ELSEVIER

PII: S0954-1810(97)10010-3

Artificial Intelligence in Engineering **12** (1998) 355–373

0954-1810/98/$19.00

Introducing deviations and multiple abstraction levels in the functional diagnosis of fluid transfer systems

Luca Chittaro[a,*], Roberto Ranon[a] & Alfredo Soldati[b]

[a]*Department of Mathematics and Computer Science, Università di Udine, Via delle Scienze 206, 33100 Udine, Italy*
[b]*Department of Chemical Science and Technology, Università di Udine, Via Cotonificio 108, 33100 Udine, Italy*

We have recently experimented the FDef (Functional Diagnosis with efforts and flows) approach on a real-world problem[1] (Chittaro, L., Fabbri, R. and López Cortés, J. Functional diagnosis goes to the sea: applying FDef to the heavy fuel oil transfer system of a ship. In *Proceedings of FLAIRS-96*, Key West, FL, USA. Florida Artificial Intelligence Research Society, 1996, pp. 419–423), i.e. the diagnosis of multiple faults in the heavy fuel oil transfer system (HFOTS) of a modern container ship. This paper builds on that preliminary work, extending it in several directions by: (i) analysing its limitations; (ii) generalizing the proposed techniques from the specific HFOTS case to a wide class of hydraulic systems in the domain of Fluid Transfer Systems; (iii) significantly increasing the diagnostic capabilities of the approach by introducing representation and reasoning about deviations from nominal values; (iv) adopting a hierarchical organization for representing the functional model to improve efficiency and to reason at multiple levels of abstraction; and (v) providing a formal validation of the employed diagnostic knowledge. © 1998 Elsevier Science Limited. All rights reserved.

Key words: diagnosis, functional reasoning, model-based reasoning, functional modeling, fluid transfer systems, hydraulic systems.

1 INTRODUCTION

Reasoning about function for diagnostic purposes has been recently investigated by several research groups.[2–8] As a result, the exploitation of functional knowledge is gaining a growing attention in model-based diagnosis. Nevertheless, a lot of work has still to be done on the functional diagnosis of real complex systems.

In this paper, we adopt one of the flow-based approaches[6,8,9] to represent function, with the aim of applying it to the diagnosis of a wide class of hydraulic engineering systems, i.e. Fluid Transfer Systems (FTS). The specific functional representation we adopt is the one proposed by the Multimodeling approach.[9]

As a significant example of a real-world FTS application, we consider the diagnosis of multiple faults in the heavy fuel oil transfer system (HFOTS) of a modern container ship. This system is a representative example in the domain of marine technical systems,[10] which are characterized by their (i) high structural complexity in terms of number of components and possible interactions, (ii) high number of possible combinations of normal operating modes of components, and (iii) exploitation of a few different types of basic components appearing in various parts of the system.

In Section 2, we present the FTS domain, the HFOTS application, and the relevant classes of faults to be identified. Section 3 motivates the research, presents a brief overview of the initial FDef approach, and illustrates the first experiments made with it on the HFOTS case study. The results of the experiments are critically discussed in Section 4, which also motivates our proposal of an improved FDef approach. Sections 5–8 present in detail the novel FDef approach in a self-contained way, without requiring familiarity with the previous FDef reasoning technique. The new approach allows us to (i) generalize the application from the specific HFOTS case to a wide class of hydraulic systems in the FTS domain; (ii) significantly increase diagnostic power by representing and reasoning about deviations from nominal values; (iii) improve efficiency and permit reasoning at multiple levels of abstraction by adopting a proper hierarchical organization for the functional model; and (iv) provide a formal validation of the employed diagnostic knowledge. In Section 9, we discuss the new FDef

*Author to whom correspondence should be addressed. E-mail: chittaro@dimi.uniud.it

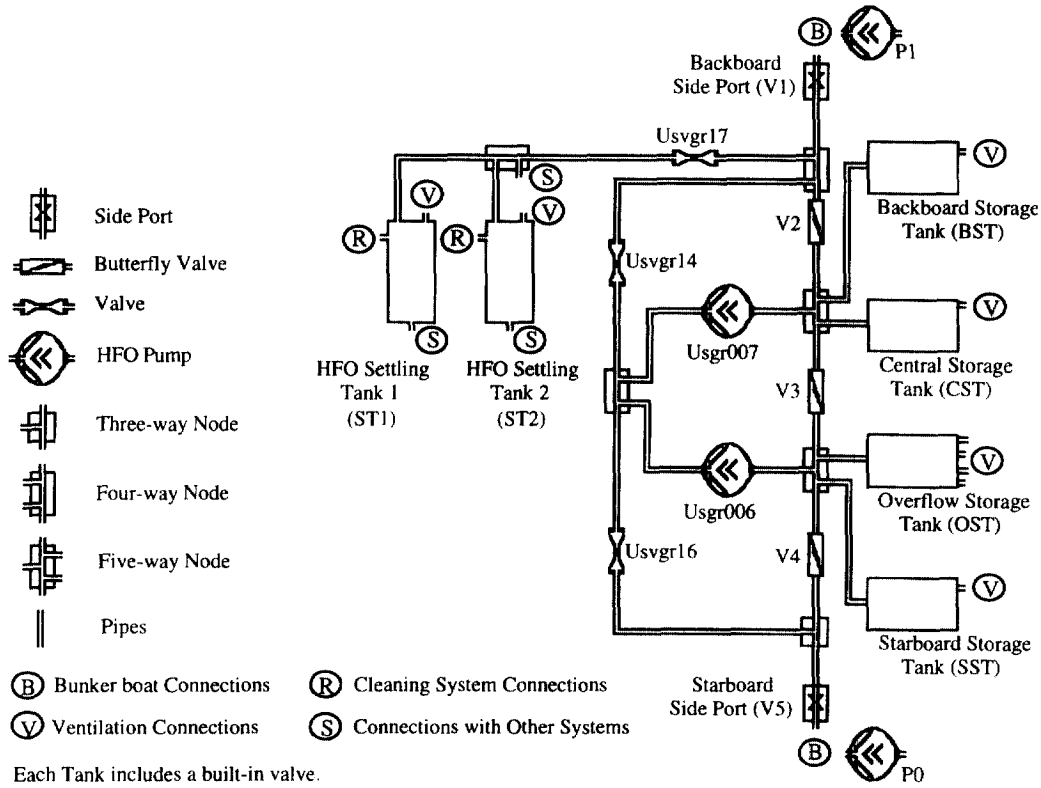

Fig. 1. Schematic of the HFOTS [1].

approach in relation to its previous version and to more traditional model-based diagnosis approaches. Finally, Section 10 concludes the paper sketching current and future research work.

2 THE PROBLEM: DIAGNOSIS OF MULTIPLE FAULTS IN FLUID TRANSFER SYSTEMS

Fluid Transfer Systems (FTS) are a class of engineering systems widely found in many industrial and civil applications. In the civil sector, they range from water ducts to sewage systems; in the industrial sector, they range from gas or oil or water transport pipelines to fluid transport rigs in process industries. Therefore, the development of general fault diagnosis techniques for FTS is undoubtedly relevant for a wide number of applications.

The main classes of components used in FTS are pumps, pipes, valves, and tanks. In this paper, we consider the most likely classes of faults in FTS:

- obstructions (which may affect pipes and open valves);
- external leaks (which may affect any component);
- internal leaks (which may affect closed valves);
- stuck components (valves stuck at close or open, pumps that do not rotate);
- wrong flow rate delivery (which may affect pumps).

We consider a wide class of pumps, i.e. positive displacement (volumetric) pumps. The characteristic behavior of a volumetric pump is to deliver the same flow rate independently of the pressure drop across it. It is normal practice to have only one of these pumps performing in the system: if the system contains several volumetric pumps, typically only one of them is active in a given configuration.

As a motivating real-world example of a significant FTS, we consider in the following the Heavy Fuel Oil Transfer System (HFOTS) of a ship, used to transfer heavy fuel oil from deck reservoirs or bunker boats to the ship on-board tanks, and to redistribute it among the tanks themselves.

2.1 A motivating example: the heavy fuel oil transfer system of a ship

Heavy fuel oil (HFO) is a low cost fuel used by main and auxiliary marine diesel engines. The low quality of HFO (high viscosity, low chemical stability, presence of undesired particles and salted water) makes it necessary to handle it properly (e.g. HFO can react and produce more stable subproducts which deposit as solids, or it can become solid under a certain temperature threshold). Three different subsystem are typically devoted to the handling of HFO on a ship: a transfer, a cleaning, and a supply system. We concentrate on the transfer system (HFOTS).

The HFOTS (Fig. 1) is devoted to the storage and transfer of HFO among tanks. The main components of the HFOTS are pumps, valves, tanks, and pipes (for clarity purposes, Fig. 1 shows the pipelines, without detailing each single pipe). Four tanks are devoted to the storage of HFO during refueling and two tanks are devoted to settling

down possible impurities such as solid particles and water. The HFOTS can work in several different modes, in order to achieve three different types of purposes: (i) *refueling*, by pumping oil from a bunker boat (through the external connections on backboard or starboard side) to one of the storage tanks (BST, CST, OST, SST), or to any combination of tanks simultaneously, exploiting the pump on the bunker boat (P0 or P1 in the figure); (ii) *transfering* fuel between any combination of tanks, including settling tanks (ST1 and ST2), exploiting the on-board pumps (Usgr006 and Usgr007); and (iii) *emptying* one or more tanks, exploiting the pump on the bunker boat or the on-board pumps.

