Fault-Driven Minimal Structurally Overdetermined Set in a Distributed Context

Carlos Gustavo Pérez[1,2], **Elodie Chanthery**[1], **Louise Travé-Massuyès**[1] and **Javier Sotomayor**[1,2]
[1]LAAS-CNRS, Université de Toulouse, CNRS, INSA, Toulouse, France
[2]Engineering Department, Pontifical Catholic University of Peru, PUCP
e-mail: {cgperez,elodie.chanthery,louise}@laas.fr
e-mail: {jsotom}@pucp.pe

Abstract

Distributed diagnosis is important for on-board systems as a way to reduce computational costs or for large geographically distributed systems that require minimizing data transfer. This paper presents a distributed diagnosis framework for continuous systems that only requires the knowledge of local models and limited knowledge of their neighboring subsystems. We introduce the notion of Fault-Driven Minimal Structurally Overdetermined (FMSO) set as the corner stone of the design of residual generators. We show that all the FMSO sets of the global system can be obtained in a distributed manner from so-called shared FMSO sets and shared CMSO sets that are computed along a structural approach for every local site.

1 Introduction

For large complex systems with constraints such as communication bandwidth or large geographic distribution, it is more appropriate (even mandatory) to use distributed approaches. In some cases, this is even the only viable solution given structural, computational and robustness issues.

In large-scale systems, diagnosis algorithms must account for two real-time requirements [Boem *et al.*, 2011]: 1) enough computation power for processing all the necessary measurements and 2) enough communication bandwidth in order to gather all the measurements to the place where they are processed. In addition to the economic implications related to the first requirement, it should be noted that the second requirement can be even more difficult to achieve if for example the system covers a large geographic area and the measurements are distributed, so that they cannot be directly wired to the processing computer. Moreover, there are contexts where a centralized architecture, even if feasible, would be undesirable because of several factors including size, robustness and security issues, e.g., aircraft and other transportation systems, large-scale energy or industrial plants, power generation, etc.

While distribution is often dictated by physical constraints, it has several other appealing properties over a centralized approach, including fault tolerance, scalability, and reusability. Fault tolerance stems from the ability of distributed systems to continue operation when one or more sensors are faulty. The scalability comes from reduced costs of system setup and update, communication, and decision making. Finally, when reconfiguration is required, implying to change some components or sensors, it can be easier to modify part of the distributed system impacted by the changes than to overhaul the centralized system as a whole [Grbovic, 2012].

In this paper, we use the structural framework that has shown to be a flexible and efficient tool for fault diagnosis and fault-tolerant control design. Fault-Driven Minimal Structurally Overdetermined (FMSO) sets [Pérez *et al.*, 2015] are used to ensure the minimal redundancy of residual generators in order to optimize local diagnosers (LD). In our approach, each subsystem is monitored by a LD using the information provided by measured local variables and, when necessary, by a minimal amount of measurements from neighboring subsystems. We assume the non-availability of a global system model. The algorithm that we propose achieves the same results as a global diagnoser by extending local models as least as possible when it is required.

This paper is structured as follows: section 2 motivates the use of a distributed approach and presents the related work. In section 3, some well known concepts of the structural approach are presented and the notion of Fault-Driven Minimal Structurally Overdetermined (FMSO) set is introduced. Section 4 presents some new fault distributed diagnosis concepts and the properties of FMSO sets are given. Section 5 explains how to design the set of LDs so that they achieve the same detectability and diagnosabiilty as a centralized diagnoser. A four tanks example is then used to illustrate the application of the approach in section 6. Finally, a conclusion and current work end the paper.

2 Related Work

Typically, centralized diagnosis solutions have been proposed for model-based diagnosis, but these solutions have several inherent shortcomings. First, if the centralized diagnoser fails, the system will have to operate without a diagnosis system (this is usually known as a single point of failure), and second, centralized solutions do not scale well as the size of the system increases [Gertler, 1998]. These shortcomings justify the development of techniques of decentralized and distributed diagnosis frameworks for complex large systems.

Researchers have developed several decentralized and distributed diagnosis schemes in the past, mostly in the discrete event framework [Debouk *et al.*, 2000; Pencolé and Cordier, 2005]. Distributed schemes, e.g., [Su and Wonham,

2005], unlike decentralized schemes, such as [Rami Debouk, 2000], do not make use of the global system model; instead, they use subsystem models for diagnosis, and the LD for each diagnosis submodel communicate their diagnosis results to each other to obtain the global solution. Decentralized diagnosis approaches, e.g., [Rami Debouk, 2000], typically start with a global system model to generate the LD among which the diagnosis computations get distributed. Each local distributed diagnoser makes their diagnosis decision based on only a subset of observable events, and they communicate these decisions to other LDs, or to a centralized coordinator (in decentralized case), which uses the global model to generate globally consistent diagnosis solutions. The level of coordination required between the LDs depends on how each LD is designed.

Distributed diagnosis methods have been proposed recently for continuous systems. [Bregon *et al.*, 2014] present a distributed diagnosis framework for physical systems with continuous behavior using structural model decomposition, using Possible Conflicts approach. They decompose the global system model into submodels that contain sufficient analytical redundancy to perform fault detection. However this is done ignoring pre-existing constraints that may be functional, geographical or privacy-based. We consider pre-existing constraints mandatory and therefore, possible predefined subsystems. [Khorasgani *et al.*, 2015] presents a distributed structural approach to the problem of fault detection and isolation using an algorithm that accepts a just determined subsystem and a set of measurement candidates. It provides a set of diagnosers that are as local as possible by extending local models with their neighboring subsystem's models until maximal isolability is achieved.

Our approach is designed in a distributed framework. It does not require a coordinator online, and there is no exchange of diagnosis information among the LDs, only the exchange of measurements. Besides, this method introduces important properties of Fault-Driven Minimal Structurally Overdetermined (FMSO) sets that allow us to establish the relation between FMSO sets for the subsystems and FMSO sets for the global system. This properties are key to demonstrate that all global FMSO sets can be generated from computations only at the level of the subsystems, hence achieving a truly distributed architecture.

3 Background theory

In this section some definitions associated with structural analysis of dynamic systems and focused residual generation are introduced.

3.1 Analytical Redundancy via Structural Analysis

Let the system description consist of a set of n_e equations involving a set of variables partitioned into a set Z of n_Z known (or measured) variables and a set X of n_X unknown (or unmeasured) variables. We refer to the vector of known variables as z and the vector of unknown variables as x. The system may be impacted by the presence of n_f faults that appear as parameters in the equations. The set of faults is denoted by F and we refer to the vector of faults as $\mathtt{f}$.

