BRIDGE: Matching Model Based Diagnosis from FDI and DX perspectives

Louise Travé-Massuyès, Teresa Escobet

Fault Diagnosis of Dynamic Systems

Teresa Escobet

Anibal Bregon

Belarmino Pulido

Vicenç Puig

January 16, 2019

Contents

Part II ADVANCED APPROACHES

Chapter 7
BRIDGE: Matching Model Based Diagnosis from FDI and DX perspectives

Louise Travé-Massuyès and Teresa Escobet

7.1 Introduction

As introduced in Chapter 1, the goal of diagnosis is to identify the possible causes explaining a set of observed symptoms. The following three tasks are commonly identified:

- *fault detection* discriminates normal system states from faulty states,
- *fault isolation*, also called *fault localization*, points at the faulty components,
- *fault identification*, identifies the type of fault.

Several scientific communities have addressed these tasks and contributed with a large spectrum of methods, in particular the Signal Processing, Control, and Artificial Intelligence (AI) communities. Diagnosis spreads from the signal acquisition level up to levels in which relevant abstractions are used to interpret the available signals qualitatively.

Qualitative interpretations of the signals exist in terms of symbols or events. To do that, discrete formalisms borrowed from AI find a natural link with continuous models from the Control community. Different facets of diagnosis investigated in the Control or the AI fields have been discussed in the literature. [24–26] provide three interesting surveys of the different approaches that exist in these fields. These two communities have their own model-based diagnosis track:

- the FDI (Fault Detection and Isolation) track, whose foundations are based on engineering disciplines, such as control theory and statistical decision making,

Louise Travé-Massuyès
LAAS-CNRS, Université de Toulouse, CNRS, Toulouse, France, e-mail: louise@lass.fr

Teresa Escobet
Department of Mining, Industrial and ICT Engineering; Research Center for Supervision, Safety and Automatic Control, Universitat Politècnica de Catalunya, e-mail: teresa.escobet@upc.edu

- the DX (Diagnosis) track, whose foundations are derived from the fields of logic, combinatorial optimization, search and complexity analysis.

There has been a growing number of researchers in both communities who have tried to understand and bridge FDI and DX approaches to build better, more robust and effective diagnostic systems. In particular, the concepts and results of the FDI and DX tracks have been put in correspondence and the lessons learned from this comparative analysis pointed out.

The FDI and DX streams both consider the diagnosis problem from a *system* point of view, which results in significant overlaps. Even the name of the two tracks are the same : *Model-Based Diagnosis* (MBD). This chapter presents and examines this "bridge".

The diagnosis principles are the same, although each community has developed its own concepts and methods, guided by different modeling paradigms and solvers. FDI relies on analytical models, linear algebra, and non-linear system theory whereas DX takes its foundations in logic.

In the 2000s, although the common goals were quite clear, the underlying concepts and the procedures of the two fields would remain mutually obscure. There were more and more researchers who tried to understand and synergistically integrate methods from the two tracks to propose more efficient diagnostic solutions.

The chapter is organized as follows. After the introduction section, section 7.2 first presents a brief overview of the approaches proposed by the FDI and DX model-based diagnosis communities. Although quite commonplace, this overview is necessary because it provides the basic concepts and principles that form the foundations of our comparative analysis. It is followed by the comparison of the mathematical objects used as input of the diagnosis procedures. Section 7.3 then establishes the correspondances of concepts on both sides and compares the techniques used by the two communities. Interestingly, the results obtained by the two approaches are shown to be the same under some assumptions that are exhibited. Finally, Section 7.4 illustrates the DX-FDI MBD bridge with the classical example of the polybox.

7.2 DX and FDI MBD approaches

Both the FDI and DX communities have a Model-Based Diagnosis (MBD) track which can be put in correspondence. After a brief reminder of the concepts of the two tracks, this section compares the models used on each side and the sets the assumptions that are adopted to favor the comparative analysis.

7.2.1 Brief overview of the FDI approach

This section briefly summarizes the concepts presented in Chapter 3.6. The FDI community generally deals with dynamic systems represented by behavioral models

that relate system inputs $u \in \mathcal{U}$ and outputs $y \in \mathcal{Y}$, gathered in the set of measurable variables $\mathcal{Z}$, and system internal states defining the set of unknown variables $\mathcal{X}$. The variables $z \in \mathcal{Z}$ and $x \in \mathcal{X}$ are functions of time. The typical model can be formulated in the temporal domain, then known as a *state-space model* :

$$\begin{array}{l} BM : d\mathbf{x}/dt = f(\mathbf{x}(t), \mathbf{u}(t), \theta) \\ OM : \mathbf{y}(t) = g(\mathbf{x}(t), \mathbf{u}(t), \theta). \end{array} \tag{7.1}$$

where $\mathbf{x}(t) \in \Re^{n_x}$ is the state vector, $\mathbf{u}(t) \in \Re^{n_u}$ is the input vector and $\mathbf{y}(t) \in \Re^{n_y}$ is the output vector. Then $\mathbf{z}(t) = (\mathbf{u}(t), \mathbf{y}(t))^T$. $\theta \in \Re^{n_\theta}$ is a constant parameter vector. The components of f and g are real functions over $\Re$. *BM* is the behavioral model and *OM* is the observation model. The whole system model is noted $SM(\mathbf{z}, \mathbf{x})$, like in [13], and assumed noise-free. The equations of $SM(\mathbf{z}, \mathbf{x})$ may be associated to components but this information is not represented explicitly. The models can also be formulated in the frequency domain, for instance in the form of transfer functions in the linear case.

Model (7.1) can be illustrated by the example of two coupled water tanks T_t and T_b. T_t is the top tank and its output fills the bottom tank T_b:

$$BM : \begin{cases} \dot{x_1}(t) = a_1\, u(t) - a_2 \sqrt{x_1(t)}, \\ \dot{x_2}(t) = a_3 \sqrt{x_1(t)} - a_4 \sqrt{x_2(t)}, \end{cases} \tag{7.2}$$

$$OM : \begin{cases} y_1(t) = \sqrt{x_1(t)}, \\ y_2(t) = \sqrt{x_2(t)}. \end{cases} \tag{7.3}$$

where $a_i, i = 1, \ldots, 4$, $a_i \neq 0$, are model parameters. $\mathbf{x}(t) = (x_1(t), x_2(t))^T$ represents the state vector and corresponds to the level in each tank, $u(t) \not\equiv 0$ is the input vector, and $\mathbf{y}(t) = (y_1(t), y_2(t))^T$ is the output vector. Measurable variables are given by the vector $\mathbf{z}(t) = (u(t), y_1(t), y_2(t))^T$.

The books [10], [4], [8], [16] provide excellent surveys, which cite the original papers that the reader is encouraged to consult. The paper [26] also provides a quite comprehensive survey. The equivalence between observers, parity space and paramater estimation has been proved in the linear case [15].

The concept central to FDI methods is the concept of *residual* and one of the main problems is to *generate residuals*. Residual generators are defined in Definition 3.15 of Chapter 2.6 and this definition is recalled below.