The slow processes that take place as well as economical considerations have led designers to reduce the number of sensors in this type of systems to a minimum. In particular, the available observations on the considered HFOTS are:

- position of hydraulically driven valves (open/closed);
- operating signals of pump driving electrical motors (powered/not powered);
- pressure drop over transfer pumps;
- levels of tanks (from 0% to 100%);
- pressure drop at pipe C10 (between OST and valve V3).

3 USING FDEF FOR FUNCTIONAL MODELING AND DIAGNOSIS OF FLUID TRANSFER SYSTEMS

This section first motivates the adoption of a flow-based functional approach, then it provides a brief overview of FDef,[3] and describes how we model FTS using functional roles. Finally, it illustrates a full HFOTS diagnosis example.

3.1 Motivations

In general, the high complexity of behavioral models of FTS leads to explore the possibility of using more abstract models (such as the functional ones) for diagnostic purposes.

Among functional representation approaches, a flow-based approach[6,8,9] is well suited in the FTS domain. Such systems are indeed naturally represented as networks of abstract operators that act on the flow of substances. In particular, the functional representation proposed by the Multimodeling approach[9] explicitly supports also the notion of effort (pressure, in the hydraulic domain) that is crucial in the considered application, and provides criteria to abstract common physical equations into functional roles.

Moreover, interaction with the domain expert has shown that the provided explanations very often refer to a limited number of abstract processes involving substances (such as transporting, storing, transforming,...), which can be mapped into generic arrangements of functions. As an additional advantage, adopting a common functional modeling language did not present acceptance problems from the domain expert side.

From a reasoning point of view, the FDef approach[3] to functional diagnosis presents some advantages in terms of diagnostic power over other functional approaches. Chittaro and Ranon[11] show that FDef is not affected by two of the typical limitations of flow-based diagnostic approaches, where: (i) easy availability of measurements is assumed, although in real cases measurements are often difficult to take or too expensive, or unreliable, (ii) the generable diagnostic output is limited (e.g. only one candidate, or only single fault candidates). On the contrary, FDef is able to fully perform its diagnostic activity, regardless of the number of observations given, and to generate all the minimal multiple faults which are consistent with the observations.

3.2 The FDef approach: an overview

In this Section, we provide a brief overview of how we represent functional knowledge, and we sketch the reasoning strategy of the initial version of FDef.

3.2.1 Representation

The functional representation of a system aims at describing how the behavior of individual components contributes to the achievement of the purposes (teleology) assigned to the system by its designer.[12] We exploit two different functional models: (i) a functional role model,[9] built with conduit, generator, and barrier roles, and (ii) a process model,[9] automatically derived from the functional role model, by recognizing patterns (called *cofunctions*) of functional roles that support a physical process (e.g. a circuit of conduits and a generator supports a transport process). In this way, the physical system is represented by a network of functional roles that act on substances flowing through them, and a number of potential physical processes that can occur.

The functional role model describes a system in terms of flow-structures, i.e. in terms of networks of functional roles acting on flows (e.g. electrical current, hydraulic flow, etc.) of substances flowing through the structure of the system, and in terms of efforts (e.g. electrical voltage, hydraulic pressure, etc.), that is the driving forces. From this perspective, the functional role of a component is an abstract interpretation of the equations which describe its behavior, characterizing how the component contributes to the realization of a flow-structure. The interpretation is carried out using the Tetrahedron Of State,[13] an abstract framework that characterizes analogies among different physical domains (such as electromagnetism, translational and rotational mechanics, fluid dynamics, thermodynamics, etc.), using a set of generalized equations which describe typical relationships among a set of generalized variables (i.e. effort, flow, impulse, and displacement) and generalized parameters (capacity, resistance, inductance, electromotive force, electromotive flow). When the TOS is instantiated in a specific domain, the ordinary physical variables and equations are obtained (e.g. effort becomes voltage, or force, or torque, or pressure, or temperature,...). The set of primitives for the functional role model has been chosen by associating different types of roles (reservoir of impulse and/or

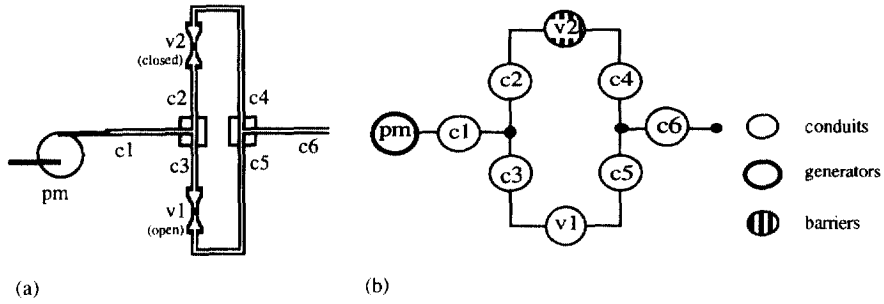

Fig. 2. A simple fluid transfer system (a), and its functional role model (b).

displacement, conduit of effort and/or flow, generator of effort and/or flow) to each generalized equation. The conduit role has been further specialized in order to distinguish special cases such as infinite resistance (barrier role) or infinite conductance (purely conductive conduit). A functional role model of a physical system is built by associating functional roles to the components of the system. As a simple example, consider the system in Fig. 2(a), composed by a positive displacement pump (pm), two valves (v1 and v2), and six pipes (c1,...,c6). Fig. 2(b) shows the functional role model of the system in a configuration where valve v2 is closed and valve v1 is open. In detail, each pipe is represented by a conduit role, and the representation of valves changes according to their operating mode: an open valve has a conduit role, and a closed valve has a barrier role. Also the representation of the positive displacement pump changes according to its operating mode: a powered pump has a flow generator role (i.e. source of flow), and an unpowered pump has a barrier role. The corresponding process model will contain two processes: a transport process with cofunction {pm, c1, c3, v1, c5, c6}, and a blocking transport process with cofunction {pm, c1, c2, v2, c4, c6}.

3.2.2 Reasoning with the initial version of FDef

The initial version[3] of FDef assumes that only very limited information from sensors is available. More specifically, the observations on generalized flows and efforts are of binary nature: a functional role is uncrossed (crossed) if the flow associated with it is (is not) zero, a functional role is unpushed (pushed) if the effort associated with it is (is not) zero. In the hydraulic domain, generalized flow and effort become hydraulic flow and pressure; a component is thus crossed (uncrossed) if it is (is not) traversed by flow, and it is unpushed (pushed) if the pressure drop across it is (is not) zero.

In general, converting raw measurements to the binary values requires to choose proper intervals for what is to be considered crossed/uncrossed or pushed/unpushed. For example, one might choose [−0.05,+0.05] bars as a pressure drop interval inside which a specific component has to be considered unpushed. In some cases, it is not necessary to choose such precise intervals. For example, Chittaro[3] presents some lighting system examples, where bulbs are considered crossed (or uncrossed) by observing if they are producing (or not) light.

The diagnostic strategy[3] was mainly based on the identification of the so-called *enabling sets* (an enabling set is a set of functional roles which are all allowing the passage of flow or effort), and *disabling sets* (a disabling set is a set of functional roles where there is at least one impediment to the passage of flow or effort). These sets were used both for exoneration purposes (identify components which are performing their function), and to generate conflicts (i.e. sets of components, each one containing at least a faulty component). When the set of conflicts is available, a simple candidate generation algorithm[14] produces the minimal diagnoses. FDef includes also an entropy-based[14] mechanism for test prescription, that can be used to suggest the most informative additional measurement to take in order to reduce the set of diagnostic candidates.

The general idea behind fault diagnosis in FDef was to use each available observation in order to generate hypotheses about which components in the system are performing their function and which are not. For example, let us assume we want to identify possible internal leaks and obstructions, considering the simple system in Fig. 2 with the following two observations: (i) there is a flow through c4, and (ii) there is no flow through c5. Considering the observation about c4, a general rule in FDef concludes that in order to explain that observation, the set of components from the generator to c4 is an enabling set that must be allowing the flow. This means that pm, c1, c2, and c4 are behaving as expected, but v2 is not (since it is closed, it should act as a barrier). Therefore, v2 is faulty. Then, considering the observation about c5, another general rule in FDef concludes that in order to explain that observation, the set of components from the generator to c5 is a disabling set, that is at least one component in the set must be an impediment to the flow. Since from the enabling set we know that this cannot be the case for pm, c1, and c6, then the possible impediments are c3, or v1, or c5. Therefore, the set of generated minimal diagnoses is: {{v2,c3}, {v2,v1}, {v2, c5}}.