Definition 1 (System)**.** *A system, denoted $\Sigma(z, x, \mathtt{f})$ or Σ for short, is any set of equations relating z, x and $\mathtt{f}$. The equations $e_i(z, x) \subseteq \Sigma(z, x, \mathtt{f})$, $i = 1, \ldots, n_e$, are assumed to be differential or algebraic in z and x.*

We use a four tank system, illustrated in Figure 1, to illustrate the concepts throughout this paper. It is composed of twenty equations. Later, we assume each tank with outlet pipe as a subsystem so this system has four subsystems. Tanks 1 and 3 have inflows. There are a set of 6 measurements y_1 to y_6.

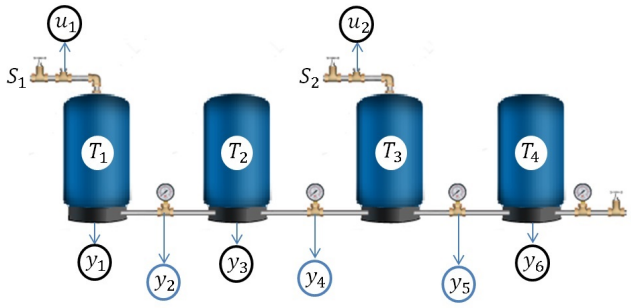


Figure 1: Four Tank System.

The model $\Sigma(z, x, \mathtt{f})$ for this system is composed of twenty equations e_1 to e_{20} relating the known variables $Z = \{u_1, u_2, y_1, y_2, y_3, y_4, y_5, y_6\}$, the unknown variables $X = \{\dot{p}_1, p_1, \dot{p}_2, p_2, \dot{p}_3, p_3, \dot{p}_4, p_4, q_{in1}, q_{in2}, q_1, q_2, q_3, q_4\}$ and the set of system faults $F = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ as given in Table 1.

Table 1: Equations for the four tank system.

e_1 :	$\dot{p}_1 = \frac{1}{C_{T_1} + f_1}(q_{in1} - q_1)$	e_4 :	$q_{in1} = u_1$
e_2 :	$q_1 = \frac{p_1 - p_2}{R_{P_1} + f_2}$	e_5 :	$p_1 = y_1$
e_3 :	$p_1 = \int \dot{p}_1 dt$	e_6 :	$q_1 = y_2$
e_7 :	$\dot{p}_2 = \frac{1}{C_{T_2} + f_3}(q_1 - q_2)$	e_{10}:	$p_2 = y_3$
e_8 :	$q_2 = \frac{p_2 - p_3}{R_{P_2} + f_4}$	e_{11}:	$q_2 = y_4$
e_9 :	$p_2 = \int \dot{p}_2 dt$		
e_{12}:	$\dot{p}_3 = \frac{1}{C_{T_3}}(q_{in2} + q_2 - q_3)$	e_{15}:	$q_{in2} = u_2$
e_{13}:	$q_3 = \frac{p_3 - p_4}{R_{P_3} + f_5}$	e_{16}:	$q_3 = y_5$
e_{14}:	$p_3 = \int \dot{p}_3 dt$		
e_{17}:	$\dot{p}_4 = \frac{1}{C_{T_4} + f_6}(q_3 - q_4)$	e_{19}:	$p_4 = \int \dot{p}_4 dt$
e_{18}:	$q_4 = \frac{p_4}{R_{P_4}}$	e_{20}:	$p_4 = y_6$

Definition 2 (ARR for $\Sigma(z, x, \mathtt{f})$)**.** *Let $\Sigma(z, x, \mathtt{f})$ be a system. Then, a relation $r(z, \dot{z}, \ddot{z}, ...) = 0$ is an Analytical Redundancy Relation (ARR) for $\Sigma(z, x, \mathtt{f})$ if for each z consistent with $\Sigma(z, x, \mathtt{f})$ the relation is fulfilled.*

Definition 3 (Residual Generator for $\Sigma(z, x, \mathtt{f})$)**.** *A system taking a subset of the variables z as input, and generating a scalar signal r as output, is a* residual generator for the model $\Sigma(z, x, \mathtt{f})$ *if, for all z consistent with $\Sigma(z, x, \mathtt{f})$, it holds that $\lim_{t \to \infty} r(t) = 0$.*

ARRs can be used to check if the measured variables z are consistent with the system model and as the basis of residual generators used for diagnosis purposes.

The *structural model* of the system $\Sigma(z, x, \mathtt{f})$, also denoted with some abuse by $\Sigma(z, x, \mathtt{f})$ or Σ in the following, can be obtained abstracting the functional relations. It only retains a representation of which variables are involved in the equations. This abstraction leads to a bipartite graph $G(\Sigma \cup X \cup Z, A)$, or equivalently to $G(\Sigma \cup X, \mathcal{A})$, where $\mathcal{A} \subseteq A$ and $\mathcal{A}$ is a set of edges such that $a(i, j) \in \mathcal{A}$ iff variable x_i is involved in equation e_j. The bipartite graph (on the right) may be equivalently represented as a biadjacency matrix (on the left) as in Figure 2.

Obtaining ARRs for a system $\Sigma(z, x, \mathtt{f})$ involves the elimination of unknown variables, which can be inferred from structural analysis [Travé-Massuyès *et al.*, 2006]. ARRs are indeed known as the causal interpretation of minimal structurally overdetermined (MSO) sets [Krysander *et al.*, 2010]. One should notice that results obtained in a structural framework are a best case scenario: causality considerations, algebraic and differential loops, etc. ultimately define which structural redundancies can be used for the design of actual residual generators [Armengol *et al.*, 2009].

3.2 Focused Residual Generation

A key tool for analyzing a structural model is the Dulmage-Mendelson (DM) canonical decomposition. It results in a partition of the system model Σ into three parts: the *structurally overdetermined* (SO) part Σ^+ that has more equations than unknown variables; the *structurally just determined* part Σ^0 that has as many equations as unknown variables, and the *structurally underdetermined* part Σ^- that has more unknown variables than equations.

Definition 4 (Structural redundancy)**.** *The structural redundancy $\rho_{\Sigma'}$ of a set of equations $\Sigma' \subseteq \Sigma$ is defined as the difference between the number of equations and the number of unknown variables.*

The structural redundancy of an SO set is positive. Let us notice that the structural redundancy of an arbitrary set of equations $\Sigma' \subseteq \Sigma$ may be positive, zero, or negative.