Definition 7.1 (Residual generator for $SM(\mathbf{z}, \mathbf{x})$). A system that takes as input a sub-set of measured variables $\tilde{\mathcal{Z}} \subseteq \mathbf{z}$ and generates as output a scalar r, is a residual generator for the model $SM(\mathbf{z}, \mathbf{x})$ if for all z consistent with $SM(\mathbf{z}, \mathbf{x})$, $\lim_{t \to +\infty} r(t) = 0$.

Let's consider the model $SM(\mathbf{z}, \mathbf{x})$ given by (7.1), then $SM(\mathbf{z}, \mathbf{x})$ is said to be consistent with an observed trajectory $\mathbf{z}$, or simply *consistent with measurements* $\mathbf{z}$, if there exists a trajectory of $\mathbf{x}$ such that the equations of $SM(\mathbf{z}, \mathbf{x})$ are satisfied. The residuals tend to zero as t tends to infinity when the system model is consistent with measurements, otherwise some residuals may be different from zero. In practice, noises may affect the residuals that are never exactly *zero*. Indeed, the noise-free

assumption adopted for (7.1) is never met. Statistical tests that account for the statistical characteristics of noise [3, 8] are used to evaluate the residuals as a Boolean value 0 or 1. The residuals are often optimized to be robust to disturbances [18] and to take into account uncertainties [1]. The reader can refer to Chapter3.6 and 9.6 for more details about how to deal with uncertainty, using decoupling methods or with interval methods respectively.

Among the three standard FDI approches, the Bridge comparison is carried out based on the so-called parity space approach [5]. In this approach, residuals are generated from relations that are inferred from the system model by eliminating unknown variables, i.e. state variables. These relations, called *Analytical Redundancy Relations* (ARR), are determined off-line. ARRs are constraints that only involve measured input and output variables and their derivatives. For linear systems, ARRs are obtained eliminating unknown state variables by linear projection on a particular space, called the *parity pace* [5]. An extension to non-linear systems is proposed in [21]. On the other hand, structural analysis [2, 22] is an interesting approach because it allows one to obtain, for linear or non-linear systems, the just overdeterminated sets of equations from which ARRs can be derived (see 2.6).

Every ARR can be put in the form $r(t) = 0$, where $r(t)$ is the *residual*.

For the two tanks system (7.2)-(7.3), the two following residuals can be obtained from the Rosenfeld-Groebner algorithm as explained in [7]:

$$\begin{aligned} r_1(t) &= -a_1 u + a_2 y_1 + 2 y_1 \dot{y_1}, \\ r_2(t) &= a_4 y_2 - a_3 y_1 + 2 y_2 \dot{y_2}. \end{aligned} \tag{7.4}$$

If the behavior of the system satisfies the model constraints, then the residuals are zero because the ARRs are satisfied. Otherwise, some of them may be different from zero when the corresponding ARRs are violated. Given a set of n residuals, a *theoretical fault signature* $FS_j = [s_{1j}, s_{2j}, \ldots, s_{nj}]$ given by the Boolean evaluation of each residual is associated to each fault F_j. Note that F_j may be a simple or multiple fault. The *signature matrix* is then defined as follows.

Definition 7.2 (Signature Matrix). Given a set of n ARRs, the signature matrix FS associated to a set of n_f faults $\mathcal{F} = [F_1, F_2, \ldots, F_{n_f}]$ is the matrix that crosses corresponding residuals as rows and faults as columns, and whose columns are given by the theoretical signatures of the faults, i.e. $\mathcal{FS} = [FS_1, FS_2, \ldots, FS_{n_f}]$.

In the two tanks example system (7.2)-(7.3), let us consider a fault f_{T_b} on the bottom tank, i.e. a leak l_b, and a fault f_{T_t} on the top tank, i.e. a leak l_t. The leak l_b of the bottom tank impacts residual $r_1(t)$ whereas the leak l_t of the top tank impacts both residuals $r_1(t)$ and $r_2(t)$. The multiple fault composed of the two leaks obviously affects the two residuals as well. The signature matrix is hence given in Table 7.1.

Diagnosis is achieved by matching the observed signature, i.e. the Boolean residual values obtained from the actual measurements, to one of the theoretical signatures of the n_f faults.

Table 7.1 Fault signature of the two tanks system.

	f_{T_b}	f_{T_l}	$f_{T_b T_l}$
$r_1(t)$	1	1	1
$r_2(t)$	0	1	1

7.2.2 Brief overview of the DX logical diagnosis theory

In the model-based logical diagnosis theory of DX as proposed by [12, 19] and presented in depth in Chapter 4.5.2, the description of the system is driven by components and relies, in its original version, on first order logic. A system is given by a tuple $(SD, COMPS, OBS)$ where:

- SD is the *system description* in the form of a set of first order logic formulas with equality,
- $COMPS$ represents the *set of components* of the system given by a finite set of constants,
- OBS is a set of first order formulas, which represent the *observations*.

SD uses the specific predicate AB, meaning *abnormal*. Applied to a component c of $COMPS$, $\neg AB(c)$ means that c is normal and $AB(c)$ that c is faulty. For instance, the model of a two inputs adder would be given by:

$$\neg AB(x) \wedge ADD(x) \Rightarrow out(x) := in_1(x) + in_2(x) \tag{7.5}$$

Definition 7.3 (Diagnosis). A diagnosis for the system $(SD, COMPS, OBS)$ is a set $\Delta \subseteq COMPS$ such that $SD \cup OBS \cup \{AB(c) \mid c \in \Delta\} \cup \{\neg AB(c) \mid c \in OBS - \Delta\}$ is satisfiable.

The above definition means that the assumption stating that the components of Δ are faulty and all the others are normal is consistent with the observations OBS and the system description SD. A diagnosis hence consists in the assignment of a mode, normal or faulty [1], to each component of the system, which is consistent with the model and the observations.

Definition 7.4 (Minimal diagnosis). A *minimal diagnosis* is a diagnosis Δ such that $\forall \Delta' \subset \Delta$, Δ' is not a diagnosis.

To obtain the set of diagnoses, it is usual to proceed in two steps, basing the first step on the concept of introduced in [19] and later extended in [12]. The original definition, that we call *R-conflict*, i.e. conflict in the sense of Reiter, is the following :

Definition 7.5 (R-conflict and minimal R-conflict). An *R-conflict* is a set $\mathcal{C} \subseteq COMPS$ such that the assumption that all the components of $\mathcal{C}$ are normal is not consistent with SD and OBS. A *minimal R-conflict* is an R-conflict that does not contain any other conflict.

[1] This framework has been extended to fault models in [12].

The set of diagnoses can be generated from the set of conflicts. [19] proved that minimal diagnoses are given by the *hitting sets* [2] of the set of minimal R-conflicts. An algorithm based on the construction of a tree, known as the HS-tree, was originally proposed in [19].