Although general and applicable to different physical domains, the initial set of diagnostic axioms[3] is not sufficient for the diagnosis of the HFOTS, because it excludes malfunctions where substance flows out from the intended structure of the system (external leaks). It has thus been extended[1] to make it applicable to the HFOTS. As an example, consider the following rule:

E1: If a role X in cofunction Cof has been observed to

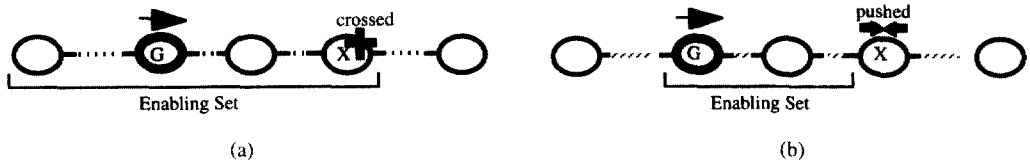

Fig. 3. Derivation of enabling sets (examples).

be crossed, and there is a generator G before X (or X is G) in Cof, and no role from the first to X has been observed to be unpushed or uncrossed, then the roles of Cof from the first (included) to X (included) are an enabling set.

The situation is illustrated in Fig. 3(a). Rule E1 allows the derivation of an enabling set starting from a crossed observation. The enabling set supports the observation about presence of flow, hypothesizing that all the roles included in the set are allowing the passage of flow. The rule deals with the case where the observed crossed role in the cofunction is after a generator. The generated enabling set explains the observation hypothesizing that all the roles from the beginning of the cofunction to the observed role are allowing the passage of flow, and nothing is concluded about roles that are after the observed one in the cofunction (e.g. one of them could be leaking).

As an example of a rule concerning effort observations, consider the following:

E3: If a role X in cofunction Cof has been observed to be pushed, and there is a generator G before X in Cof with no generators in between, and no role from G (included) to X has been observed to be unpushed, then the roles of Cof from G (included) to X (excluded) are an enabling set.

Fig. 3(b) illustrates a situation which is similar to the previous one with the difference that the observation now concerns an effort, and the generated enabling set is thus smaller than the previous one, comprising the roles from the generator before the role (included) to the role itself (excluded), with no conclusions about the other roles in the cofunction.

3.3 Functional representation of the HFOTS

In the hydraulic functional role model of the HFOTS, pipes (denoted with c0,...,c42) are represented as conduits. The representation of valves (v1,...,v5) changes according to their operating mode: an open valve is a conduit, and a closed valve is a barrier.

The representation of pumps (usgr006 and usgr007 are the on-board pumps, while p0 and p1 are pumps on the bunker boat) changes according to their operating mode. As mentioned before, volumetric pumps are generators or barriers: a powered pump is a generator, and an unpowered pump is a barrier.

All the tanks can be in a closed or open operating mode (each tank is provided with a built-in valve to switch between the two modes) and the associated functional role is conduit (when open) or barrier (when closed). As a result, some capacitive aspects of tanks are neglected in the current representation. In general, a tank can be considered a reservoir of mass and of energy: since the fluid can be stored in the reservoir, the tank is a reservoir of mass; since it can accumulate potential energy if it is placed at an higher elevation than other components, it can be also a reservoir of energy. The energy capacitance aspect of the reservoirs may be of relevance in the analysis of the transient behavior of FTS, which is not the object of the present work: we did not deal with energy capacitance aspects, and we considered reservoirs as either sources or sinks of mass. In the model, roles st1 and st2 are the two settling tanks, and sst, bst, cst and ost are the storage tanks.

The four-way and five-way nodes in Fig. 1 are aggregated components and thus they have been decomposed in their elementary components (pipes and three-way nodes), as shown in Fig. 4. Three-way nodes have been simply represented only as connections between two different flows (graphically depicted as black filled circles) in the functional role model. Indeed, it can be safely assumed that three-way nodes do not have faulty behaviors, and an actual fault in a three-way node will not go unnoticed by the diagnostic system, which will locate it in one of the components connected to the node (the node is thus simply seen as the final or initial part of the connected components). Fig. 5 illustrates the hydraulic functional role model of the HFOTS in a mode devoted to the simultaneous refueling of the four storage tanks. In the illustrated operating mode, HFO is expected to flow from the pump p0 to the four storage tanks through c0, v5, c1, c3, v4, c4, c6, c8, c10, v3, c11, c13, c15.

3.4 Reasoning example

The measurements (described in Section 2.1) available on the HFOTS are translated respectively into the following information in the functional role model:

- expected functional roles (conduits or barriers) associated with valves;
- expected functional roles (generators or barriers) associated to pumps;
- effort observation (pushed or unpushed) for p0, p1, usgr006, and usgr007;
- flow observation (crossed or uncrossed) for st1, st2, ost, cst, sst, and bst;
- effort measurement (pushed or unpushed) for c10.

More specifically, the measurements are translated as

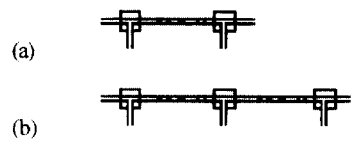

Fig. 4. Decomposition of (a) a four-way node, and (b) a five-way node.

follows. If the measurement of the position of a hydraulically driven valve returns open (closed), the expected functional role of the valve is conduit (barrier). If the measurement on a pump driving electrical motor is powered (not powered), the expected functional role is generator (barrier). A role is considered pushed when the measured pressure drop is sufficiently high to assume that it is due to the action of a pump, unpushed otherwise. Flow observations concerning tanks are deduced from the measurements on their level: if the level is steady, the role is uncrossed, otherwise it is crossed.

Suppose that the HFOTS is in the operating mode of Fig. 5 and the following values are obtained for the available flow and effort observations: p0, usgr006, usgr007, and c10 are pushed; p1 is unpushed; ost, cst, and bst are crossed; sst, st1, and st2 are uncrossed.

Some examples of enabling sets are the following: the set {p0, c0, v5, c1, c3, v4, c4, c6, c8, c10, v3, c11, c13, c15, bst} is an enabling set generated by rule E1 from observation 'bst is crossed', i.e. a possible explanation of the observation is that all the functional roles in the set are allowing the passage of flow. The set {p0, c0, v5, c1, c3, v4, c4, c6, c8} is an enabling set generated by rule E3 to explain 'c10 is pushed', while an alternative explanation is given, for example, by the enabling set {p0, c0, v5, c1, c2, usvgr16, c27, c28, usgr007, c13, c11, v3}, generated by rule E3 too. Both sets can explain the observation by assuming that the specified roles are allowing the passage of effort.

The set {p0, c0, v5, c1, c3, v4, c4, sst} is an example of disabling set generated from the observation 'sst is uncrossed', i.e. at least one functional role in this set must be an impediment to the passage of the intended flow. Another example of disabling set generated from 'sst is uncrossed' is {p0, c0, v5, c1, c2, usvgr16, c29, usgr006, c6, sst}, with an analogous meaning.

The following is the set of 16 minimal diagnoses generated by FDef using the enabling and disabling sets produced by the new rules:

{ {sst},
{usgr006,c6,v4}, {usgr006,c6,c4},
{usgr006,c6,c3}, {usvgr14,c8,v4},
{usvgr14,c6,v4}, {usvgr14,c8,c4},
{usvgr14,c6,c4}, {usvgr14,c8,c3},
{usvgr14,c6,c3}, {usgr007,c8,v4},
{usgr007,c6,v4}, {usgr007,c8,c4},
{usgr007,c6,c4}, {usgr007,c8,c3},
{usgr007,c6,c3} }

The first candidate is the most probable one: a faulty sst explains why pressure normally reaches c10, usgr007 and usgr006, and flow reaches ost, cst and bst, but not sst.

The other candidates are less likely triple faults. Consider, for example, the second candidate: {usgr006, c6, v4}. In this case, v4 is faulty, and flow cannot thus reach SST through it, a faulty usgr006 allows the flow to reach all the other storage tanks (ost, cst, and bst), while the flow does not reach sst through usgr006 because c6 is faulty. The explanations for the other triple faults are similar to this one. The considered triple fault is also an example of a fault masking case, where the effect of the faulty v4 on the ost, cst, and bst tanks is masked by a simultaneous fault on usgr006 which allows the flow to reach the three tanks.

The most informative additional measurement determined for the generated candidate set, using the entropy-based mechanism for test prescription, is the pressure associated to sst.

In general, this and other experiments considering several different situations showed that diagnosing the model in Fig. 5 with the initial version of FDef requires an average time of 10 seconds on a PC.

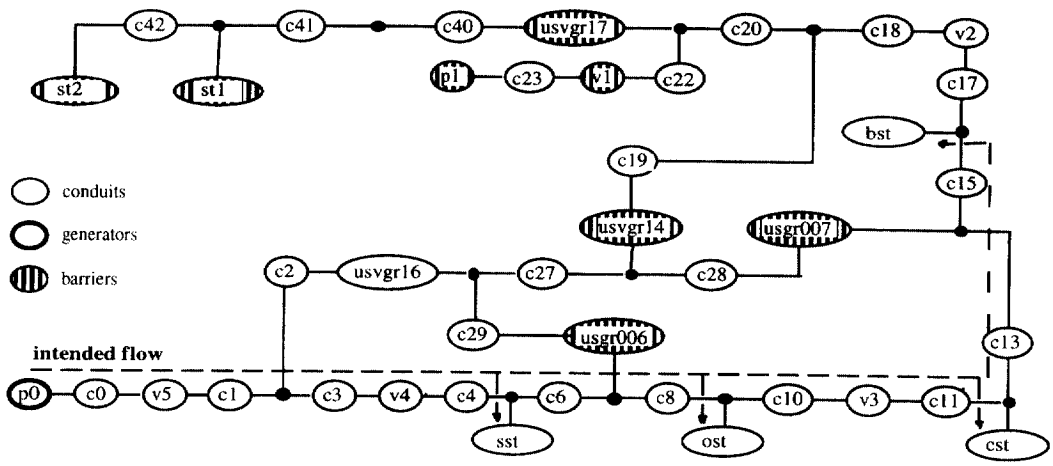

Fig. 5. Functional role model of the HFOTS (a configuration for refuelling all the four storage tanks).