Proposition 3.1. *Consider two sets of equations $\Sigma' \subseteq \Sigma$ and $\Sigma'' \subseteq \Sigma$, then $\rho_{\Sigma' \cup \Sigma''} = \rho_{\Sigma'} + \rho_{\Sigma''} + |X_{\Sigma'} \cap X_{\Sigma''}|$.*

Definition 5 (PSO and MSO sets)**.** *A set of equations Σ is proper structurally overdetermined (PSO) if $\Sigma = \Sigma^+$ and minimally structurally overdetermined (MSO) if no proper subset of Σ is overdetermined [Krysander* et al.*, 2010].*

Since PSO and MSO sets have more equations than variables, they can be used to generate ARRs and residuals. MSO sets are of special interest since they are just overdetermined, i.e. they have structural redundancy 1. However, not all MSO sets are interesting to construct residual generators, in particular those that are not impacted by faults. Hence it is desirable to consider a fault-focused concept. The concept of *test equation support* (TES) has been introduced in [Krysander *et al.*, 2010]. A TES is a set of equations expressing redundancy specific to a set of considered faults, known as the *test support* (TS) or as the *fault support*, term that we use in this paper. A minimal TES (MTES) is such that no proper subset is a TES.

It is necessary to notice that, whereas an MSO set is just overdeterminated and hence has redundancy 1, an MTES may have higher redundancy. This may be an advantage to develop more powerful tests; however, for the distribution problem, the aim is to minimize the information shared by subsystems, hence the concept of *Fault-Driven Minimal Structurally Overdetermined* set defined below is preferable [Pérez *et al.*, 2015].

A Fault-Driven Minimal Structurally Overdetermined (FMSO) set φ is an MTES of structural redundancy 1. Equivalently, it can be defined as an MSO set of $\Sigma(z, x, \mathtt{f})$ whose fault support is not empty.

Let us define $Z_\varphi \subseteq Z$, $X_\varphi \subseteq X$, and $F_\varphi \subseteq F$ as the set of known variables, unknown variables involved in the FMSO set φ, and the set of faults in its fault support, respectively. We then have the following formal definition.

Definition 6 (FMSO set)**.** *A subset of equations $\varphi \subseteq \Sigma(z, x, f)$ is an FMSO set of $\Sigma(z, x, f)$ if $F_\varphi \neq \emptyset$ and $\rho_\varphi = 1$ that means $|\varphi| = |X_\varphi| + 1$.*

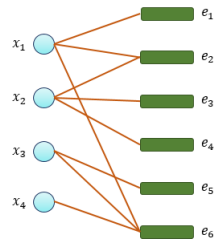
We also define the concept of *Clear Minimal Structurally Overdetermined* (CMSO) set as an MSO set of $\Sigma(z, x, \mathtt{f})$ whose fault support is empty.

Definition 7 (CMSO set)**.** *A subset of equations $\Lambda \subseteq \Sigma(z, x, f)$ is a CMSO set of $\Sigma(z, x, f)$ if $F_\Lambda = \emptyset$ and $\rho_\Lambda = 1$ that means $|\Lambda| = |X_\Lambda| + 1$.*

To illustrate these concepts, we consider an academic example with: $\Sigma = \{e_1, e_2, e_3, e_4, e_5, e_6\}$, $X = \{x_1, x_2, x_3, x_4\}$ and $F = \{f_1, f_2\}$ as shown in Figure 2.

Eq	Unknown				Faults	
	x_1	x_2	x_3	x_4	f_1	f_2
e_1	X					
e_2	X	X			X	
e_3		X				
e_4		X				
e_5			X			
e_6	X		X	X		X

(a) Biadjency matrix



(b) Bip. graph

Figure 2: Academic example.

If we consider the fault f_1 and use the algorithm proposed in [Krysander *et al.*, 2010], there exists an *MTES* focused in fault f_1, $\Sigma_1 = \{e_1, e_2, e_3, e_4\}$ with redundancy $\rho_{\Sigma_1} = 2$. In the other hand, using our approach we can find minimal redundancy by two FMSO sets: $\varphi_1 = \{e_1, e_2, e_3\}$ and $\varphi_2 = \{e_1, e_2, e_4\}$ both focused on fault f_1 which is more efficient for distribution.

4 Distributed Diagnosis

This section defines the notion of subsystems and reconsiders the concept of FMSO set in the distributed case. Important properties of FMSO sets are provided that allow us to establish the relation between FMSO sets for the subsystems and FMSO sets for the global system. This properties are key to demonstrate that all global FMSO sets can be generated from computations only at the level of the subsystems, hence achieving a truly distributed architecture.

4.1 Distribution and Related Notions

Let us consider the system Σ and define the following:

Definition 8 (Global FMSO set)**.** *A global FMSO set is an FMSO set of $\Sigma(z, x, f)$. The set of global FMSO sets is denoted by Φ.*

A decomposition of the system Σ, into several subsystems Σ_i is defined as a partition of its equations. Let $\Sigma = \{\Sigma_1, \Sigma_2, ..., \Sigma_n\}$ with $\Sigma_i \subseteq \Sigma$, $\bigcup_{i=1}^{n} \Sigma_i = \Sigma$, $\Sigma_i \neq \varnothing$ and $\Sigma_i \cap \Sigma_j = \varnothing$ if $i \neq j$.

This decomposition leads to n subsystems denoted $\Sigma_i(z_i, x_i, \mathtt{f}_i)$, with $i = 1, ..., n$, where z_i is the vector of known variables in Σ_i, x_i the vector of unknown variables in Σ_i and $\mathtt{f}_i$ refers to the vector of faults in Σ_i. The set of variables and faults of the i^{th} subsystem Σ_i, denoted as X_i, Z_i, and F_i respectively, are defined as the subset of variables of X, Z, and F respectively, that are involved in the subsystem Σ_i.

For the four tanks system example, we consider (as [Khorasgani *et al.*, 2015]) that each tank and the outlet pipe to its right, constitute a subsystem (Table 2).

Table 2: Model decomposition of the four tanks system into subsystems $\Sigma_i(z_i, x_i, \mathtt{f}_i)$, $i = 1, 2, 3, 4$.