The parsimony principle indicates that preference should be given to minimal diagnoses. Another reason why minimal diagnoses are important is because in many cases, they characterize the whole set of diagnoses. In other words, all the supersets of minimal diagnoses are diagnoses. The conditions for this to be true were provided in [12] by extending the definition of an R-conflict to a disjunction of AB-literals, $AB(c)$ or $\neg AB(c)$, containing no complementary pair, entailed by $SD \cup OBS$. Then, a *positive conflict* is a conflict for which all of its literals are positive and one can identify a with an R-conflict [19] as defined above.

Diagnoses are characterized by minimal diagnoses if and only if all minimal conflicts are positive [12]. Unfortunately, only sufficient conditions exist on the syntactic form of SD and OBS. One of those is that the clause form of $SD \cup OBS$ only contains positive AB-literals. This is verified, for instance, if all sentences of SD are of the same form as (7.5), which means that only necessary conditions of correct behavior are expressed.

7.2.3 Modeling comparison

Given the frameworks defined in Sections 7.2.1 and 7.2.2, it is important to compare the models that are used on both sides to represent the knowledge useful to diagnosis. Three dimensions can be analyzed:

- the system representation,
- observations,
- and, faults.

7.2.3.1 System reperesentation

The modeling paradigm of FDI does not make explicit use of the concept of component, the system model SM is composed of the behavior model BM and the observation model OM of the non faulty system. The behavioral model (7.1) describes the system as a whole. On the contrary, the DX approach models every component independently, and specifies the structure of the system, i.e. how the different components are connected. Another important difference is that the assumption of correct behavior is represented explicitly in SD thanks to the predicate AB. If $\mathcal{F}$ is a formula describing the normal behavior of a component, SM only contains $\mathcal{F}$ whereas SD contains the formula $\neg AB(c) \Rightarrow \mathcal{F}$.

[2] The hitting sets of a collection of sets are given by the sets that intersect every set of the collection.

The comparison of the two approaches is only possible if the models on both sides represent the same system and the observations/measurements capture the same reality. This is formalized by the *System Representation Equivalence* (SRE) property introduced in [6], which requires that *SM* is obtained from *SD* by setting to *false* all the occurrences of the predicate *AB*. It is also assumed that the same observation language is used, i.e. *OBS* is a conjunction of equality relations, which assign a value to every measured variable.

7.2.3.2 Observations

In DX, the set of observations expresses as a set of first-order formulas. It is hence possible to express disjunctions of observations, which provides a powerful language. However, very often, only conjunctions of atomic formulas are used. In FDI, the observations are always conjunctions of equalities assigning a real value and/or possibly an interval value to an observed variable. In the following, to favor the comparative analysis, we do assume that we have the same observation language. In both FDI and DX approaches, *OBS* is identical and made up of relations $OBS = \mathbf{z}$.

7.2.3.3 Faults

DX adopts a component-centered modeling approach and defines a diagnosis as a set of (faulty) components. In FDI the concept of component is not central. FDI represents faults as variables that are explicitly involved in the equations of *BM* and/or *OM* [9]. For deterministic models, fault variables can be associated:

- to parameters, indicating that the parameter changes value when the fault is present, in which case they are referred as *multiplicative faults*,
- to input and/or output variables, indicating actuators and sensors faults, in which case they are referred as *additive faults*.

FDI faults rather correspond to the DX concept of fault mode. In general, several parameters can be associated with a given component, giving rise to different fault modes. FDI faults are viewed as deviations with respect to the models of normal behavior whereas in the DX's logical view the faulty behavior cannot be predicted from the normal model.

The parameters of FDI models may not have straightforward physical semantics. The model developer must be able to link model parameters to physical parameters to perform fault isolation.

Note that the DX approach can account for parametric faults by expressing the model at a finer level. For instance, considering a single-input single-output (static) component c whose behavior depends on two parameters θ_1 and θ_2, the standard DX model given by:

$$COMPS(x) \wedge \neg AB(x) \Rightarrow out(x) = f(in(x), \theta_1, \theta_2) \tag{7.6}$$

could be replaced by:

$$\begin{aligned} COMPS(x) \wedge PARM1(y) \wedge PARM2(z) \wedge \neg AB(x) \wedge \neg AB(y) \wedge \neg AB(z) \Rightarrow \\ out(x) = f(in(x), y, z) \\ PARM1(\theta_1), PARM2(\theta_2), COMPS(c) \end{aligned} \tag{7.7}$$

The component-based DX approach can hence be generalized by allowing the set *COMPS* to include not only components (including sensors and actuators), but also parameters.

7.3 DX and FDI model-based diagnosis Bridge

This section provides the theoretical links and an analysis of the diagnosis results of the DX approach and the parity space FDI approach as presented in [6, 23]. Practical comparison and potential synergies are also discussed.

7.3.1 ARR vs. R-conflict

In the two approaches, diagnosis is triggered when discrepancies occur between the modeled (correct) behavior and the observations (*OBS*). As seen in Section 7.2, the detection of discrepancies corresponds to:

- R-conflicts in DX,
- ARRs that are not satisfied by *OBS* in FDI.

The fault signature matrix FS, as defined in Definition 7.2, can be used to explain the relation between R-conflicts and ARRs. FS crosses ARRs in rows and faults/-components in columns (here faults are univocally associated to components). The concept of *ARR Support* is also necessary.

Definition 7.6 (ARR Support). Consider ARR_i to be an ARR for $SM(\mathbf{z}, \mathbf{x})$, then the *support* of ARR_i, noted $supp(ARR_i)$, is the set of components $\{c_j\}$ (columns of the signature matrix FS) whose corresponding matrix cells FS_{ij} are non zero on the ARR_i line.

The support of an *ARR* of the form $r(\mathbf{z}, \dot{\mathbf{z}}, \ddot{\mathbf{z}}, \dots) = 0$ indicates the set of components whose models, or submodels, are involved in the obtention of the relation $r(\mathbf{z}, \dot{\mathbf{z}}, \ddot{\mathbf{z}}, \dots) = 0$. The equations of the model $SM(\mathbf{z}, \mathbf{x})$ can indeed be partitioned in component models and every equation of $SM(\mathbf{z}, \mathbf{x})$ can be labelled as being part of the model of some component. Let $SM(C)$ denote the subset of equations defining the model of a component $c \in COMPS$ and $SM(C) = \bigcup_{c \in C} SM(c)$ the subset of equations corresponding to $C \subseteq COMPS$.

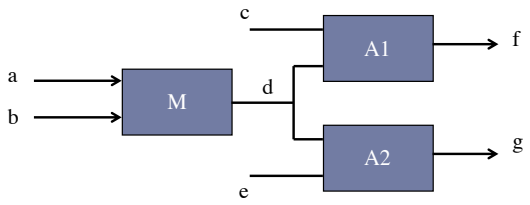

Fig. 7.1 Small polybox example.

Let us now introduce two completeness properties, which refer to *detectability* indicated by a *d*, and to *isolability* indicated by an *i*.

Property 7.1 (ARR–d–completeness). A set E of ARRs is said to be *d-complete* if:

- E is finite;
- $\forall OBS$, if $SM \cup OBS \models \perp$, then $\exists ARR_i \in E$ such that $\{ARR_i\} \cup OBS \models \perp$.