4 CRITICAL ANALYSIS

We have evaluated the application of the initial version of FDef to the HFOTS on a large set of examples, in order to highlight its strengths and weaknesses, and pinpoint directions for further investigation. In the following, we discuss the main conclusions of the evaluation.

First, we can say that the approach is adequate to isolate faults when they result in a total loss of functionality (e.g. complete obstruction faults). Since many faults in the considered domain are preceded by a slow degradation in performance before possibly turning into a loss of functionality, they can be detected by the application only if and after the degradation becomes severe. To face the problem of diagnosing partial losses of functionality, it is necessary to obtain more informative observations than just presence/absence of flows/efforts. To face this problem, we propose to exploit *too-low/too-high* effort and flow values. These observations characterize deviations from the expected nominal value of measurements. For example, consider again the system in Fig. 2, and suppose there are two observations available: flow at the input of c6 is too low, and pressure at the input of c1 is too high. If these two observations were in terms of presence/absence of flows/efforts (presence of flow at the input of c6, presence of effort at the input of c1), the situation would be considered normal. On the contrary, from the first deviation observation, one can conclude that either the generator pm is not delivering enough flow, or there is an external leak downstream the pump (including a possible external loss from the pump) and before c6. From the second deviation observation, one can conclude that either the generator pm is delivering a too high flow, or there is an obstruction in the branch leading from c1 to c6 through the open valve. The logical combination of the two conclusions would allow us to generate the set of detailed diagnoses. One pair would be logically excluded (the pump cannot be producing a too high and a too low flow at the same time), while all other pairs are consistent and would be included in the set of diagnoses. For example, one of the valid faults is given by an external leak in c5, and a simultaneous obstruction in c3. An example involving the pump is given by a failure in pm (it does not deliver enough flow) and a simultaneous partial closure of valve v1.

With respect to the five classes of faults of interest presented in Section 2, a major problem of the evaluated approach concerns the handling of external leaks. In general, there are many factors involved in determining which effects an external leak will have on a fluid transport system, and it is impossible to give them a single schematic characterization: the rules used for the HFOTS experiments covered just a small subset of the possible different leak situations that can be theoretically imagined. More specifically, they cover the situation where the considered leak is able to stop the flow after the leaking component, but does not prevent flow in those paths to which it does not belong. This choice was mainly due to the limited information contained in the binary observations about pressures and flows. Therefore, one useful extension which would allow a more complete handling of leaks is again the introduction and exploitation of *too-low/too-high* effort and flow values.

Another limitation of the experimented approach concerns the generality and reusability of the diagnostic rules. Since they have been developed by studying the specific application context of the HFOTS, there is no formal guarantee that they are easily generalizable to the domain of FTS. It is thus important to re-think them in a general setting and to properly validate them formally.

Finally, one of the goals of the first experiments was also to study the scaling up of the size of the considered models. Since it turned out that much of the diagnostic system running time was devoted to matching rules to the flat representation of the whole model and processing enabling and disabling sets of considerable size, it would be important to introduce a proper organizing structure for model representation which should (i) optimize the matching, e.g. allowing an efficient identification of interesting relations among any component (e.g. which components are in parallel/series to a given one?), and (ii) support reasoning at different levels of abstraction, which would allow either to reducing the size of the generated sets or better substitute generation of enabling/disabling sets with a more focused diagnostic reasoning.

In the following, we will show how we have solved the above illustrated problems by proposing a novel FDef approach characterized by more complete and general fault identification capabilities. The presentation is self-contained and does not require familiarity with the previous FDef reasoning technique. We generalize the approach, by moving from the HFOTS case study to the wider class of systems introduced in Section 2, and we significantly increase its diagnostic capabilities by moving from the binary (presence/absence) quantity space to a new quantity space which represents deviations from nominal values (Section 5). We adopt a proper organizing structure for representing and reasoning with the functional role model at different levels of abstraction (Section 6), and we introduce a novel reasoning technique (Section 7) that exploits this structure to achieve diagnosis focusing capabilities, and make the generation of enabling/disabling sets unnecessary. Finally, we will show how the new formulation of diagnostic knowledge can be formally validated (Section 8), and we will discuss the advantages of the new proposal both in relation to the initial version of FDef and to more traditional model-based diagnosis approaches (Section 9).

5 REPRESENTING DEVIATIONS

As previously anticipated, one of our goals in this paper is to augment the power of functional diagnosis by exploiting a more informative quantity space for flow and effort variables. While the quantity space previously adopted was limited to *presence* or *absence* values for observed flows and efforts, we now consider a deviation quantity space where the value of a measurement provided to the diagnostic system

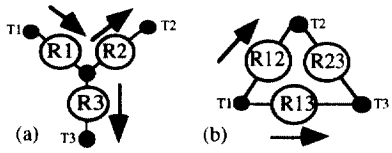

Fig. 6. Three-star removal rule in the functional role model.

can be *too-low*, *nominal*, or *too-high*. If $\tilde{X}$ is the nominal value expected by design (or possibly by numerical simulation) for a physical quantity, and X is its actual value, the deviation is defined as:

$$\Delta X = X - \tilde{X} \tag{1}$$

For the qualitative deviation (denoted $[\Delta X]$), the chosen value set is the well known $\{-, 0, +\}$, so that *too-low* corresponds to the negative sign, *nominal* to zero, and *too-high* to the positive sign.

It is interesting to note that while we, after having started from a binary presence/absence representation, are enriching it to move to a deviation quantity space, other researchers,[15,16] after having started from richer representations, are simplifying them to move to the same deviation quantity space. This suggests that, among the qualitative representations which could be adopted, a deviation quantity space gives possibly the best compromise between simplicity of computation and completeness of diagnosis, i.e. it is not too complex to be handled computationally, and at the same time it allows one to generate a candidate set which is not too simplified. In particular, Williams and Nayak[16] point out that their and others experience has shown that extremely weak qualitative representations such as deviations from nominal values are sufficient for many model-based real-world autonomy tasks, and go as far as to say that 'counter to the folklore of the field, ambiguity and intractable branching has not proven to be a significant practical issue'.

Nevertheless, we want to stress that, as with any qualitative representation, there will always be some faults which cannot be isolated precisely. For example, if both the input and the output flow rate of a leaking pipe are *too-low* (or if they are both *too-high*), and in absence of other information, there is no way of hypothesizing the leak. On one hand, this problem cannot be solved by allowing the system to hypothesize that the pipe is faulty, because this would imply that the normal qualitative model of the component is also an abnormal one. On the other hand, enriching the qualitative representation does not solve the problem either, because there will be always cases where the two flows, although quantitatively different, qualitatively coincide.

6 REPRESENTING THE MODEL AT MULTIPLE LEVELS OF ABSTRACTION

In this section, we introduce the hierarchical structure we use in order to represent and reason about the functional role model. This structure allows an efficient recognition of the topological relations among any component, and supports reasoning at different levels of abstraction.

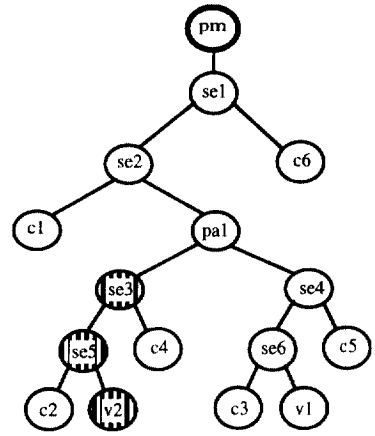

Fig. 7. SPS tree for System A.

The adopted structure is a tree built by using well established ideas for circuit reduction.[17] The root node of the tree is an active generator, while the other functional roles are leaf nodes. The nodes at the intermediate levels represent abstract subsystems based on the standard notions of series and parallel connection. However, a system cannot always be represented using only series and parallel reduction. These cases are solved by using the star removal rule (also known as star-mesh conversion). In general, star-mesh conversion identifies star patterns in a circuit and substitutes them with a behaviorally equivalent topology to which series and parallel reduction can then be applied. The correspondence between the components in the real system and the components in the new topology is precisely established by simple equations. Fig. 6 illustrates the 3-star removal rule in the context of our functional role model: the 3-star configuration in Fig. 6(a) can be removed and replaced by the triangle configuration in Fig. 6(b). The general equations of star-mesh conversion in this case express the relations between the flows and the efforts in the two topologies, e.g. the flow through role R1 is equal to the sum of the flows through R12 and R13. The direction of intended flow for R23 in Fig. 6 is not indicated, because it depends on the difference of pressure between terminals T2 and T3 in the figure: as a sign convention for the general equations, we choose to consider this flow positive when it goes from T3 to T2. Accordingly, between the two possible choices for performing removal of a given 3-star, we always adopt the one that derives an R23 whose intended flow goes from T3 to T2.

