \end{aligned}$$

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

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

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

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

for at least one subsystem $i \in \mathbb{S}^k$. Using the triangle inequality and the threshold definition (11), the following is implied

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

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

$$\exists t_1 > T_0 : \left| \sum_{h=T_0}^{t_1-1} \lambda^{t_1-1-h} \phi_k(h) \right| > 2\bar{\epsilon}_{[i,k]}(t_1) \quad (14)$$

for at least one component $k \in \{1, \dots, \tilde{n}_i\}$, thus allowing the detection of a fault at time t_1 . Condition (14) implicitly characterizes the class of faults that are detectable by the proposed FD architecture. Moreover, thanks to the introduction of the time-varying consensus weighting matrix, the threshold on the right-hand-side of (14) can be decreased thus enlarging the class of detectable faults.

Remark 3: It is worth emphasizing the influence of the control inputs on the fault detectability condition:

$$\begin{aligned} \left| \sum_{h=T_0}^{t_1-1} \lambda^{t_1-1-h} \phi_k(h) \right| &> 2 \left(\sum_{j \in \mathbb{S}^k} W_{i,j}^k [\lambda \bar{\epsilon}_{[j,k]}(t_1) \right. \\ &\quad + |\tilde{B}_{j,k}| \Delta g_j |u_{[j]}(t_1)| + \bar{w}_{j,k}(t_1) + |\tilde{A}_{j,k}| \bar{\varrho}_{[j]}(t_1) \\ &\quad \left. + \lambda \bar{\varrho}_{[j,k]}(t_1) \right] + \lambda \bar{\varrho}_{[i,k]}(t_1) + \bar{\varrho}_{[i,k]}^+(t_1). \end{aligned}$$

Actually, the control term $u_{[j]}(t_1)$ affects the threshold and, in particular, it may have a detrimental effect on the fault detectability by increasing the detection threshold. This is an important issue that deserves further investigation.

VI. RECONFIGURATION STRATEGY

In this section, the reconfiguration of the LSS in case of detection of a fault in one of the subsystems is addressed. In general, depending on the specific application context, two distinct actions may turn out to be feasible: i) immediate “disconnection” of the faulty subsystem or ii) continuation of the system operation in “safety mode”. As in this paper we deal with an *active distributed fault-tolerant* control scheme, we consider only the first scenario and, in the following, the *unplugging* after fault-detection and the possible *plug-in* after subsystem repair/replacement are addressed separately.

A. Subsystem unplugging after fault detection

Unplugging of the j -th subsystem at detection time $t = t_1$ is modelled in the distributed FD architecture as follows.

- In the children subsystems $i \in \mathcal{F}_j$, for $t \geq t_1$, the components of $\tilde{\psi}_{[i]}$ and $z_{[i]}$ related to subsystem $\tilde{\Sigma}_{[j]}$ become equal to 0. Hence, for $t \geq t_1$, the related interconnection variables and measurements do not influence the time-behavior of (10).
- In the children subsystems $i \in \mathcal{F}_j$, the adaptive threshold $\bar{\epsilon}_{[i]}$ is computed through (11) by not considering the coupling terms related to the j -th subsystem when computing $\bar{w}_i$ for $t \geq t_1$.
- In the neighboring subsystems i , with $i \in \mathcal{F}_j$ or $i \in \mathcal{N}_j$, sharing some variables with $\tilde{\Sigma}_{[j]}$, the weights associated with $\tilde{\Sigma}_{[j]}$ in the consensus matrices W^k computed in (12) are set to zero.

Beyond the above changes in the local models embedded in the distributed FD component as a consequence of the subsystem unplugging after the detection of a fault, the reconfiguration of the control architecture has to be addressed as well, taking into account that the control and the FD architectures operate referring to different decompositions of the LSS.