Property 7.2 (ARR–i–completeness). A set E of ARRs is said to be *i-complete* if:

- E is finite;
- $\forall C$, set of components such that $C \subseteq COMPS$, and $\forall OBS$, if $SM(C) \cup OBS \models \perp$, then $\exists ARR_i \in E$ such that $supp(ARR_i)$ is included in C and $\{ARR_i\} \cup OBS \models \perp$.

ARR–d–completeness and ARR–i–completeness express the theoretical capability of a set of ARRs to be sensitive, hence to detect, any inconsistency between the corresponding sub-model of *SM* and observations *OBS*.

Example 7.1. Consider the small polybox example represented in Figure 7.1.

The elementary components are one multiplier M, two adders A1 and A2 together with a set of sensors. The Behavioral Model *BM* is the following:

$$\begin{aligned} \text{M} &: d = a \times b \\ \text{A1} &: f = c + d \\ \text{A2} &: g = e + d \end{aligned} \tag{7.8}$$

All the variables are sensored but d. For the sake of simplicity, let us assume that sensor models are identity operators, then the Observation model *OM* is the following:

Table 7.2 Small polybox single fault signature matrix.

	f_{A1}	f_{A2}	f_M
$ARR1$	1	0	1
$ARR2$	0	1	1
$ARR3$	1	1	0

$$\begin{array}{r} \text{Sa} : a = a_{obs} \\ \text{Sb} : b = b_{obs} \\ \text{Sc} : c = c_{obs} \\ \text{Se} : e = e_{obs} \\ \text{Sf} : f = f_{obs} \\ \text{Sg} : g = g_{obs} \end{array} \tag{7.9}$$

We can easily obtain three ARRs for this simple system by following the paths between inputs and/or outputs.

$$\begin{array}{l} ARR1 : r_1 = 0 \text{ where } r_1 \equiv f_{obs} - a_{obs} \cdot b_{obs} - c_{obs} \\ ARR2 : r_2 = 0 \text{ where } r_2 \equiv g_{obs} - a_{obs} \cdot b_{obs} - e_{obs} \\ ARR3 : r_3 = 0 \text{ where } r_3 \equiv f_{obs} - g_{obs} - c_{obs} + e_{obs} \end{array} \tag{7.10}$$

Their supports are :

$$\begin{array}{c} supp(ARR1) = \{A1, M\} \\ supp(ARR2) = \{A2, M\} \\ supp(ARR3) = \{A1, A2\} \end{array} \tag{7.11}$$

Hence, the signature matrix for the set of single faults corresponding to components A1, A2, and M is given by Table 7.2.

We can notice that the set of ARRs composed of $ARR1$ and $ARR2$ seems to be sufficient to guaranty detectability and isolability of the three possible faults. As a matter of fact, $ARR3$ can be obtained by combining $ARR1$ and $ARR2$ (more precisely subtracting $ARR1$ and $ARR2$). The detectability power of $\{ARR1, ARR2\}$ is confirmed by the fact that this set is d-complete according to Property 1 defined above. However, let us now consider the following set of observations $OBS = \{a = 2, b = 3, c = 2, e = 2, f = 12, g = 10\}$ and the set of components $C = \{A1, A2\}$. Then, we have $SM(C) \cup OBS \models \perp$ but :

$$\begin{array}{c} supp(ARR1) = \{A1, M\} \not\subseteq C \\ supp(ARR2) = \{A2, M\} \not\subseteq C \end{array} \tag{7.12}$$

Hence the set of ARRs $\{ARR1, ARR2\}$ is not i-complete. This means that the isolability power of this set of ARRs is not maximal. For this simple example, this is easy to show by considering double faults.

Table 7.3 Small polybox double fault signature matrix for $c_i, c_j \in \{A1, A2, M\}, c_i \neq c_j$.

	f_{A1}	f_{A2}	f_M	$f_{c_i c_j}$
$ARR1$	1	0	1	1
$ARR2$	0	1	1	1
$ARR3$	1	1	0	1

Obviously, the set of ARRS $\{ARR1, ARR2\}$ does not differentiate any double fault from f_M and $ARR3$ turns to be useful for isolating the faults.

ARR–d–completeness and ARR–i–completeness are key to the comparison of the FDI and DX approaches. The main results can be summarized by the following proposition [6].

Proposition 7.1. *Assuming the SRE property and that OBS is the set of observations for the system given by SM (or SD), then :*

1. *If ARR_i is violated by OBS, then $supp(ARR_i)$ is an R-conflict;*
2. *If E is a d-complete set of ARRs, and if C is an R-conflict for $(SD, COMPS, OBS)$, then there exists $ARR_i \in E$ that is violated by OBS;*
3. *If E is an i-complete set of ARRs, then given an R-conflict C for $(SD, COMPS, OBS)$, there exists $ARR_i \in E$ that is violated by OBS and $supp(ARR_i)$ is included in C.*

The result 1 of Proposition 7.1 is intuitive and can be explained by the fact that the inconsistencies between the model and observations are captured by R-conflicts in the DX approach and by ARRs violated by *OBS* in the FDI approach. Consequently, the support of an ARR can be defined as a *potential R-conflict*. This concept is also called *possible conflict* in [17].

The results 2 and 3 of proposition 7.1 refer to fault detectability and fault isolability. The result 2 outlines the ARR–d–completeness property as the condition for *fault detectability*. From the result 3, the ARR–i–completeness property appears as the condition under which a formal equivalence between R-conflicts and ARR supports holds, as stated by the following corollary.

Corollary 7.1. *If both the SRE and the ARR–i–completeness properties hold, the set of minimal R-conflicts for OBS and the set of minimal supports of ARRs (taken in any i-complete set of ARRs) violated by OBS are identical.*

The detailed proofs of Proposition 7.1 and Corollary 7.1 can be found in [6].

7.3.2 Redundant ARRs

An important result coming from ARR–i–completeness refers to redundant ARRs. In FDI, it is generally accepted that if ARR_j is obtained from a linear combination of two other ARRs, ARR_{i_1} and ARR_{i_2}, then ARR_j is redundant (unless some

considerations about noises and sensitivity to faults come into play). Nevertheless the i-completeness property states that not only the analytical expression of ARR_j must be taken into account but also its support to conclude about the fact that it is redundant. The formal conditions are stated in the proposition below from [6].

Proposition 7.2. *A given ARR_j is redundant with respect to a set of ARR_is, $i \in I, j \notin I$, where I is a set of integer indexes such that $card(I) \geq 2$, if and only if $\exists I' \subseteq I$ such that :*

1) $\forall OBS$, if all ARR_is, $i \in I'$, are satisfied by OBS, then ARR_j is satisfied by OBS,

2) $supp(ARR_j) \supseteq supp(ARR_i)$, $\forall i \in I'$.

The above proposition can be explained by the fact that if $supp(ARR_j)$ does not satisfy condition 2, then it captures an inconsistency that is not captured by the initial ARR_is, $i \in I$. Added to the initial ARR_is, it hence contributes to the achievement of ARR–i–completeness.