Another interesting point is that the SPS tree can be built automatically, starting from the available structural connectivity information among the components in the system. In particular, among existing graph translation techniques, we adopt the algorithm proposed by Mauss and Neumann[18] to automatically build a series-parallel-star (SPS) reduction tree for an arbitrary network.

Fig. 7 shows the SPS tree representing the functional role model illustrated in Fig. 2(b). Hereinafter, we refer to this

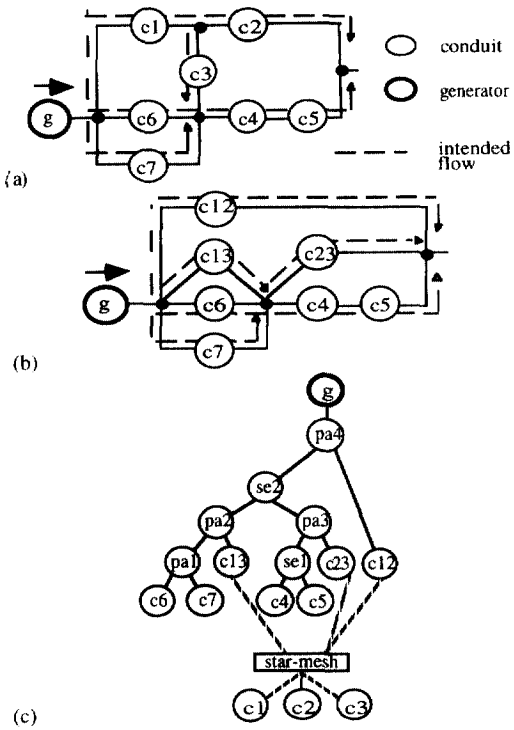

Fig. 8. (a) Functional role model for System B; (b) result of star-mesh conversion; and (c) SPS tree representation of System B.

system as System A. The simple topology of System A can be represented using only series and parallel abstractions, without any star-mesh conversion. The series nodes in Fig. 7 are se1, se2, se3, se4, se5, and se6, while pa1 is a parallel node. For example, se6 abstracts roles c3 and v1 into a single subsystem (series connection of c3 and v1), and pa1 abstracts se3 and se4 into a single subsystem (parallel connection of se3 and se4).

Fig. 8(a) shows the functional role model of a more complex FTS topology. Hereinafter, we refer to this system as System B. Fig. 8(b) shows the results of star-mesh conversion for System B, and Fig. 8(c) shows its SPS tree. The series nodes in the SPS tree are se1, and se2. For example, se1 abstracts roles c4 and c5 into a single component (series connection of c4 and c5). The parallel nodes are pa1, pa2, pa3, and pa4. For example, pa1 abstracts roles c6 and c7 into a single component (parallel connection of c4 and c5). The abstracted nodes are subject to further abstraction, e.g. se2 is the series connection of pa2 and pa3. Star-mesh conversion has converted roles c1, c2, and c3 into three other roles c12, c23, and c13, which are then used for parallel and series reduction.

In general, since we restrict the analysis of hydraulic systems to a qualitative deviation space, all conclusions drawn in the electric domain can be applied directly to the hydraulic domain: in the considered space, the correspondence between the qualitative laws which describe the electric components and those describing hydraulic components is straightforward, and preserves the qualitative correspondence among the *deviations* of variables in the two domains. Therefore, in a deviation space, the implications of star-mesh conversion for hydraulic systems are the same as for electric systems.

7 REASONING WITH DEVIATIONS AT MULTIPLE ABSTRACTION LEVELS

As pointed out in Section 4, FDef rules such as those presented in Section 3.2 tended to be conceptually very complex, and not easy to formally verify both from the correctness and the generality point of view. Therefore, we replace them with a novel formulation: not with respect to a whole model, but with respect to well structured abstractions, such as series and parallel connections of roles. Moreover, we aim at clearly separating and organizing them into different classes of axioms, devoted to conceptually different activities, in order to further simplify their understanding, exploitation, and reusability.

In the following, we first provide some basic definitions, then we present the three different classes of axioms we defined (value mapping, fault generation, and fault mapping), providing examples of application of axioms for each class. Finally, we sketch the control algorithm that manages axioms application in diagnostic reasoning.

For all the following definitions, the convention of beginning variables names with an uppercase letter and constants names with a lowercase letter is adopted.

7.1 Basic definitions

The predicates conduit(N) and barrier(N) are true when N is a node of the SPS tree and respectively corresponds to a conduit and barrier functional role. The predicate generator(N,L) is true when N is a node of the SPS tree corresponding to a generator functional role, and L is its load (the son of N in the SPS tree).

The predicate series(N,N1,N2) is true when N is a series node of the SPS tree, N1 is the left son of N, and N2 is the right son of N (N is the series of nodes N1 and N2). With respect to the intended direction of flow, N1 precedes N2. Considering System A, for example, series(se6,c3,v1) and series(se4,se6,c5) are true.

The predicate parallel(N,N1,N2) is true when N is a parallel node of the SPS tree, and N1 and N2 are its two sons (N is the parallel of nodes N1 and N2). For any parallel node, the following implication holds:

$$\text{parallel}(X, N1, N2) \Leftrightarrow \text{parallel}(X, N2, N1)$$

i.e. a parallel node in the model can always satisfy the parallel predicate in two different ways. For example, in System B, parallel(pa1,c6,c7) and parallel(pa1,c7,c6) are both true.

The predicate star(R1,R2,R3,R12,R13,R23) represents a star-mesh conversion between the three roles R1, R2, R3, and their abstract counterparts R12, R13, and R23. In System B, star(c1,c2,c3,c12,c13,c23) is true, stating that nodes c12, c13 and c23 are obtained by star-mesh conversion from roles c1, c2 and c3.

Finally, the predicate node(X) is true if X is a node (series, parallel, generator, conduit, barrier) of the SPS tree.

Nodes which are not at the component level act as barriers if they satisfy certain configurations (e.g. if one son of a series node is a barrier, no flow is allowed through the series node, which is a barrier too). The full set of these configurations is captured by the following axioms:

$$\text{barrier(X)} \Leftarrow \text{parallel(X,N1,N2)} \wedge \text{barrier(N1)} \wedge \text{barrier(N2)}$$

$$\text{barrier(X)} \Leftarrow \text{series(X,N1,N2)} \wedge (\text{barrier(N1)} \vee \text{barrier(N2)})$$

$$\text{barrier(R12)} \wedge \text{barrier(R13)} \Leftarrow \text{star(R1,R2,R3,R12,R13,R23)} \wedge \text{barrier(R1)}$$

$$\text{barrier(R12)} \wedge \text{barrier(R23)} \Leftarrow \text{star(R1,R2,R3,R12,R13,R23)} \wedge \text{barrier(R2)}$$

$$\text{barrier(R13)} \wedge \text{barrier(R23)} \Leftarrow \text{star(R1,R2,R3,R12,R13,R23)} \wedge \text{barrier(R3)}$$

During the automatic building of the tree, these axioms allow us to assign automatically barrier roles in the upper levels, starting from the barrier roles assigned at the component level. Fig. 7 graphically highlights the two barrier roles (se5 and se3) determined starting from barrier v2 at the component level.

We associate four variables to any node N in the SPS tree: (i) $[\Delta F_{in}(N)]$ is the qualitative deviation of the node inlet flow, (ii) $[\Delta F_{out}(N)]$ is the qualitative deviation of the node outlet flow, (iii) $[\Delta E_{in}(N)]$ is the qualitative deviation of the node inlet effort, and (iv) $[\Delta E_{out}(N)]$ is the qualitative deviation of the node outlet effort.

The following relation holds:

$$\text{node(N)} \Rightarrow [\Delta F_{in}(N)] \geq [\Delta F_{out}(N)]$$

i.e. the qualitative deviation of inlet flow in any node must be greater or equal to the qualitative deviation of outlet flow. This relation is used to support a simple propagation activity: knowing that $[\Delta F_{in}(N)] = [\,-\,]$, it allows us to conclude that $[\Delta F_{out}(N)] = [\,-\,]$, or knowing that $[\Delta F_{out}(N)] = [\,+\,]$, it allows us to conclude that $[\Delta F_{in}(N)] = [\,+\,]$.