Let $\Sigma_{[j]}$ denote the subsystem in the decentralized control decomposition corresponding to the above subsystem $\tilde{\Sigma}_{[j]}$ in the FD decomposition. Under Assumption 1-(III), for each $i \in \mathcal{F}_j$, a contraction of the set $\mathcal{N}_i$ takes place. Then, a contraction takes place also on set $\mathbb{W}_i$ in (9) and the set $\tilde{\mathbb{Z}}_i^0$ already computed still verifies the inclusions in Step (III) of Algorithm 1. Therefore, for each $i \in \mathcal{F}_j$, the choice of $\tilde{\mathbb{Z}}_i^0$ made before the unplugging still guarantees the feasibility of the LP problem in Step (IV) which finally implies that there is no need of redesigning the controller $\mathcal{C}_{[i]}$ to keep the overall stability.²

B. Subsystem plugging-in

The operation of plugging-in a subsystem into the LSS interconnected structure may be needed either in case of addition of a new subsystem or replacement of a previously un-plugged subsystem. This operation might be critical and not always feasible. Moreover, the effects of this operation have to be dealt with reference to both the FD scheme and the decentralized controller.

Concerning the FD component, after plugging-in a subsystem, a new fault diagnoser has to be provided taking into account the information exchange pattern depending on the topology of the interconnected LSS. Each new state variable is estimated using the estimator (10). We assume that the structure of the function $\tilde{w}_i$, describing the bounds on the coupling terms, is not influenced as far as the subsystems already in place before the plugging-in are concerned. Similarly we assume that plugging-in of a novel subsystem does not change the structure of the function $\tilde{g}_i$ of the already connected subsystems $i \in \mathcal{M}$, since the local model is designed so to consider all the possible connections of subsystem $\tilde{\Sigma}_{[i]}$ with other subsystems by means of the shared variables (by defining a-priori a maximum number of possible connections). Also, the state vectors $\tilde{x}_{[i]}$ of each subsystem already consider all possible shared variables even if they are null at the current instant.

Concerning the decentralized controller, the plugging-in of a new subsystem requires to design a new controller and to redesign controllers of children subsystems. Indeed, assume that subsystem $\Sigma_{[M+1]}$ is plugged in. In order to design the controller $\mathcal{C}_{[M+1]}$, we execute Algorithm 1 that needs information only from subsystems $\Sigma_{[j]}$, $j \in \mathcal{N}_{M+1}$. If Algorithm 1 stops, it turns out that $\Sigma_{[M+1]}$ cannot be plugged in.

²As the number of parent subsystems of $\Sigma_{[i]}$, $i \in \mathcal{F}_j$ decreased after unplugging, a redesign of controllers $\mathcal{C}_{[i]}$ through Algorithm 1, though not necessary for stability, could lead to performance improvement.

VII. PRELIMINARY SIMULATION RESULTS

In this section, some preliminary simulation results on a simple academic example are shown in order to shed some light on the potentialities and effectiveness of the proposed PnP architecture. Specifically, a low-order system composed by the interconnection of two mass-spring-damper systems is considered (see Fig. 2).

Fig. 2. Example system.