Example 7.2. Let us consider the small polybox of Example 7.1, then $ARR3$ can be obtained as a linear combination of $ARR1$ and $ARR2$, however it is not redundant. This has already been shown by noticing that it is necessary to discrimitate any double fault from f_M. This can also be confirmed because it does not satisfy condition 2 of Proposition 7.2. Indeed, $supp(ARR3) = \{A1, A2\} \not\subseteq supp(ARR1) = \{A1, M\}$ and $supp(ARR3) = \{A1, A2\} \not\subseteq supp(ARR2) = \{A2, M\}$.

7.3.3 Exoneration assumptions

The exoneration assumptions, *ARR-exoneration* and *component-exoneration*, used by DX and FDI, respectively, are different.

Definition 7.7 (ARR-exoneration). Given *OBS*, any component in the support of an ARR satisfied by *OBS* is exonerated, i.e. considered as normal.

Definition 7.8 (Component-exoneration). Given *OBS* and $c \in COMP$, if $SM(c) \cup OBS$ is consistent, then c is exonerated, i.e. considered as normal.

The FDI approach generally uses the ARR-exoneration assumption without formulating it explicitly. On the other hand, the DX approach generally proceeds with no exoneration assumption at all. When this is not the case, it uses the component-exoneration assumption and represents it explicitly. If a component c is exonerated, its model is written as:

$$COMP(c) \wedge \neg AB(c) \Longleftrightarrow SM(c)$$

where the simple logical implication, found in (7.5) for instance, is replaced by a double implication. Explicit assumptions guarantee logical correctness of the DX diagnoses obtained by the DX method. Interestingly, *ARR-exoneration* cannot be expressed in the DX formalism and conversely, *component-exoneration* cannot be expressed in the FDI formalism.

It has been shown that under the same assumptions, in particular in the case of no exoneration, the diagnoses that are obtained by the DX and the FDI approach are the same [6].

Theorem 7.1. *Under the i-completeness and no exoneration assumptions, the diagnoses obtained by the FDI approach are identical to the (non empty) diagnoses obtained by the DX approach.*

7.3.4 Comparison in practice

Although diagnosis results have been shown to be the same with the DX and the FDI approach, the frameworks and procedures adopted by the two approaches have practical impacts. In particular, we can note the following two points:

- *Handling single and multiple faults*: in the FDI approach, because the fault signatures are determined off-line for every fault, the number of considered faults is generally limited. Most of the time, only single faults are considered. On the contrary, the DX approach naturally deals with multiple faults. A consequence is that the number of diagnoses is exponential and this is why it is common to introduce preference criteria, like fault probabilities, to order the diagnoses. Several search methods have been proposed to find the *preferred diagnoses* or to retrieve the diagnoses in preference order (see for instance [20, 29]).
- *Off-line versus on-line processing*: in the FDI approach, ARRs are determined off-line and only a simple consistency check is performed on-line. This may be quite relevant for real-time applications with hard temporal constraints. Inversely, in the DX approach, the whole diagnosis process is on-line, the advantage being that only the models need to be updated in case of any evolution of the system. The two approaches have been integrated to obtain the advantages of both: some DX works have used the idea of the FDI community to construct ARRs off-line [11, 14, 17, 28] and some FDI works have proposed to base the fault isolation phase on the conflicts derived from violated ARRs [27].

7.4 Case studies

7.4.1 Polybox case study

The comparison of the DX and FDI approach is first performed on the well know Polybox example.

7.4.1.1 FDI approach

The elementary components of the polybox example are the adders, A1 and A2, multipliers M1, M2 and M3 together with the set of sensors. The Behavioral Model *BM* is the following:

$$\begin{array}{c} \text{M1} : x = a \times c \\ \text{M2} : y = b \times d \\ \text{M3} : z = c \times e \\ \text{A1} : f = x + y \\ \text{A2} : g = y + z \end{array} \tag{7.13}$$

and the Observation Model *OM* assumes that sensor models are identity operators for the sake of simplicity :

$$\begin{array}{c} \text{Sa} : a = a_{obs} \\ \text{Sb} : b = b_{obs} \\ \text{Sc} : c = c_{obs} \\ \text{Sd} : d = d_{obs} \\ \text{Se} : e = e_{obs} \\ \text{Sf} : f = f_{obs} \\ \text{Sg} : g = g_{obs} \end{array} \tag{7.14}$$

The set of observations is for example $OBS = \{a_{obs} = 2, b_{obs} = 2, c_{obs} = 3, d_{obs} = 3, e_{obs} = 2, f_{obs} = 10, g_{obs} = 12\}$.

Three redundancy relations can be found :

$$\begin{array}{l} ARR1 : r_1 = 0 \text{ where } r_1 \equiv f_{obs} - a_{obs} \cdot c_{obs} - b_{obs} \cdot d_{obs} \\ ARR2 : r_2 = 0 \text{ where } r_2 \equiv g_{obs} - d_{obs} \cdot d_{obs} - c_{obs} \cdot e_{obs} \\ ARR3 : r_3 = 0 \text{ where } r_3 \equiv f_{obs} - g_{obs} - a_{obs} \cdot c_{obs} - c_{obs} \cdot e_{obs} \end{array} \tag{7.15}$$

*ARR*1, *ARR*2 and *ARR*3 are obtained from the models of {M1, M2, A1}, {M2, M3, A2} and {M1, M3, A1, A2}, respectively. If we assume that the sensors are not faulty, the ARRs can be written as:

Table 7.4 Polybox single fault signauture matrix.

	f_{A1}	f_{A2}	f_{M1}	f_{M2}	f_{M3}
$ARR1$	1	0	1	1	0
$ARR2$	0	1	0	1	1
$ARR3$	1	1	1	0	1

Table 7.5 Polybox double fault signature matrix.

	f_{A1}	f_{A2}	f_{M1}	f_{M2}	f_{M3}	f_{A1A2}	f_{A1M1}	f_{A1M2}	f_{A1M3}	f_{A2M1}	f_{A2M2}	f_{A2M3}	f_{M1M2}	f_{M1M3}	f_{M2M3}
$ARR1$	1	0	1	1	0	1	1	1	1	1	1	0	1	1	1
$ARR2$	0	1	0	1	1	1	0	1	1	1	1	1	1	1	1
$ARR3$	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1

Table 7.6 Polybox FDI diagnosis results for different observations signatures.

	OS				
$ARR1$	0	0	1	1	1
$ARR2$	0	1	0	1	1
$ARR3$	0	1	1	0	1
Single fault diagnoses	none	A2; M3	A1; M1	M2	none
Multiple fault diagnoses	none	(A2, M3)	(A1, M1)	none	All double faults but (A2, M3) and (A1, M1)

$$\begin{aligned} &ARR1: f-(a\cdot c+b\cdot d)=0\\ &ARR2: g-(b\cdot d+c\cdot e)=0\\ &ARR3: f-g-a\cdot c+c\cdot e=0 \end{aligned} \tag{7.16}$$

The signature matrix for the set of single faults corresponding to components A1, A2, M1, M2 and M3 in the case of component exoneration assumption defined in Definition 7.8, is given in Table 7.4.