7.2 Value mapping axioms

Since the representation of our model is organized into different levels of detail, the need arises for translating observations among the levels. The value mapping axioms are used to this purpose. They have been obtained by simply applying the physical definitions of series, parallel and star-mesh configurations to the adopted qualitative representation. We list in the following the definitions of the adopted value mapping axioms:

$$\text{series(SE,N1,N2)} \Rightarrow [\Delta F_{in}(N1)] = [\Delta F_{in}(SE)] \wedge [\Delta F_{out}(N1)] = [\Delta F_{in}(N2)] \wedge [\Delta F_{out}(N2)] = [\Delta F_{out}(SE)] \quad \text{(VM1)}$$

$$\text{series(SE,N1,N2)} \Rightarrow [\Delta E_{in}(N1)] = [\Delta E_{in}(SE)] \wedge [\Delta E_{out}(N1)] = [\Delta E_{in}(N2)] \wedge [\Delta E_{out}(N2)] = [\Delta E_{out}(SE)] \quad \text{(VM2)}$$

$$\text{parallel(PA,N1,N2)} \Rightarrow [\Delta F_{in}(N1)] + [\Delta F_{in}(N2)] = [\Delta F_{in}(PA)] \wedge [\Delta F_{out}(N1)] + [\Delta F_{out}(N2)] = [\Delta F_{out}(PA)] \quad \text{(VM3)}$$

$$\text{parallel(PA,N1,N2)} \Rightarrow [\Delta E_{in}(N1)] = [\Delta E_{in}(N2)] = [\Delta E_{in}(PA)] \wedge [\Delta E_{out}(N1)] = [\Delta E_{out}(N2)] = [\Delta E_{out}(PA)] \quad \text{(VM4)}$$

$$\text{star(R1,R2,R3,R12,R13,R23)} \Rightarrow [\Delta F_{in}(R12)] + [\Delta F_{in}(R13)] = [\Delta F_{in}(R1)] \wedge [\Delta F_{out}(R12)] + [\Delta F_{out}(R13)] = [\Delta F_{out}(R1)] \wedge [\Delta F_{in}(R13)] - [\Delta F_{in}(R23)] = [\Delta F_{in}(R3)] \wedge [\Delta F_{out}(R13)] - [\Delta F_{out}(R23)] = [\Delta F_{out}(R3)] \wedge [\Delta F_{in}(R12)] + [\Delta F_{in}(R23)] = [\Delta F_{in}(R2)] \wedge [\Delta F_{out}(R12)] + [\Delta F_{out}(R23)] = [\Delta F_{out}(R2)] \quad \text{(VM5)}$$

$$\text{star(R1,R2,R3,R12,R13,R23)} \Rightarrow [\Delta E_{in}(R1)] = [\Delta E_{in}(R12)] = [\Delta E_{in}(R13)] \wedge [\Delta E_{out}(R3)] = [\Delta E_{out}(R13)] = [\Delta E_{in}(R23)] \wedge [\Delta E_{out}(R2)] = [\Delta E_{out}(R12)] = [\Delta E_{out}(R23)] \quad \text{(VM6)}$$

$$\text{generator(N,L)} \Rightarrow [\Delta F_{in}(L)] = [\Delta F_{out}(N)] \quad \text{(VM7)}$$

Since axioms VM3 and VM5 contain qualitative sums and differences, their equations can be affected by ambiguity (e.g. the sum of a $[\,+\,]$ and a $[\,-\,]$). In the case of ambiguity in axiom VM3 (parallel nodes), the diagnostic system will not use the affected equation to generate the possible cases, while in the case of ambiguity in axiom VM5 (star-mesh conversion), all the minimal possibilities will be developed. This is due to the fact that the different possibilities concerning series and parallel nodes are taken into account by the fault generation mechanism (Section 7.3 and Section 7.5), while observations concerning a star need to be taken to the mesh level in order to be considered by the fault generation mechanism.

To exemplify value mapping, we consider two different situations.

7.2.1 Example A

Consider system A with the following observations:

$$[\Delta F_{out}(v2)] = [\,+\,]$$
$$[\Delta F_{out}(c3)] = [\,-\,]$$

Using value mapping axiom VM1, and the simple propagation activity discussed in Section 7.1, the following conclusions are reached: $[\Delta F_{in}(v2)] = [\,+\,]$, $[\Delta F_{out}(c2)] = [\,+\,]$, $[\Delta F_{in}(c2)] = [\,+\,]$, $[\Delta F_{out}(se5)] = [\,+\,]$, $[\Delta F_{in}(se5)] = [\,+\,]$, $[\Delta F_{in}(c4)] = [\,+\,]$, $[\Delta F_{in}(se3)] = [\,+\,]$, $[\Delta F_{in}(v1)] = [\,-\,]$, $[\Delta F_{out}(v1)] = [\,-\,]$, $[\Delta F_{out}(se6)] = [\,-\,]$, $[\Delta F_{in}(c5)] = [\,-\,]$, $[\Delta F_{out}(c5)] = [\,-\,]$, and $[\Delta F_{out}(se4)] = [\,-\,]$.

7.2.2 Example B

Consider system B with the following observations:

$$[\Delta F_{in}(c1)] = [\ -\ ]$$
$$[\Delta F_{in}(c6)] = [\ -\ ]$$
$$[\Delta F_{in}(c7)] = [\ +\ ]$$

In this case, observations $[\Delta F_{in}(c6)] = [\ -\ ]$ and $[\Delta F_{in}(c7)] = [\ +\ ]$ are not mapped to the upper level due to ambiguity in axiom VM3; $[\Delta F_{in}(c1)] = [\ -\ ]$ yields $[\Delta F_{out}(c1)] = [\ -\ ]$; moreover, $[\Delta F_{in}(c1)] = [\ -\ ]$ is abstracted by using the qualitative relations of axiom VM5 into two possibilities: $[\Delta F_{in}(c12)] = [\ -\ ]$ (and thus $[\Delta F_{out}(c12)] = [\ -\ ]$) or $[\Delta F_{in}(c13)] = [\ -\ ]$ (and thus $[\Delta F_{out}(c13)] = [\ -\ ]$). This is obtained by considering the relation $[\Delta F_{in}(c12)] + [\Delta F_{in}(c13)] = [\Delta F_{in}(c1)]$ given by VM5: since the result of the sum is $[\ -\ ]$, then at least one of the two operands in the sum must be $[\ -\ ]$.

7.3 Fault generation axioms

The purpose of this class of axioms is to hypothesize faults associated to nodes of the SPS tree. Each axiom characterizes the effects of a fault, located in the part of the system represented by the node, on the variables associated to the node (or possibly to its two sons). Note that different axioms may refer to the same fault, because they characterize the effects of the fault with respect to different types of nodes. We list in the following the definitions of the main fault generation axioms:

$$\text{fault(N,extLeak)} \Leftarrow \text{node(N)}$$
$$\wedge\ [\Delta F_{in}(N)] > [\Delta F_{out}(N)] \qquad \text{(FG1)}$$

i.e. there is an external leak (extLeak) in a node N, if the qualitative deviation of its input flow is greater than the one of its output flow (this is a precise indication of a mass deficit).

$$\text{fault(N,intLeak)} \Leftarrow \text{barrier(N)}$$
$$[\Delta F_{in}(N)] = [\Delta F_{out}(N)] \neq [0] \qquad \text{(FG2)}$$

i.e. there is an internal leak (intLeak) in a barrier node N, if the qualitative deviations of its input and output flow are equal and not nominal (note that the nominal output flow for a barrier node is null).

$$\text{fault(N1,extLeak)} \Leftarrow \text{parallel(PA,N1,N2)}$$
$$\wedge\ \neg\text{barrier(N2)}$$
$$\wedge\ [\Delta F_{in}(N1)] > [\Delta F_{out}(N1)]$$
$$\wedge\ [\Delta F_{in}(N1)] > [\Delta F_{in}(N2)] \qquad \text{(FG3)}$$

i.e. in a parallel node PA with sons N1 and N2, where N2 is not a barrier, there is an external leak (extLeak) in N1 if the qualitative deviation of its input flow is greater than the one of the output flow (mass deficit), and greater than the one for the input flow of N2 (this indicates that due to the external leak in N1, part of the flow expected through N2 is drained to N1).

$$\text{fault(N2,intLeak)} \Leftarrow \text{parallel(PA,N1,N2)} \wedge \text{barrier(N2)}$$
$$\wedge\ [\Delta F_{in}(N2)] = [\Delta F_{out}(N2)] \neq [0]$$
$$\wedge\ [\Delta F_{in}(N2)] > [\Delta F_{in}(N1)] \qquad \text{(FG4)}$$

i.e. in a parallel node PA with sons N1 and N2, with N2 barrier, there is an internal leak (intLeak) in N2 if the qualitative deviations of the input and output flow of N2 are equal and not nominal (in other words, they are not null as expected), and the qualitative deviation of the input flow of N2 is greater than the one of the input flow of N1 (for example, when N1 is not a barrier, this indicates that due the internal leak in N2, part of the flow expected through N1 is drained to N2).

$$\text{fault(N,lowGen)} \Leftarrow \text{generator(N,L)} \wedge \neg\text{barrier(L)}$$
$$\wedge\ [\Delta F_{out}(N)] = [\ -\ ] \qquad \text{(FG5)}$$

$$\text{fault(N,highGen)} \Leftarrow \text{generator(N)} \wedge \neg\text{barrier(L)}$$
$$\wedge\ [\Delta F_{out}(N)] = [\ +\ ] \qquad \text{(FG6)}$$

i.e. a generator N delivers a wrong flow rate, too low (lowGen) or too high (highGen), if the deviation of its output flow is respectively too low or too high. The two axioms also require that the load L is not a barrier, otherwise the nominal output flow from N would be null, and possible deviations would be an indication of a fault in L (and not N), which has to be dealt with by other fault generation axioms (such as FG2).