$\Sigma_1 = \{e_1, e_2, e_3, e_4, e_5, e_6\}$	$F_1 = \{f_1, f_2\}$
$X_1 = \{\dot{p_1}, p_1, p_2, q_{in1}, q_1\}$	$Z_1 = \{u_1, y_1, y_2\}$
$\Sigma_2 = \{e_7, e_8, e_9, e_{10}, e_{11}\}$	$F_2 = \{f_3, f_4\}$
$X_2 = \{\dot{p_2}, p_2, p_3, q_1, q_2\}$	$Z_2 = \{y_3, y_4\}$
$\Sigma_3 = \{e_{12}, e_{13}, e_{14}, e_{15}, e_{16}\}$	$F_3 = \{f_5\}$
$X_3 = \{\dot{p_3}, p_3, p_4, q_{in2}, q_2, q_3\}$	$Z_3 = \{u_2, y_5\}$
$\Sigma_4 = \{e_{17}, e_{18}, e_{19}, e_{20}\}$	$F_4 = \{f_6\}$
$X_4 = \{\dot{p_4}, p_4, q_3, q_4\}$	$Z_4 = \{y_6\}$

Definition 9 (Local variables)**.** *The set of local variables of the i^{th} subsystem, denoted X_i^l, is defined as the subset of variables of X_i that are only involved in the subsystem Σ_i:*

$$X_i^l = X_i \setminus (\bigcup_{j=1, j\neq i}^{n} (X_i \cap X_j)) \tag{1}$$

Definition 10 (Shared Variables)**.** *The set of shared variables of the i^{th} subsystem, denoted as X_i^s, is defined as:*

$$X_i^s = \bigcup_{j=1, j\neq i}^{n} (X_i \cap X_j) = X_i \setminus X_i^l \tag{2}$$

The set of shared variables of the whole system Σ is denoted by X^s.

For instance, consider the subsystem Σ_3 of Table 2, $X_3^l = \{\dot{p_3}, q_{in2}\}$, which means that the variables of this subset are only involved in equations of Σ_3. $X_3^s = \{p_3, p_4, q_2, q_3\}$, which means that the variables of this subset link the behavior of Σ_3 with other subsystems, namely Σ_2 and Σ_4.

Without loss of generality, we consider that all known variables of Z_i are local to the subsystem Σ_i, for $i = 1, \ldots, n$. If the same input was applied to several subsystems, it could be artificially replicated.

4.2 Distributed FMSO sets

Definition 11 (Local FMSO set)**.** *φ is a local FMSO set of $\Sigma_i(z_i, x_i, \mathtt{f}_i)$ if φ is an MFSO set of $\Sigma(z, x, \mathtt{f})$ and if $\varphi \subseteq \Sigma_i$, $X_\varphi \subseteq X_i$ and $Z_\varphi \subseteq Z_i^l$. The set of local FMSO sets of Σ_i is denoted by Φ_i^l. The set of all local FMSO sets is denoted by $\Phi^l = \bigcup_{i=1}^{n} \Phi_i^l$.*

Obviously, a local FMSO set for any subsystem Σ_i is also an FMSO set of Σ, hence a global FMSO set.

For the four tanks example, a local FMSO set $\varphi_1 = \{e_1, e_3, e_4, e_5, e_6\}$ is obtained for Σ_1. These equations include local and shared variables of Σ_1 and only involve the fault f_1. It can be deduced that to achieve detectability of fault f_1, only the equations included in φ_1 are required.

We now define *shared FMSO sets* for a subsystem Σ_i by considering shared variables as known variables and computing FMSO sets. FMSO sets including equations with shared variables are called *shared FMSO sets*.

Definition 12 (Shared FMSO set)**.** *φ is a shared FMSO set of subsystem $\Sigma_i(z_i, x_i, \mathtt{f}_i)$ if φ is an FMSO set of $\tilde{\Sigma}_i(\tilde{z}_i, \tilde{x}_i, \tilde{\mathtt{f}}_i)$, where $\tilde{z}_i$ is the vector of variables in $\tilde{Z}_i = Z_i \cup X_i^s$, $\tilde{x}_i$ is the vector of variables in $\tilde{X}_i = X_i^l$, and $\tilde{\mathtt{f}}_i = \mathtt{f}_i$). The set of shared FMSO sets for Σ_i is denoted by Φ_i^s. The set of all shared FMSO sets is denoted by $\Phi^s = \bigcup_{i=1}^{n} \Phi_i^s$.*

From the above definition, a shared FMSO set φ for subsystem $\Sigma_i(z_i, x_i, \mathtt{f}_i)$ is such that $\varphi \subseteq \Sigma_i$, $X_\varphi \subseteq X_i^l$, $Z_\varphi \cap X_i^s \neq \emptyset$, and $Z_\varphi \subseteq (Z_i \cup X_i^s)$.

Let us take the example of the subsystem Σ_1 of Table 2, then the set of shared FMSO sets is Φ_1^s is $\{\varphi_1, \varphi_2, \varphi_3\}$:

$$\varphi_1 = \{e_2, e_5\}, where:$$
$$X_{\varphi_1} = \{p_1\}, Z_{\varphi_1} = \{q_1, p_2, y_1, y_2\}, F_{\varphi_1} = \{f_2\}$$
$$\varphi_2 = \{e_1, e_2, e_3, e_4\}, where:$$
$$X_{\varphi_2} = \{\dot{p}_1, p_1, q_{in1}\}, Z_{\varphi_2} = \{q_1, p_2, u_1\}, F_{\varphi_2} = \{f_1, f_2\}$$
$$\varphi_3 = \{e_1, e_3, e_4, e_5\}, where:$$
$$X_{\varphi_3} = \{\dot{p}_1, p_1, q_{in1}\}, Z_{\varphi_3} = \{q_1, u_1, y_1\}, F_{\varphi_3} = \{f_1\}$$

Definitions 11 and 12 can also be applied to CMSO sets to define *local CMSO sets* Λ_i^l and *shared CMSO sets* Λ_i^s. The set of all shared CMSO sets is denoted by Λ^s.