The case of multiple faults can be dealt with by expanding the number of columns of the signature matrix, leading to a total number of 2^m-1 columns if all the possible multiple faults are considered.

The interpretation of multiple fault signature entries is the same as for single faults. Given the way multiple fault signatures are derived from single fault signatures, this interpretation implies that the simultaneous occurrence of several faults is not expected to lead to situations in which the faults compensate, resulting in the non-observation of the multiple fault. As it will be stated later more formally, this is known as the *multiple fault exoneration assumption*, which is a generalization of the exoneration assumption defined for single faults.

For different *observed signatures* (OS) formed by the observed residual vector $(r_1, r_2, r_3)^T$, the diagnosis results are summarized in Table 7.6 that resumes single and multiple fault signatures from Table 7.4 and Table 7.5.

Another interesting point to note is that, in the polybox example, the same diagnosis results would be obtained using the partial signature corresponding to ARR1 and ARR2 only in these three cases:

- $(r_1, r_2) = (0,0)$: no fault
- $(r_1, r_2) = (0,1)$: A2 or M3 faulty
- $(r_1, r_2) = (1,0)$: A1 or M1 faulty

In these three cases, the use of ARR3, associated with r_3, does not provide any more localization power. This is obviously not the case for the two last observed signatures (columns 5 and 6 of Table 7.6) for which r_3 is needed to disambiguate the signature $(r_1 = 1, r_2 = 1)$. It can be noticed that ARR3 was obtained from the combination of ARR1 and ARR2.

7.4.1.2 DX logical diagnosis approach

The system description is:

$$\begin{aligned}
COMPS &= \{\text{M1, M2, M3, A1, A2}\}\\
SD &= \{ADD(\text{c}) \wedge \neg AB(\text{c}) \Rightarrow Output(\text{c}) = Input1(\text{c}) + Input2(\text{c}),\\
&\quad MULT(\text{c}) \wedge \neg AB(\text{c}) \Rightarrow Output(\text{c}) = Input1(\text{c}) \times Input2(\text{c}),\\
&\quad MULT(\text{M1}), MULT(\text{M2}), MULT(\text{M3}), ADD(\text{A1}), ADD(\text{A2}),\\
&\quad Output(\text{M1}) = Input1(\text{A1}), Output(\text{M2}) = Input2(\text{A1}),\\
&\quad Output(\text{M2}) = Input1(\text{A2}), Output(\text{M3}) = Input2(\text{A2})\},\\
&\quad \text{for c} \in COMPS\\
OBS &= \{Input1(\text{M1}), Input2(\text{M1}), Input1(\text{M2}), Input2(\text{M2}),\\
&\quad Input1(\text{M3}), Input2(\text{M3}), Output(\text{A1}), Output(\text{A2})\}
\end{aligned}$$

Suppose the polybox is given the inputs $a = 2$, $b = 2$, $c = 3$, $d = 3$, $e = 2$, and it outputs $f = 10$, $g = 12$ in response. The set of observations is represented by:

$$\begin{aligned}
OBS = \{&Input1(M1) = 2, Input2(M1) = 3, Input1(M2) = 2, Input2(M2) = 3,\\
&Input2(M3) = 2, Output(A1) = 10, Output(A2) = 12\}.
\end{aligned}$$

The polybox with the observations as seen above ($f = 10$, $g = 12$) has the following minimal R-conflicts: $\{A1, M1, M2\}$ and $\{A1, A2, M1, M3\}$ due to the abnormal value of 10 for f. Symmetrically, $f = 12$ and $g = 10$ yield $\{A2, M2, M3\}$ and $\{A1, A2, M1, M3\}$. In the case $f = 10$ and $g = 10$, the two minimal R-conflicts are: $\{A1, M1, M2\}$ and $\{A2, M2, M3\}$. In the case $f = 10$ and $g = 14$, the three minimal R-conflicts are: $\{A2, M2, M3\}$, $\{A1, M1, M2\}$, and $\{A1, A2, M1, M3\}$.

The corresponding minimal diagnoses are presented in Table 7.7.

7.4.1.3 Bridge

Releasing the exoneration assumption in the polybox example leads to the single fault signature matrix shown in Table 7.8 and to the extended fault signature matrix

Table 7.7 Polybox DX diagnosis results for different observation signatures.

	OBS				
f =	12	12	10	10	10
g =	12	10	12	10	14
Minimal R-conflicts	none	{A2, M2, M3} {A1, A2, M1, M3}	{A1, M1, M2} {A1, A2, M1, M3}	{A1, M1, M2} {A2, M2, M3}	{A1, M1, M2} {A1, A2, M1, M3} {A2, M2, M3}
Minimal diagnoses	{}	{A2} {M3} {A1, A2} {M1, M2}	{A1} {M1} {A2, M2} {M2, M3}	{M2} {A1, A2} {A1, M3} {M1, M3} {M1, M3}	All double faults but (A2, M3) and (A1, M1)

Table 7.8 Polybox single faults without exoneration.

	f_{A1}	f_{A2}	f_{M1}	f_{M2}	f_{M3}
$ARR1$	×	0	×	×	0
$ARR2$	0	×	0	×	×
$ARR3$	×	×	×	0	×

Table 7.9 Polybox double faults signature matrix.

	f_{A1}	f_{A2}	f_{M1}	f_{M2}	f_{M3}	f_{A1A2}	f_{A1M1}	f_{A1M2}	f_{A1M3}	f_{A2M1}	f_{A2M2}	f_{A2M3}	f_{M1M2}	f_{M1M3}	f_{M2M3}
$ARR1$	×	0	×	×	0	×	×	×	×	×	×	0	×	×	×
$ARR2$	0	×	0	×	×	×	0	×	×	×	×	×	×	×	×
$ARR3$	×	×	×	0	×	×	×	×	×	×	×	×	×	×	×

presented in Table 7.9. These are obtained from the standard ones (see Table 7.4 and and 7.5) by replacing 1's by ×'s, which allows these entries to be matched with 0 or 1 in the observed signature. Note that all signatures of triple faults and more are equal to $(\times, \times, \times)^T$).

The following results are then obtained:

- With outputs f = 12 and g = 10, i.e. observed signature (0,1,1), there are 4 minimal diagnoses: 2 single fault diagnoses {A2} and {M3} and 2 double fault diagnoses {A1, A2} and {M1, M1}, and 22 superset diagnoses.
- With outputs f = 10 and g = 12, i.e. observed signature (1,0,1), there are 4 minimal diagnoses: 2 single fault diagnoses {A1} and {M1} and 2 double fault diagnoses {A2, M2} and {M2, M3}, and 22 superset diagnoses.
- With outputs f = 10 and g = 10, i.e. observed signature (1,1,0), there are 5 minimal diagnoses: one single fault diagnosis {M2} and 4 double fault diagnoses {A1, A2}, {A1, M3}, {M1, A2} and {M1, M3}, and 20 superset diagnoses.
- With outputs f = 10 and g = 14, i.e. observed signature (1,1,1), there are 8 minimal double fault diagnoses: {A1, A2}, {A1, M2}, {A1, M3}, {A2, M1}, {A2, M2}, {M1, M2}, {M1, M3} and {M2, M3}, and 16 superset diagnoses.