$$\text{fault(N2,obstr)} \Leftarrow \text{parallel(PA,N1,N2)}$$
$$\wedge\ \neg\text{barrier(N1)}$$
$$\wedge\ \neg\text{barrier(N2)} \wedge [\Delta F_{in}(N1)] = [\Delta F_{out}(N1)]$$
$$\wedge\ [\Delta F_{in}(N2)] = [\Delta F_{out}(N2)]$$
$$\wedge\ [\Delta F_{in}(N1)] > [\Delta F_{in}(N2)] \qquad \text{(FG7)}$$

i.e. in a parallel node PA with sons N1 and N2, none of which is a barrier, there is an obstruction (obstr) in N2 if the qualitative deviations of the input and the output flow of N1 are equal (i.e. there are no detectable external leaks in N1), the qualitative deviations of the input and the output flow of N2 are equal (i.e. there are no detectable external leaks in N2), and the qualitative deviation of the input flow of N1 is greater than the one of N2 (an obstruction in node N2 forces part of its expected flow towards node N1).

$$\text{fault(N,obstr)} \Leftarrow \text{node(N)} \wedge \neg\text{barrier(N)}$$
$$\wedge\ [\Delta E_{in}(N)] = [\ +\ ] \wedge [\Delta E_{out}(N)] \leq [0]$$
$$\wedge\ [\Delta F_{in}(N)] = [\Delta F_{out}(N)] \leq [0] \qquad \text{(FG8)}$$

i.e. in a node N which is not a barrier, there is an obstruction (obstr) if there is an increase in the input pressure (its qualitative deviation is $[\ +\ ]$), which is not followed by the output pressure (which remains nominal or has decreased) and the qualitative deviations of the input and the output flow are equal (i.e. there are no detectable external leaks) and are not positive.

Since some fault generation axioms contain references to more than one node, when we say that one instance of these axioms is *applicable to a node*, we always refer to the higher level node mentioned in the instance.

In general, a fault generation axiom is considered applicable in order to hypothesize faults, also when the values of

some of the qualitative variables it refers to are unknown, provided that the axiom refers to at least one variable which is known to be deviated, and no condition of the axiom is known to be false. However, only a subset of the applicable fault generation axioms has to be actually applied, as we will show in Section 7.5.

Note that stuck valve faults are covered by the axioms which diagnose internal leak and obstruction: an internal leak is derived for a valve expected to be closed which is instead stuck at open or partially open, while an obstruction is derived for a valve expected to be open which is instead stuck at close or only partially open. The stuck pump fault is covered by the axiom which diagnoses low delivered flow rate in generators of flow.

To show applicable instances of the previously shown fault generation axioms, let us consider again the two diagnostic examples introduced in the previous section.

7.3.1 Example A

Considering the given observations and the results of value mapping, the applicable axioms are: FG1 to c4 (hypothesizing an extleak in node c4), to se3 (extleak in se3), to c3 (extleak in c3), to se6 (extleak in se6), and to se4 (extleak in se4); FG2 to v2 (intleak in v2), to se5 (intleak in se5), and to se3 (intleak in se3); FG3 to pa1 (extleak in se3); FG4 to pa1 (intleak in se3); FG8 to c3 (obstr in c3), to v1 (obstr in v1), to se6 (obstr in se6), to c5 (obstr in c5), and to se4 (obstr in se4).

7.3.2 Example B

Considering the given observations and the results of value mapping, the applicable axioms are: FG1 to c7 (extleak in c7); FG3 to pa1 (extleak in c7); FG7 to pa1 (obstr in c6); FG8 to c6 (obstr in c6), and to c1 (obstr in c1). Moreover, in the case where the first of the two possibilities (i.e. $[\Delta F_{in}(c12)] = [\ -\ ]$) generated by value mapping is considered, the following additional axioms are applicable: FG3 to pa4 (extleak in se2), FG7 to pa4 (obstr in c12), and FG8 to c12 (obstr in c12). In the case where the second possibility (i.e. $[\Delta F_{in}(c13)] = [\ -\ ]$) is considered, the following additional axioms are applicable: FG3 to pa2 (extleak in pa1), FG7 to pa2 (obstr in c13), and FG8 to c13 (obstr in c13).

7.4 Fault mapping axioms

Fault mapping axioms are able to identify the counterpart of a fault at any level of detail. These axioms are used to support a flexible reasoning strategy: for example, if a fault can be identified only at a given level, we use them to translate it to lower levels, providing more detailed fault descriptions. On the other hand, if a fault can be identified at several levels, we want our diagnostic system to identify it at the most detailed possible level, and to translate it to upper levels with fault mapping axioms. This mapping activity is performed to ensure efficiency (i.e. reasoning which would detect less detailed versions of the same fault at upper levels is not performed), correctness (i.e. consistency with other diagnostic conclusions possibly reached at other nodes), and proper detail of the final candidates (the final candidates have to be produced at the component level). We list in the following the definitions of fault mapping axioms:

series(N,N1,N2) ⇒
(fault(N,obstr) ⇔ fault(N1,obstr) ∨ fault(N2,obstr)) (FM1)

parallel(N,N1,N2) ∧ ¬barrier(N1)
∧ barrier(N2) ⇒
(fault(N,obstr) ⇔ fault(N1,obstr)) (FM2)

parallel(N,N1,N2) ∧ ¬barrier(N1)
∧ ¬barrier(N2) ⇒
(fault(N,obstr) ⇔ fault(N1,obstr) ∨ fault(N2,obstr)) (FM3)

parallel(N,N1,N2) ⇒
(fault(N,extLeak) ⇔ fault(N1,extLeak)
∨ fault(N2,extLeak)) (FM4)

series(N,N1,N2) ∧ barrier(N1) ⇒
(fault(N,extLeak) ⇔ fault(N1,extLeak)
∨ (fault(N1,intLeak) ∧ fault(N2,extLeak))) (FM5)

series(N,N1,N2) ∧ ¬barrier(N1) ⇒
(fault(N,extLeak) ⇔ fault(N1,extLeak)
∨ fault(N2,extLeak)) (FM6)

parallel(N,N1,N2) ∧ ¬barrier(N1)
∧ barrier(N2) ⇒
(fault(N,intLeak) ⇔ fault(N2,intLeak)) (FM7)

parallel(N,N1,N2) ∧ barrier(N) ⇒
(fault(N,intLeak) ⇔ fault(N1,intLeak)
∨ fault(N2,intLeak)) (FM8)

series(N,N1,N2) ∧ barrier(N1)
∧ barrier(N2) ⇒
(fault(N,intLeak) ⇔ fault(N1,intLeak)
∧ fault(N2,intLeak)) (FM9)

series(N,N1,N2) ∧ barrier(N1)
∧ ¬barrier(N2) ⇒
(fault(N,intLeak) ⇔ fault(N1,intLeak)) (FM10)

series(N,N1,N2) ∧ barrier(N2)
∧ ¬barrier(N1) ⇒
(fault(N,intLeak) ⇔ fault(N2,intLeak)) (FM11)

star(R1,R2,R3,R12,R13,R23) ⇒
(fault(R12,F) ⇔ fault(R1,F) ∨ fault(R2,F)) (FM12)

star(R1,R2,R3,R12,R13,R23) ⇒
(fault(R13,F) ⇔ fault(R1,F) ∨ fault(R3,F)) (FM13)

star(R1,R2,R3,R12,R13,R23) ⇒
(fault(R23,F) ⇔ fault(R2,F) ∨ fault(R3,F)) (FM14)

For example, consider System A, and suppose there is an external leak in c3. This fault can be mapped by axiom FM6 into an external leak in se6, which can then be mapped again by FM6 into an external leak in se4. The upward mapping of the leak can proceed up to se1, by three further applications of fault mapping axioms (one application of FM4 and two of FM6). On the other hand, suppose to know only that there is an external leak in se4, and it is mapped to lower levels: FM6 maps the leak into an external leak in se6 or c5, then FM6 again maps the external leak in se6 into an external leak in c3 or v1. Thus, the diagnostic conclusions at the component level in this case are that the external leak is in c3, or v1, or c5.

In general, the application of a fault mapping axiom to a node in the downward sense proposes all possible candidates at the lower level (e.g. an extLeak in a parallel node is mapped into two possibilities, i.e. an extLeak in one of the two sons). In a specific diagnostic situation, the available information allows us to restrict the candidates to just one of the two possibilities. For example, we cannot derive an extLeak in a son node whose qualitative deviations for the input and the output flow are known to be equal.

7.5 Control

In this Section, we sketch how the three classes of axioms are used in reasoning, which is organized in three steps.

In the first step, value mapping axioms are used to translate observations at all reachable levels of detail (as seen in Section 7.2).

The purpose of the second and the third step is to generate the candidates explaining the given observations. Each node of the SPS tree has initially an associated empty candidate. At each iteration of the second and the third step, partial candidates are generated and associated to nodes, providing an explanation of some given observations. Each node can obviously have more than one partial candidate associated to it if there are different faults that explain the situation.