Definition 13 (Compound FMSO set)**.** *A global FMSO set φ that includes at least one shared FMSO set $\varphi' \in \Phi_i^s$ is called a compound FMSO set. The set of compound FMSO sets of Σ_i is denoted by Φ_i^c. The set of all compound FMSO sets is denoted by $\Phi^c = \bigcup_{i=1}^{n} \Phi_i^c$.*

Definition 14 (Root FMSO set)**.** *If a compound FMSO set $\varphi \in \Phi^c$ includes a shared FMSO set $\varphi' \in \Phi^s$, then φ' is a root FMSO set of φ.*

Definition 15 (Locally detectable fault)**.** *$f \in F_i$ is locally detectable in the subsystem $\Sigma_i(z_i, x_i, \mathtt{f}_i)$ if there is an FMSO set $\varphi \in \Phi_i^l$ such that $f \in F_\varphi$.*

Definition 16 (Locally isolable fault)**.** *Given two locally detectable faults f_j and f_k of F_i, $j \neq k$, f_j is locally isolable from f_k if there exists an FMSO set $\varphi \in \Phi_i^l$ such that $f_j \in F_\varphi$ and $f_k \notin F_\varphi$.*

4.3 Properties of FMSO sets

This section aims at stating the properties of locally computed FMSO sets, i.e. local FMSO sets and shared FMSO sets, with regards to the generation of global FMSO sets. Interestingly, these properties allow us to prove that the whole set of global FMSO sets Φ can be obtained from the set of locally computed FMSO sets.

Property 1. *A compound FMSO set φ contains equations from at least two subsystems.*

Property 2. *A local FMSO set $\varphi \in \Phi^l$ is also a global FMSO set.*

Property 3. *A global FMSO set $\varphi \in \Phi$ for which $\exists! i \in 1, \ldots, n$ such that $X_\varphi \subseteq X_i^l$ is also a local FMSO set of Σ_i.*

In the following, we show that global FMSO sets can be obtained from locally computed FMSO sets only, by forming compound FMSO sets with shared FMSO sets and shared CMSO sets.

Begin with a simple reasoning. Consider a shared FMSO set $\varphi \in \Phi_i^s$. The particularity of shared FMSO sets is that they are computed hypothesizing that the shared variables they include are known (cf. Definition 12). Actually, this hypothesis is just a trick that allows us to account locally for the FMSO sets that can possibly be generated if equations of other subsystems, indicated by the shared variables, are introduced. However, shared variables are actually unknown so we can define $X_\varphi^s = Z_\varphi \cap X^s$.

The shared FMSO set φ can give rise to an actual FMSO set if it can be completed with sets of equations of subsystems other than Σ_i (more precisely shared FMSO or CMSO sets) to balance the number of shared variables X_φ^s of φ and achieve structural redundancy 1.

Let us notice that the shared FMSO set φ has an actual structural redundancy of $1 - |X_\varphi^s|$. As a matter of fact, every shared variable $x^s \in X_\varphi^s$ decreases the actual structural redundancy of φ by 1. Consider a shared FMSO set $\varphi' \in \Phi_j^s, j \neq i$ for which x^s is also a shared variable, i.e. $x^s \in X_{\varphi'}^s$.

By Proposition 3.1, unioning φ' to φ potentially balances the structural redundancy deficiency for one shared variable, say x^s, in φ. However, if φ' introduces new shared variables, these also need to be balanced, each by an additional shared FMSO set. In addition, if x^s is not the only shared variable of φ, the other shared variables each require unioning a different shared FMSO set. The same reasoning also holds if φ' is a shared CMSO set. This leads to the following proposition.

Proposition 4.1. *Let $G(\mathbb{X}, \Gamma)$ be a bipartite graph such that $\mathbb{X} = \mathbb{X}_1 \cup \mathbb{X}_2$ where:*

- *$\mathbb{X}_1 = \Phi^s \cup \Lambda^s$ is the set of shared FMSO sets and shared CMSO sets of the system,*
- *$\mathbb{X}_2 = X^s$ is the set of shared variables of the system,*
- *$\Gamma : \mathbb{X}_1 \longrightarrow 2^{\mathbb{X}_2}$ is a function that gives the set of successors of each $\varphi \in \mathbb{X}_1$.*

Let $\varphi \in \mathbb{X}_1$ and $x \in \mathbb{X}_2$ then (φ, x) belongs to the edges of G if $x \in X_\varphi$.

A compound FMSO set $\mathbb{X}_1'$ is built by a subgraph $G_s(\mathbb{X}', \Gamma')$ of $G(\mathbb{X}, \Gamma)$, where $\mathbb{X}' = \mathbb{X}_1' \cup \mathbb{X}_2'$, $\mathbb{X}_1' \subset \mathbb{X}_1$, $\mathbb{X}_2' \subset \mathbb{X}_2$ if:

(i) $G_s(\mathbb{X}', \Gamma')$ contains no cycles.

(ii) $\forall \varphi \in \mathbb{X}_1', \Gamma(\varphi) \subset \mathbb{X}_2'$ and $\forall x \in \mathbb{X}_2' \; \exists \varphi \in \mathbb{X}_1'$ such that $\Gamma'(\varphi) = x$.

(iii) The terminal nodes of the graph belong to $\mathbb{X}_1'$.

The Proposition 4.1 states that a union of shared FMSO/CMOS sets originating from different subsystems forms a compound FMSO set if there are no cycles in the corresponding subgraph. Condition (ii) guarantees that if an FMSO set belongs to the subgraph, then all shared variables are in this subgraph and for all shared variables there exists one shared FMSO/CMSO set that belongs to a subsystem different from any subsystem at the above level. Condition (iii) guarantees that the structural redundancy of $\mathbb{X}_1'$ is equal to one and that $\mathbb{X}_1' = \varphi^c$ is a compound FMSO set.

Lemma 1. *The subgraph $G_s(\mathbb{X}', \Gamma')$ corresponding to a compound FMSO set has the specific AND/OR tree structure shown in Figure 3.*

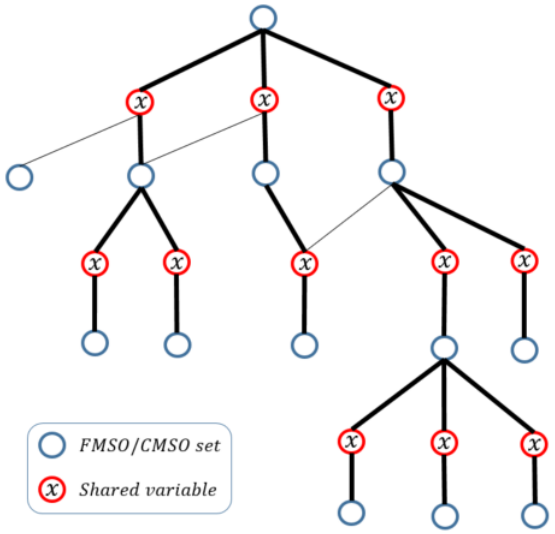


Figure 3: AND/OR tree structure of a compound FMSO set.