These results obtained by FDI are identical to those obtained by DX (see Table 7.7). In the case where f = 12 and g = 12, i.e. observed signature (0,0,0), the empty subset is a minimal diagnosis according to DX and any non empty subset of

components is a diagnosis according to both approaches: there are 5 minimal single fault diagnoses and 26 superset diagnoses. The only difference between FDI and DX is that, the "no-fault" column of signature (0,0,0) which would correspond to the empty diagnosis subset is left implicit in the signature matrix.

It can be noticed that, except in the $f = 10$ and $g = 14$ case (where anyhow, no exoneration can apply as no ARR is satisfied), the results are different from those obtained under the default exoneration assumption (see Table 7.6).

7.4.2 Three-tanks case study

For this case study, we use the FDI approach to derive ARRs, then apply the Bridge result to obtain the DX counterpart results.

The system (cf. 2.2) is made up of three identical tanks T_1, T_2, T_3. All three tanks have the same physical features such as height and cross sectional area, A. There is a measured input flow q_i for tank T_1, which is drained into T_2 via a pipe q_{12}. A similar process gets the flow from T_2 to T_3 via pipe q_{23}. Finally, there is an output flow q_{30} from T_3. The system has three sensors measuring the level in thanks T_1 and T_3 (level transducers $LT1$ and $LT2$, respectively), and another sensor measuring the flow through pipe q_{23} (flow transducer $FT1$).

Adopting the FDI approach, the following three dynamic system equations model the normal behavior of the system. The change in the level in each tank, $\dot{h}_{T_i}$, is computed according to mass balances:

$$
\begin{aligned}
e1_n &: \dot{h}_{T_1} = \frac{q_i - q_{12}}{A}, \\
e2_n &: \dot{h}_{T_2} = \frac{q_{12} - q_{23}}{A}, \\
e3_n &: \dot{h}_{T_3} = \frac{q_{23} - q_{30}}{A}.
\end{aligned}
$$

Flows between tanks q_{12}, q_{23}, q_{30} are modeled as:

$$
\begin{aligned}
e4_n &: q_{12} = S_{p_1} \cdot \text{sign}(h_{T_1} - h_{T_2}) \cdot \sqrt{2g \mid h_{T_1} - h_{T_2} \mid}, \\
e6_n &: q_{23} = S_{p_2} \cdot \text{sign}(h_{T_2} - h_{T_3}) \cdot \sqrt{2g \mid h_{T_2} - h_{T_3} \mid}, \\
e8_n &: q_{30} = S_{p_3} \cdot \sqrt{2g \cdot h_{T_3}},
\end{aligned}
$$

being S_{p_i}, $i = 1, \ldots, 3$, the cross sectional area of the pipes. The relation between the state variables, h_{T_i}, and their derivatives $\dot{h}_{T_i}$ are given by:

$$
e13 : h_{T_1} = \int \dot{h}_{T_1} \cdot dt,
$$

$$e14 : h_{T_2} = \int \dot{h}_{T_2} \cdot dt,$$
$$e15 : h_{T_3} = \int \dot{h}_{T_3} \cdot dt.$$

The above nine equations form the behavioral model *BM*.

The observational model *OM* is given by the following equations:

$$e10 : h_{T_1,obs} = h_{T_1},$$
$$e11 : h_{T_3,obs} = h_{T_3},$$
$$e12 : q_{23,obs} = q_{23}.$$

Six possible faults are considered: three tank leakages and three pipe blockages as presented in Section 2.2.

To obtain ARRs, we can use the structural analysis approach as presented in Section 3.4.3 or the possible conflicts approach as presented in Section 6.1.1. Three ARRs are obtained from the three equation sets below:

$$\{\ (e3_n)(e8_n)(e11)(e12)(\mathrm{e}15)\ \},$$
$$\{\ (e2_n)\ (e4_n)\ (e6_n)(e10)\ (e11)(e12)\ (e14)\},$$
$$\{(e1_n)\ (e4_n)\ (e6_n)\ (e10)\ (e11)(e12)\ (e13)\}.$$

The fault signature matrix with and without exoneration are given in Table 7.10 and in Table 7.11 respectively, where f_{T_i} represents a leakage at the bottom of tank T_i, $i = 1, \ldots, 3$, and $f_{P_{jk}}$ represents a stuck closed fault on the pipe connecting tank T_j and tank T_k or the atmosphere, $i = 1, \ldots, 3$, $k \in \{2, 3, 0\}$.

Table 7.10 Three tanks fault signature matrix.

	f_{T_1}	f_{T_2}	f_{T_3}	$f_{P_{12}}$	$f_{P_{23}}$	$f_{P_{30}}$
$ARR1$	0	0	1	0	0	1
$ARR2$	0	1	0	1	1	0
$ARR3$	1	0	0	1	1	0

Table 7.11 Three tanks fault signature matrix without exoneration.

	f_{T_1}	f_{T_2}	f_{T_3}	$f_{P_{12}}$	$f_{P_{23}}$	$f_{P_{30}}$
$ARR1$	0	0	×	0	0	×
$ARR2$	0	×	0	×	×	0
$ARR3$	×	0	0	×	×	0

Assume that the observed signature is $(0, 0, 1)^T$ then by item 1 of Proposition 7.1, we know that $\{T_1, P_{12}, P_{30}\}$ is an R-conflict.

If we use the standard FDI approach and the fault signature matrix of Table 7.10, f_{T_1} is the only fault signature that can be matched. So we get one unique diagnosis $\Delta = \{T_1\}$.

On the other hand, the DX approach can obtain the diagnoses as the hitting sets of the R-conflicts [19]. In this case, we have one single R-conflict $\{T_1, P_{12}, P_{30}\}$, which indicates that three minimal diagnoses are $\Delta_1 = \{T_1\}$, $\Delta_2 = \{P_{12}\}$, and $\Delta_3 = \{P_{30}\}$. This result seems in contradiction with the result obtained with the standard FDI approach. However, let us now apply the FDI approach by relaxing the ARR-exoneration assumption.

If we now use the FDI approach with no ARR-exoneration, the fault signature matrix of Table 7.11 must be considered. Given that a "$\times$" entry can be matched to "0" or "1" in the observed signature, not only f_{T_1} but also $f_{P_{12}}$ and $f_{P_{30}}$ can be matched. The diagnosis results are hence the same as for the DX approach, exemplifying Theorem 7.1.

Assume now that the observed signature is $(1,1,0)^T$ then by item 1 of Proposition 7.1, we know that $\{T_3, P_{30}\}$ and $\{T_2, P_{12}, P_{23}\}$ are R-conflict.

If we use the FDI approach with (cf. Table 7.10) or without ARR-exoneration (cf. 7.11), no fault signature matches the observed signature.