The system is composed by two trucks coupled by a spring and a damper. Parameters values are: $m_1 = m_2 = 8$ and $k_{12} = h_{12} = 0.5$. Each truck $i \in \mathcal{M} = \{1, 2\}$, is a subsystem with state variables $x_{[i]} = (x_{[i,1]}, x_{[i,2]})$ and input $u_{[i]}$, where $x_{[i,1]}$ is the displacement of truck i with respect to a given equilibrium position, $x_{[i,2]}$ is the velocity of the truck i and $100u_{[i]}$ is a force applied to truck i . Subsystems are equipped with the state constraints $|x_{[i,1]}| \leq 1.5$, $|x_{[i,2]}| \leq 1$, $i \in \mathcal{M}$ and with the input constraints $|u_{[i]}| \leq 1.5$, $i \in \{1, 2\}$. We obtain models $\Sigma_{[i]}$ by discretizing the second order continuous-time system representing each truck with 0.2 sec sampling time, using exact discretization and treating $u_{[i]}$ and $x_{[j]}$, $j \in \mathcal{N}_i$ as exogenous signals. Moreover the position and velocity measurements are affected by bounded disturbances, respectively $|\varrho_{[i,1]}| \leq 0.1$ and $|\varrho_{[i,2]}| \leq 0.05$, $i \in \{1, 2\}$. We synthesized controllers $\mathcal{C}_{[i]}$, $i \in \mathcal{M}$ using Algorithm 1. At time t we compute the control action $u_{[i]}$ and apply it to the continuous-time system, keeping the value constant between time t and $t+1$. As regards the FD architecture, in this simple academic example we consider a non-shared decomposition, hence the two FD estimators are designed for subsystems $\Sigma_{[i]}$, $i \in \{1, 2\}$ as proposed in Section IV with $\lambda = 0.5$. We assume $x_{[1]}(0) = (1, 0)$ and $x_{[2]}(0) = (1, 0)$. At time $t = 2$ sec, a fault occurs: the mass of subsystem $\Sigma_{[2]}$ changes in $m_2 = 2$. In two time instants, the FD architecture detects a fault in $\Sigma_{[2]}$. Since the controllers and the detectors are designed in a PnP fashion as proposed in Sections III and IV, respectively, and the faulty in $\Sigma_{[2]}$ does not impact on the design of controller and fault detector for $\Sigma_{[1]}$, we need to redesign only controller $\mathcal{C}_{[2]}$ and FD estimator for state variables of truck 2. We also note that, irrespectively of the number of masses, the reconfiguration process involves only the second mass. In Fig. 3 we note that for $t > 2$ sec, the velocity of the second truck increases due to the presence of the fault and the next reconfiguration of the controller. We also highlight that without reconfiguration, the MPC optimization problem for subsystem $\Sigma_{[2]}$ becomes infeasible.

VIII. CONCLUDING REMARKS

In this paper, a novel integrated architecture composed of a decentralized MPC scheme and of a distributed FD

Fig. 3. Simulation with initial state $x_{[1]}(0) = (1, 0)$ and $x_{[2]}(0) = (1, 0)$. The fault occurs at time $t = 2$ sec.

architecture has been proposed in the context of fault-tolerant control of a class of large-scale nonlinear systems. The integrated control scheme guarantees closed-loop asymptotic stability and constraints satisfaction at each time instant, while the FD architecture allows to detect faulty subsystems guaranteeing the absence of false-alarms. The innovative idea is to combine DiMPC and Di FD architectures, where local controllers and state estimators can be designed in a PnP fashion, i.e. the overall model of the LSS is never used in any step of the design phase. The proposed architecture is suitable for several large-scale applications, allowing revamping of actuators and isolating faulty subsystems avoiding to propagate the fault of a subsystem in the network of subsystems. Future research efforts will be devoted to generalizing the approach to a larger class of nonlinear systems and to apply it to realistic large-scale systems scenarios.