The FMSO set at the top of Figure 3 can be considered as the root FMSO set. The set of shared variables that belongs to the root FMSO set is included in the structure. For each of them, only one FMSO set is chosen among the FMSO/CMSO sets that include the shared variable. For each chosen FMSO/CMSO set, the shared variables are included in the structure. This property repeats down the graph levels until there is no additional shared variable to include in the structure. We talk of an *iterative matching procedure*.

It can be proved that all the global FMSO sets can be obtained from locally computed FMSO sets.

Proposition 4.2. *The set of global FMSO sets Φ is given by the union of the set of local FMSO sets Φ^l and the set of compound FMSO sets Φ^c.*

$$\Phi = \Phi^l \cup \Phi^c \tag{3}$$

5 Operational procedure for distributed diagnosis

5.1 Distributed generation of all global FMSO sets

Like [Khorasgani *et al.*, 2015], our approach assumes the non-availability of a global system model. The difference comes from the results of section 4.3 that prove that it is possible to obtain the set of global FMSO sets without recomputing FMSO sets for the local models extended by neighboring subsystem's models. Instead, our approach uses a search algorithm that identifies the sets of shared FMSO/CMSO sets computed locally that form global FMSO sets. Algorithm 1 implements the procedure

for computing the set of global FMSO sets following the proposed distributed approach. Like [Khorasgani *et al.*, 2015], our approach guaranties maximal diagnosability, i.e. the same diagnosability as a centralized approach.

$\Phi = \emptyset$;
for *i=1...n* **do**
  $\Phi_i^l \leftarrow$ Calculate local FMSO sets of Σ_i;
  $\Phi_i^s \leftarrow$Calculate shared FMSO sets of Σ_i;
  $\Lambda_i^s \leftarrow$ Calculate shared CMSO sets of Σ_i;
  for *each shared FMSO set* $\varphi \in \Phi_i^s$ **do**
    Label φ as root FMSO: $\varphi_r \leftarrow \varphi$;
    Let $X^s_{\varphi_r}$ be the set of shared variables of φ_r;
    while *it is possible to find a set* $\varphi^c \supseteq \varphi_r$ *that can be a set* $\mathbb{X}_1'$ *in Proposition 4.1 and such that* φ^c *is not included in* Φ **do**
      Store the global FMSO set φ^c:
      $\Phi \leftarrow \Phi \cup \varphi^c$;
    end
  end
  $\Phi \leftarrow \Phi \cup \Phi_i^l$
end
Return Φ;

Algorithm 1: Generation of the set of global FMSO sets

In Algorithm 1 the procedure to compute a global FMSO set φ^c that can be a set $\mathbb{X}_1'$ in Proposition 4.1 starts by searching in the bipartite graph $G(\mathbb{X}, \Gamma)$ for a matching that covers each shared variable of $X^s_{\varphi_r}$ (φ_r is the root FMSO set). This procedure is repeated for the new sets of shared variables that come with newly introduced shared FMSO sets. Iterations stop when no new shared variables are introduced. The computational complexity of the search problem increases with the number of shared variables. However, in practice, subsystems are generally designed so that their links are quite weak, hence sharing few variables. This makes the proposed approach applicable to complex dynamic systems made up of several subsystems.

5.2 Distributed generation of an optimized set of global FMSO sets

If the residuals corresponding to all the global FMSO sets were generated and used on-line to monitor the system, they would obviously achieve maximal detectability and isolability. However, all of them are not necessary and it is more efficient to minimize their number while maintaining the same property.

The aim of this section is to obtain a set of distributed local diagnosers (LD) that together make the entire system completely diagnosable through local and compound FMSO sets. These LDs are designed to achieve maximal diagnosability with minimal communication between subsystems. First, local FMSO sets are determined for every subsystem Σ_i. If these are not sufficient to detect and isolate all of the faults in F_i, then a set of compound FMSO sets is determined to achieve full diagnosability for all the faults in F_i, considering constraints of distance and amount of communication between subsystems. This set is computed as explained in Section 5.1.

The diagnosers design is done off-line and consists of the steps given in Algorithm 2, performed for each subsystem Σ_i, $i = 1...n$. The procedure to compute 'good' compound FMSO sets starting with φ^* as a root FMSO set makes use of an optimization heuristic based on the number of shared variables. In Algorithm 2, the term 'best' is hence used in the sense of this heuristic.

for *i=1...n* **do**
  $\Phi_i = \emptyset$;
  $\Phi_i^l \leftarrow$ Calculate local FMSO sets of Σ_i;
  if *there is any fault* $f \in F_i$ *not locally detectable or not locally isolable with the set of local FMSO sets* Φ_i^l **then**
    $\Phi_i^s \leftarrow$ Calculate shared FMSO sets of Σ_i;
    $\Lambda_i^s \leftarrow$ Calculate shared CMSO sets of Σ_i;
  end
  while *it exists* $f \in F_i$ *that is not detectable or isolable* **do**
    Let $\varphi^* \in \Phi_i^s$ such that $f \in F_{\varphi^*}$ be the 'best' (not already selected) shared FMSO set of Φ_i^s ;
    Label φ^* as root FMSO set: $\varphi_r \leftarrow \varphi^*$;
    Let $X^s_{\varphi_r}$ be the set of shared variables of φ_r;
    $\Phi_i^{c*} \leftarrow$ Find a 'good' compound FMSO set including φ^* by always selecting the 'best' shared FMSO sets to cover newly introduced shared variables;
    $\Phi_i \leftarrow \Phi_i \cup \Phi_i^{c*}$;
    $\Phi_i^{l*} \leftarrow$ Find a minimal cardinality set of local FMSO sets achieving the same diagnosability as all local FMSO sets;
    $\Phi_i \leftarrow \Phi_i \cup \Phi_i^{l*}$;
  end
end

Algorithm 2: Generation of LDs.

Algorithm 2 is intended to produce a minimal cardinality set of global FMSO sets while minimizing subsystems interactions. It is based on a heuristic and further work must be performed to assess its properties in terms of optimality.

6 Application to the four tanks system

6.1 Finding of Global FMSO sets

According to operational procedure of section 5, by algorithm 1 it is possible to get the set of global FMSO sets Φ from the set of local FMSO sets Φ^l, shared FMSO sets Φ^s and shared CMSO sets Λ^s.

Running the algorithm 1, first we calculate local FMSO sets Φ_i^l, shared FMSO sets Φ_i^s and shared CMSO sets Λ_i^s of each subsystem $(i = 1..4)$ as shown in Table 3. Then with each shared FMSO set as root FMSO set, we found all compound FMSO sets $\varphi \in \Phi^c$ for the four tank system as if a global model is not available.