On the other hand, if we obtain the diagnoses from the two R-conflicts following the DX approach, we obtain six minimal diagnoses $\Delta_1 = \{T_3, T_2\}$, $\Delta_2 = \{T_3, P_{12}\}$, $\Delta_3 = \{T_3, P_{23}\}$, $\Delta_4 = \{T_2, P_{30}\}$, $\Delta_5 = \{P_{30}, P_{12}\}$, and $\Delta_6 = \{P_{30}, P_{23}\}$. As a matter of fact, all of them are double fault diagnoses. This is the reason why they could not be found with the single fault signature matrix. Interestingly, the DX approach handles single and multiple faults in the same framework while the FDI approach requires to generate the extended fault signature matrix.

7.5 Conclusions

In this chapter, the FDI approach based on ARRs and the DX logical approach have been compared and the hypotheses underlying the two approaches have been clearly stated. The concepts on both sides have been bridged and it has been shown that the two approaches provide the same diagnosis results under some assumptions referring to exoneration. The classical polybox and the three tanks case studies have been used to illustrate the MBD Bridge from which potential synergies are possible.

The links and the understanding of the MBD Bridge provide sound ground for merging the best of both worlds and producing ever better diagnosers for real complex systems.

References

[1] Adrot, O., Maquin, D., Ragot, J.: Fault detection with model parameter structured uncertainties. In: Proceedings of the European Control Conference, ECC'99. Karlsruhe (1999)

[2] Armengol, J., Bregon, A., Escobet, T., Gelso, E., Krysander, M., Nyberg, M., Olive, X., Pulido, B., Travé-Massuyès, L.: Minimal Structurally Overdetermined sets for residual generation: A comparison of alternative approaches. Proceedings of the 7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, Safeprocess'09 (2009)
[3] Basseville, M., Nikiforov, I.: Detection of abrupt changes: theory and application. Citeseer (1993)
[4] Blanke, M., Kinnaert, M., Lunze, J., Staroswiecki, M.: Diagnosis and fault-tolerant control. Springer Verlag (2003)
[5] Chow, E., Willsky, A.: Analytical redundancy and the design of robust failure detection systems. IEEE Transactions on automatic control **29**(7), 603–614 (1984)
[6] Cordier, M., Dague, P., Lévy, F., Montmain, J., Staroswiecki, M., Travé-Massuyès, L.: Conflicts versus analytical redundancy relations: a comparative analysis of the model based diagnosis approach from the artificial intelligence and automatic control perspectives. IEEE Transactions on Systems, Man, and Cybernetics, Part B **34**(5), 2163–2177 (2004)
[7] Denis-Vidal, L., Joly-Blanchard, G., Noiret, C.: Some effective approaches to check the identifiability of uncontrolled nonlinear systems. Mathematics and computers in simulation **57**(1-2), 35–44 (2001)
[8] Dubuisson, B.: Automatique et statistiques pour le diagnostic. Hermes Science Europe Ltd (2001)
[9] Gertler, J.: Analytical redundancy methods in failure detection and isolation. In: Preprints of the IFAC SAFEPROCESS Symposium, pp. 9–21 (1991)
[10] Gertler, J.: Fault Detection and Diagnosis in Engineering Systems. Marcel Deker (1998)
[11] Katsillis, G., Chantler, M.: Can dependency-based diagnosis cope with simultaneous equations. In: Proceedings of the 8th International Workshop on Principles of Diagnosis DX-97, pp. 51–59 (1997)
[12] Kleer, J., Mackworth, A., Reiter, R.: Characterizing diagnoses and systems. Artificial Intelligence **56**(2-3), 197–222 (1992)
[13] Krysander, M., Aslund, J., Nyberg, M.: An efficient algorithm for finding minimal overconstrained subsystems for model-based diagnosis. IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans **38**(1), 197–206 (2008)
[14] Loiez, E., Taillibert, P.: Polynomial temporal band sequences for analog diagnosis. In: Proceedings of the Fifteenth International Joint Conference on Artificial Intelligence IJCAI-97, Nagoya, Japan, August 23-29, 1997, p. 474 (1997)
[15] Patton, R., Chen, J.: A re-examination of the relationship between parity space and observer-based approaches in fault diagnosis. European Journal of Diagnosis and Safety in Automation **1**(2), 183–200 (1991)
[16] Patton, R., Frank, P., Clark, R.: Fault diagnosis in dynamic systems. Theory and Applications (1989)

[17] Pulido, B., Gonzalez, C.: Possible conflicts: A compilation technique for consistency-based diagnosis. IEEE Transactions on Systems, Man, and Cybernetics - Part B: Cybernetics **34**(5), 2192–2206 (2004)
[18] Qiu, Z., Gertler, J.: Robust FDI and $H_{\inf}$ optimization. In: Proceedings of the 32nd IEEE Conference on Control and Decision CDC'93. San Antonio, Texas (1993)
[19] Reiter, R.: A theory of diagnosis from first principles. Artificial Intelligence **32**(1), 57–95 (1987)
[20] Sachenbacher, M., Williams, B.: Diagnosis as semiring-based constraint optimization. In: Proceedings of the European Conference on Artificial Intelligence ECAI'04, vol. 16, p. 873 (2004)
[21] Staroswiecki, M., Comtet-Varga, G.: Analytical redundancy relations for fault detection and isolation in algebraic dynamic systems. Automatica **37**(5), 687–699 (2001)
[22] Staroswiecki, M., Declerck, P.: Analytical redundancy in non linear interconnected systems by means of structural analysis. In: Proceedings of the IFAC Symposium on Advanced Information Processing in Automatic Control, pp. 51–55 (1989)
[23] Travé-Massuyès, L.: Bridging control and artificial intelligence theories for diagnosis: A survey. Engineering Applications of Artificial Intelligence **27**, 1–16 (2014)
[24] Venkatasubramanian, V., Rengaswamy, R., Kavuri, S.N.: A review of process fault detection and diagnosis part ii: Qualitative models and search strategies. Computers and Chemical Engineering **27**(3), 313–326 (2003)
[25] Venkatasubramanian, V., Rengaswamy, R., Kavuri, S.N., Yin, K.: A review of process fault detection and diagnosis part iii: Process history based methods. Computers and Chemical Engineering **27**(3), 327–346 (2003). DOI 10.1016/S0098-1354(02)00162-X-a3
[26] Venkatasubramanian, V., Rengaswamy, R., Yin, K., Kavuri, S.N.: A review of process fault detection and diagnosis part i: Quantitative model-based methods. Computers and Chemical Engineering **27**(3), 293–311 (2003)
[27] Vento, J., Puig, V., Sarrate, R., Travé-Massuyès, L.: Fault detection and isolation of hybrid systems using diagnosers that reason on components. IFAC Proceedings Volumes **45**(20), 1250–1255 (2012)
[28] Washio, T., Motoda, H., Niwa, Y., INSS, I.: Discovering Admissible Model Equations from Observed Data. In: Proceedings of the 16th International Joint Conference on Artificial Intelligence IJCAI'99, vol. 2, pp. 772–779. Citeseer (1999)
[29] Williams, B., Ragno, R.: Conflict-directed A* and its role in model-based embedded systems. In: Journal of Discrete Applied Mathematics. Citeseer (2003)