REFERENCES

- [1] T. Samad and T. Parisini, "Systems of Systems," in *The Impact of Control Technology*, T. Samad and A. M. Annaswamy, Eds. IEEE Control Systems Society, 2011, pp. 175–183. [Online]. Available: ieeecss.org/general/impact-control-technology
- [2] K. Baheti and H. Gill, "Cyber-physical systems," *The Impact of Control Technology (T.Samad and A.Annaswamy, eds.)*, 2011. [Online]. Available: www.ieeecss.org
- [3] J. Lunze, *Feedback control of large scale systems*. Upper Saddle River, NJ, USA: Prentice Hall, Systems and Control Engineering, 1992.
- [4] A. I. Zečević and D. D. Šiljak, *Control of complex systems: Structural constraints and uncertainty*. Berlin, Germany: Springer, Communications and Control Engineering, 2010.
- [5] P. D. Christofides, R. Scattolini, D. Muñoz de la Peña, and J. Liu, "Distributed model predictive control: A tutorial review and future research directions," *Computers and Chemical Engineering*, vol. 51, pp. 21–41, 2013.
- [6] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and Fault Tolerant Control*. Berlin, Germany: Springer, 2003.
- [7] R. Isermann, *Fault-Diagnosis Systems: An Introduction from Fault Detection to Fault Tolerance*. Springer-Verlag, 2006.
- [8] V. Venkatasubramanian, R. Rengaswamy, S. N. Kavuri, and K. Yin, "A review of process fault detection and diagnosis: Part I: Quantitative model-based methods," *Computers and Chemical Engineering*, vol. 27, pp. 293–311, 2003.
- [9] 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.
- [10] W. Li, W. Gui, Y. Xie, and S. Ding, "Decentralized fault detection system design for large-scale interconnected systems," in *Proceedings of the 7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, Barcelona, Spain, June 30-July 3, 2009, pp. 816–821.
- [11] 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.
- [12] F. Boem, R. M. G. Ferrari, T. Parisini, and M. M. Polycarpou, "A distributed fault detection methodology for a class of large-scale uncertain input-output discrete-time nonlinear systems," in *Proceedings of the 50th IEEE Conference on Decision and Control, and the European Control Conference*, Orlando, FL, USA, December 12-15, 2011, pp. 897–902.
- [13] 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.
- [14] S. Rivero, 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.
- [15] —, "Plug-and-Play Model Predictive Control based on robust control invariant sets," Dipartimento di Ingegneria Industriale e dell'Informazione, Università degli Studi di Pavia, Pavia, Italy, Tech. Rep., 2012. [Online]. Available: [arXiv:1210.6927](https://arxiv.org/abs/1210.6927)
- [16] J. Stoustrup, "Plug & Play Control: Control Technology towards new Challenges," in *Proceedings of the 10th European Control Conference*, Budapest, Hungary, August 23-26, 2009, pp. 1668–1683.
- [17] 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.
- [18] J. Prakash, S. Narasimhan, and S. C. Patwardhan, "Integrating Model Based Fault Diagnosis with Model Predictive Control," *Industrial & Engineering Chemistry Research*, vol. 44, no. 12, pp. 4344–4360, 2005.
- [19] K. Tsudal, D. Mignone, G. Ferrari-Trecate, and M. Morari, "Reconfiguration Strategies for Hybrid Systems," in *Proceedings of American Control Conference 2001*, Arlington, VA, USA, June 25-27, 2001, pp. 868–873.
- [20] D. M. Raimondo, S. Rivero, S. Summers, C. N. Jones, J. Lygeros, and M. Morari, "A set theoretic method for verifying feasibility of a fast explicit nonlinear Model Predictive Controller," in *Distributed Decision Making and Control*, R. Johansson and A. Rantzer, Eds. Springer, Lecture Notes in Control and Information Sciences vol. 417, 2012, ch. 13, pp. 289–311.
- [21] S. V. Raković, A. R. Teel, D. Q. Mayne, and A. Astolfi, "Simple Robust Control Invariant Tubes for Some Classes of Nonlinear Discrete Time Systems," in *Proceedings of the 45th IEEE Conference on Decision and Control*, San Diego, CA, USA, December 13-15, 2006, pp. 6397–6402.
- [22] D. M. Raimondo, S. Rivero, C. N. Jones, and M. Morari, "A Robust Explicit Nonlinear MPC Controller with Input-To-State Stability Guarantees," in *Proceedings of the 18th IFAC World Congress*, Milano, Italy, August 28 - September 2, 2011, pp. 9284–9289.
- [23] D. Q. Mayne, M. M. Seron, and S. V. Raković, "Robust model predictive control of constrained linear systems with bounded disturbances," *Automatica*, vol. 41, no. 2, pp. 219–224, 2005.
- [24] S. V. Raković and M. Baric, "Parameterized Robust Control Invariant Sets for Linear Systems: Theoretical Advances and Computational Remarks," *IEEE Transactions on Automatic Control*, vol. 55, no. 7, pp. 1599–1614, 2010.
- [25] S. Rivero, "Distributed and plug-and-play control for constrained systems," Ph.D. dissertation, Università degli studi di Pavia, 2014.
- [26] F. Boem, R. M. G. Ferrari, T. Parisini, and M. M. Polycarpou, "Distributed Fault Detection for Uncertain Nonlinear Systems: a Network Delay Compensation Strategy," in *Proceedings of American Control Conference 2013*, Washington, DC, USA, June 17-19, 2013, pp. 3549–3554.
- [27] M. L. Sichertiu and P. H. Bauer, "Stability of discrete time-varying linear delay systems and applications to network control," in *Stability*

and Control of Dynamical Systems with Applications. Springer, 2003,
pp. 117–130.