As illustration, in the subsystem Σ_1, considering the shared FMSO set φ_1 as a root FMSO set with the set of $X^s_{\varphi_1} = \{q_1, p_2\}$, a compound FMSO set is computed iteratively by the set $\varphi^c = \cup_{k=1}^c \varphi_k = \varphi_1 \cup \varphi_5 \cup \varphi_6 \cup \lambda_3 \cup \varphi_7 \cup \lambda_4 \cup \lambda_6$, with $\cup_{k=1}^c X^s_{\varphi_k} = \{q_1, p_2, q_2, p_3, q_3, p_4\}$, where each shared variable x^s is covered by two shared FMSO/CMSO sets as it is shown in the corresponding subgraph of Figure 4. As a result, the compound FMSO set φ' obtained is $\{e_2, e_5, e_7, e_8, e_9, e_{11}, e_{13}, e_{16}, e_{20}\}$. Considering all possible φ^c that can be a set $\mathbb{X}_1'$ in Proposition 4.1, 164 compound FMSO sets are computed for this system.

Table 3: local FMSO sets Φ_i^l, shared FMSO sets Φ_i^s and shared CMSO sets: Λ_i^s, $(i = 1..4)$.

$\Phi_1^s = \{\varphi_1, \varphi_2, \varphi_3\}$, $\Phi_1^l = \{\varphi_4\}$, $\Lambda_1^s = \{\lambda_1\}$,
$\Phi_2^s = \{\varphi_5, \varphi_6\}$, $\Phi_2^l = \emptyset$, $\Lambda_2^s = \{\lambda_2, \lambda_3\}$,
$\Phi_3^s = \{\varphi_7\}$, $\Phi_3^l = \emptyset$, $\Lambda_3^s = \{\lambda_4, \lambda_5\}$,
$\Phi_4^s = \{\varphi_8\}$, $\Phi_4^l = \emptyset$, $\Lambda_4^s = \{\lambda_6\}$,

Φ_i	X^s						F_i
Σ_1	q_1	p_2	q_2	p_3	q_3	p_4	F_1
$\varphi_1 = \{e_2, e_5\}$	X	X					$\{f_2\}$
$\varphi_2 = \{e_1, e_3, e_4, e_5\}$	X						$\{f_1\}$
$\varphi_3 = \{e_1, e_2, e_3, e_4\}$	X	X					$\{f_1, f_2\}$
$\varphi_4 = \{e_1, e_3, ..., e_6\}$	X	X					$\{f_1\}$
$\lambda_1 = \{e_6\}$	X						

Σ_2	q_1	p_2	q_2	p_3	q_3	p_4	F_2
$\varphi_5 = \{e_8\}$		X	X	X			$\{f_4\}$
$\varphi_6 = \{e_7, e_9\}$	X	X	X				$\{f_3\}$
$\lambda_2 = \{e_{10}\}$		X					
$\lambda_3 = \{e_{11}\}$			X				

Σ_3	q_1	p_2	q_2	p_3	q_3	p_4	F_3
$\varphi_7 = \{e_{13}\}$				X	X	X	$\{f_5\}$
$\lambda_4 = \{e_{16}\}$					X		
$\lambda_5 = \{e_{12}, e_{14}, e_{15}\}$			X	X	X		

Σ_4	q_1	p_2	q_2	p_3	q_3	p_4	F_4
$\varphi_8 = \{e_{17}, e_{18}, e_{19}\}$					X	X	$\{f_6\}$
$\lambda_6 = \{e_{20}\}$						X	

Added to $\varphi_4 = \{e_1, e_3, e_4, e_5, e_6\} \in \Phi_1^l$, we found 165 global FMSO sets in Φ.

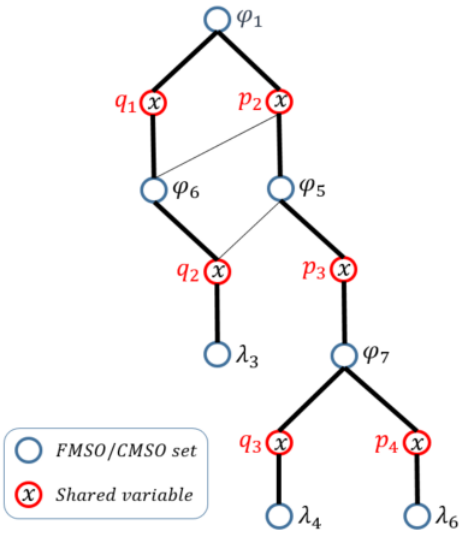


Figure 4: Subgraph of φ'.

6.2 Distributed Diagnosis

Given a set of faults, measurements and local models for every subsystem, we construct diagnosers that together make the entire system completely diagnosable. Using the Algorithm 2 and definitions of Section 4, we can develop a local full diagnosis for every subsystem. Computing the set of local FMSO sets Φ_i^l , $i = 1..4$ and adding subsets of shared variables to found the set of shared FMSO sets Φ_i^s for each subsystem $i = 1..4$ in the model in Table 2, we found FMSO sets for all faults as it is shown in in Table 4.

Table 4: Optimal compound FMSO sets Φ_i^c, $(i = 1..4)$ for distributed diagnosis.

$\Phi_1^c = \{\varphi_9\}$	F_{Φ_1}
$\varphi_9 = \{e_2, e_5, e_6, e_{10}\}$	$F_{\varphi_9} = \{f_2\}$
$\Phi_2^c = \{\varphi_{10}, \varphi_{11}\}$	F_{Φ_2}
$\varphi_{10} = \{e_6, e_7, e_9, e_{10}, e_{11}\}$	$F_{\varphi_{10}} = \{f_3\}$
$\varphi_{11} = \{e_8, e_{10}, e_{11}, e_{13}, e_{16}, e_{20}\}$	$F_{\varphi_{11}} = \{f_4\}$
$\Phi_3^c = \{\varphi_{12}\}$	F_{Φ_3}
$\varphi_{12} = \{e_{11}, e_{12}, e_{13}, e_{14}, e_{15}, e_{16}, e_{20}\}$	$F_{\varphi_{12}} = \{f_5\}$
$\Phi_4^c = \{\varphi_{13}\}$	F_{Φ_4}
$\varphi_{13} = \{e_{16}, e_{17}, e_{18}, e_{19}, e_{20}\}$	$F_{\varphi_{13}} = \{f_6\}$

These results demonstrate that all considered faults can be detected and isolated, e.g. in Σ_1: detectability is achieved for f_1 using $\varphi_4 \in \Phi_i^l$ of Table 3 (not additional measurement is needed). For f_2, detectability is achieved obtaining a compound FMSO set $\varphi_9 \in \Phi_i^c$ lumping $\varphi_1 \in \Phi_1^s$ (as root FMSO set) with $\lambda_1 \in \Lambda_1^s$ and $\lambda_2 \in \Lambda_2^s$. Figure 5 shows a scheme of the proposed model based diagnosis for this system: the four subsystems with their physical interactions are represented on the left. On the right, each local diagnoser LD_i is rendered as a rectangle with selected FMSO sets. The arrows from the corresponding subsystem symbolize the direct measurement of local variables by the LD, while the arrows between the local diagnosers account for shared information necessary to complete local diagnosis.

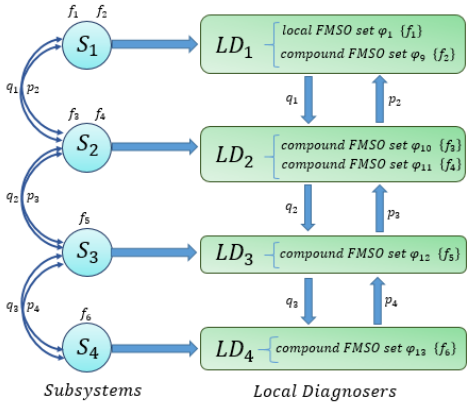


Figure 5: Scheme of the decentralized diagnosis designed.

7 Conclusion

In this paper, a distributed fault diagnosis method is presented. Distributed diagnosis is of interest for on-board systems as a way to reduce computational costs or for large geographically distributed systems that require to minimize data transfer. First, we introduce the Fault-Driven Minimal Structurally-Overdetermined (FMSO) set concept, which can be directly used to construct one ARR or residual generator, as compared to MTES that lead to several. We believe that FMSO sets represent a more practical solution in

distributed contexts in which communication must be minimized. The paper then provides the results that show that all the global FMSO sets, i.e. those that would be obtained along a centralized approach, can be obtained from computations performed at the level of local subsystems plus a search procedure. This is possible thanks to the concept of local FMSO set and shared FMSO/CMSO sets. The operational procedures for deriving in a distributed way all the global FMSO sets and a 'good' set of global FMSO sets are presented. These are illustrated with the four tanks benchmark.

We are currently pursuing our work on the optimization problem of generating a minimal cardinality set of compound FMSO sets that minimize subsystems interactions. The properties of the algorithm proposed in this paper, that is based on a heuristic, also need to be assessed. Thereby, we aim at obtaining optimal local diagnosers that guarantee the same properties as the global diagnosis.

References

[Armengol *et al.*, 2009] Joaquim Armengol, Anibal Bregón, Teresa Escobet, E Gelso, Mattias Krysander, Mattias Nyberg, Xavier Olive, Belarmino Pulido, and Louise Travé-Massuyès. Minimal structurally overdetermined sets for residual generation: A comparison of alternative approaches. In *Proceedings of the 7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, SAFEPROCESS09*, pages 1480–1485, 2009.

[Boem *et al.*, 2011] Francesca Boem, Riccardo M. G. Ferrari, and Thomas Parisini. Distributed fault detection and isolation of continuous-time non-linear systems. *European Journal of Control, Volume 17, Issues 5-6, 2011, Pages 603-620*, 2011.

[Bregon *et al.*, 2014] Anibal Bregon, Matthew Daigle, Indranil Roychoudhury, Gautam Biswas, Xenofon Koutsoukos, and Belarmino Pulido. An event-based distributed diagnosis framework using structural model decomposition. *Journal- Artif.Intell vol 210, pp. 1-35*, 2014.

[Debouk *et al.*, 2000] Rami Debouk, Stéphane Lafortune, and Demosthenis Teneketzis. Coordinated decentralized protocols for failure diagnosis of discrete event systems. *Discrete Event Dynamic Systems January 2000, Volume 10, Issue 1, pp 33-86*, 2000.

[Gertler, 1998] Janos Gertler. *Fault Detection and Diagnosis in Engineering Systems*. CRC Press, 1998.

[Grbovic, 2012] Mihajlo Grbovic. *Data Mining Algorithms for Decentralized Fault Detection and Diagnosis in Industrial Systems*. PhD thesis, Temple University Graduate Board, 2012.

[Khorasgani *et al.*, 2015] Hamed Khorasgani, Daniel Jung, and Gautam Biswas. Structural approach for distributed fault detection and isolation. In *9th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes SAFEPROCESS 2015, Volume 48, Issue 21, 2015, Pages 72-77*, 2015.

[Krysander *et al.*, 2010] Mattias Krysander, Jan Aslund, and Erik Frisk. A structural algorithm for finding testable sub-models and multiple fault isolability analysis. In *21st International Workshop on the Principles of Diagnosis*, 2010.

[Pencolé and Cordier, 2005] Yannick Pencolé and Marie-Odile Cordier. A formal framework for the decentralised diagnosis of large scale discrete event systems and its application to telecommunication networks. *Artificial Intelligence Volume 164, Issues 1-2, May 2005, Pages 121-170*, 2005.

[Pérez *et al.*, 2015] Carlos Gustavo Pérez, Louise Travé-Massuyès, Elodie Chanthery, and Javier Sotomayor. Decentralized diagnosis in a spacecraft attitude determination and control system. *Journal of Phys: Conf Series, IOP Publishing, 2015, 659, <10.1088/1742-6596/659/1/012054>. <hal-01229097>*, 2015.

[Rami Debouk, 2000] Demosthenis Teneketzis Rami Debouk, Stéphane Lafortune. Coordinated decentralized protocols for failure diagnosis of discrete event systems. *Discrete Event Dynamic Systems, January 2000, Volume 10, Issue 1, pp 33-86*, 2000.

[Su and Wonham, 2005] R. Su and W. M. Wonham. Global and local consistencies in distributed fault diagnosis for discrete-event systems. *IEEE Transactions on Automatic Control (Volume:50 , Issue: 12) pp 1923-1935 dec 2005*, 2005.

[Travé-Massuyès *et al.*, 2006] Louise Travé-Massuyès, Teresa Escobet, and Xavier Olive. Diagnosability analysis based on component-supported analytical redundancy relations. *IEEE Trans. Syst., Man, Cybern. Part A: Sys and Humans, VOL. 36, NO. 6, PP. 1146-1160, Nov. 2006*, 2006.