More specifically, the second step pairs a node and a partial (possibly empty) candidate associated to it and applies fault generation axioms to refine the partial candidate. The choice of the pair is based on the following criteria:

(i) only nodes for which there are deviations to explain are considered;
(ii) the choice of a node for refinement of a partial candidate is prevented if the candidate already explains the faulty situation for that node (in other words, if at least one of the fault generation axioms applicable to the node would derive again the same explanation for the faulty situation). The choice of descendants of the node for refinement of that candidate is also prevented;
(iii) axioms applicable to nodes where there is evidence of fault are preferred (this criterion is defined precisely in the following); and
(iv) nodes at finer levels of detail are preferred to those at coarser levels.

After fault generation axioms are applied to a node for refining a partial candidate, the choice of descendants of the node for refinement of the same candidate is prevented.

In the third step, the partial candidates derived by the second step are mapped to other nodes of the SPS tree (as discussed in Section 7.4), thus obtaining the counterpart of the hypothesized faults at the different levels of detail. The mapping is performed both upwards (to prevent application of some axioms), and downwards (to generate candidates at the component level).

The second and third steps are repeated until step two is no more able to choose a node with an associated partial candidate to be refined.

In order to determine evidence of fault for criterion (iii), at least one of the three following constraints (which characterize normality) must be violated:

$$\text{node(N)} \wedge \neg\text{barrier(N)} \Rightarrow$$
$$[\Delta F_{in}(N)] = [\Delta F_{out}(N)] \wedge [\Delta E_{in}(N)] = [\Delta E_{out}(N)]$$

$$\text{barrier(N)} \Rightarrow$$
$$[\Delta F_{in}(N)] = [\Delta F_{out}(N)] = [0]$$

$$\text{generator(N,L)} \wedge \neg\text{barrier(L)} \Rightarrow$$
$$[\Delta F_{in}(N)] = [\Delta F_{out}(N)] = [0]$$

$$\text{parallel(PA,N1,N2)} \wedge \neg\text{barrier(N1)} \wedge \neg\text{barrier(N2)} \Rightarrow$$
$$[\Delta F_{in}(N1)] = [\Delta F_{in}(N2)] = [\Delta F_{out}(N1)] = [\Delta F_{out}(N2)]$$

In particular, a situation in which the fourth constraint is violated occurs when the qualitative deviations of the two flows in a parallel are different from each other. When the four observations are not all available and the available ones do not violate the constraint, it is still possible to exploit information available at lower levels in order to recognize the evidence of fault: if the qualitative deviations of flows available for the descendants of the left node have all the same value V1 (e.g. [−]), and those available for the descendants of the right node have all the same value V2 (e.g. [+]), and V1 is different from V2, then there is evidence of fault. This indeed characterizes a situation where the resistance of one of the two branches of the parallel has changed with respect to nominal conditions.

Finally, if there is evidence of fault in a node, then there is evidence of fault in every ancestor of that node.

We can now continue and conclude the two diagnostic examples from the previous sections.

7.5.1 Example A

Axiom FG2 applied to v2 is preferred because it fully matches a situation where there is evidence of fault and it also applies to the finest level of detail. In this way, the partial candidate fault(v2,intleak) is derived. Then, the obtained partial candidate is mapped by fault mapping axioms FM11 and FM10, deriving its abstract counterparts at every upper level., i.e. fault(se5,intLeak), fault(se3, intleak), fault(pa1,intleak), fault(se2,intleak), and fault(se1,

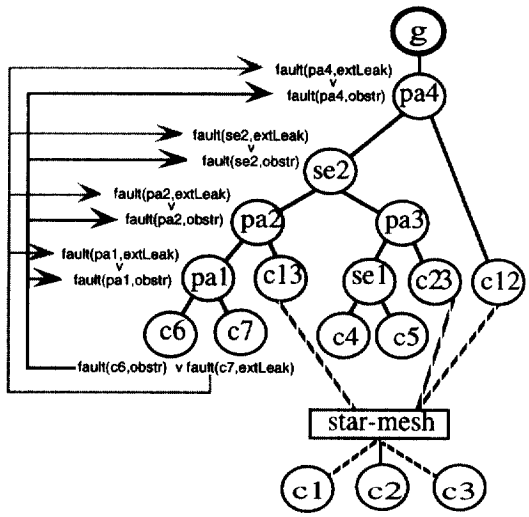

Fig. 9. Linking partial candidates at multiple levels.

intleak). The second reasoning step is now not able to choose a further node, because axiom FG4 applied to node pa1 would produce candidate fault(se3,intleak), i.e. again the same explanation for the faulty situation. This prevents the choice of node pa1 and its descendants for the refinement of the current partial candidate. As a consequence, no other axiom is applied, and the generated candidate at the component level {fault(v2,intleak)} is the only final candidate.

7.5.2 Example B

Axioms FG3 and FG7 applied to pa1 are both deemed more relevant than the other axioms, because they refer to a node where there is evidence of fault, and the node is at the finest level of detail among those nodes which present evidence of fault. They produce two different partial candidates to explain the faulty situation at node pa1: fault(c7,extleak), or fault(c6,obstr). The two partial candidates are mapped to upper levels (by FM4, FM6, FM1, and FM3): Fig. 9 shows with gray arrows the upward mapping of fault(c7, extleak), and with black arrows the upward mapping of fault(c6, obstr).

When the first of the two possible value mappings from the star to the mesh level (i.e. $[\Delta F_{in}(c12)] = [\ -\ ]$) is considered, node pa4 is chosen for refinement of the partial candidates associated to it, because there is a deviated value (i.e. $[\Delta F_{in}(c12)] = [\ -\ ]$) that refers to one of its sons, and there is evidence of fault for it (it is an ancestor of node pa1). Considering the first of the two partial candidates associated to pa4 (see Fig. 9), i.e. fault(pa4,extLeak) mapped from fault(c7,extLeak), the application of other axioms to node pa4 and its descendants is prevented, because axiom FG3 applied to pa4 would produce fault(se2, extLeak), i.e. again the same explanation. Therefore, {fault(c7,extLeak)} is sufficient to explain the current observations and thus belongs to the final candidate set at the component level. On the contrary, considering the second partial candidate associated to node pa4, i.e. fault(pa4,obstr) mapped from fault(c6,obstr), no fault generation axioms applicable to pa4 would derive again the same explanation for the faulty situation, and the refinement has to proceed. The two axioms (FG7 and FG3) applicable to pa4 are thus considered. Axiom FG7 hypothesizes an obstr in c12. This fault is mapped downwards (by FM12) into an obstr in c1 or c2. The additional final candidates are then {fault(c6,obstr), fault(c1,obstr)}, and {fault(c6,obstr), fault(c2,obstr)}. Fig. 10 illustrates the context of this last reasoning step: it shows that the partial candidate under current refinement (i.e. fault(pa4, obstr)) has been obtained by upward mapping from fault(c6, obstr), and then completed by adding fault(c12, obstr), which is mapped downwards, deriving two different possibilities at the component level. An alternative refinement of partial candidate fault(pa4,obstr) is obtained with the application of FG3 to pa4, hypothesizing an extLeak in se2. This fault is mapped downwards (by FM6) into an extLeak in pa2 or pa3, which is mapped (by FM4, FM6, FM13, and FM14) to the leaf nodes. The additional minimal candidates added to the final candidate set are: {fault(c6,obstr), fault(c4,extLeak)}, {fault(c6,obstr), fault(c5, extLeak)}.

When the second of the two possible value mappings from the star to the mesh level (i.e. $[\Delta F_{in}(c13)] = [\ -\ ]$) is considered, node pa2 is chosen for refinement of the partial candidates associated to it, because there is a deviated value (i.e. $[\Delta F_{in}(c13)] = [\ -\ ]$) that refers to one of its sons, and there is evidence of fault for it (it is an ancestor of node pa1). Considering the first of the two partial candidates associated to pa2 (see Fig. 9), i.e. fault(pa2, extLeak) mapped from fault(c7,extLeak), the application of other axioms to node pa2 and its descendants is prevented, because axiom FG3 applied to pa2 would produce fault(pa1, extLeak), i.e. again the same explanation. Since the final candidate {fault(c7,extLeak)} has been already produced, no candidate is added to the final candidate set. Considering node pa2 and the second partial candidate associated to it, i.e. fault(pa2,obstr) mapped from fault(c6,obstr), no fault generation axioms applicable to pa2 would derive again the same explanation for the faulty situation, and the refinement has to proceed. The two instances of axioms applicable to pa2 are thus considered. Axiom FG7 hypothesizes an obstr in c13. This fault is mapped downwards (by FM12) into an obstr in c1 or c3. The additional final candidate is then {fault(c6,obstr), fault(c3,obstr)} (the other one has already been generated). Then, FG3 applied to pa2 hypothesizes an extLeak in pa1. This fault does not add any candidate to the final candidate set, because the candidate {fault(c6,obstr), fault(c7,extLeak)} is not minimal and {fault(c6,obstr), fault(c6,extLeak)} is not a valid candidate (component c6 cannot obviously be in two alternative states at the same time).

The final candidate set at the component level thus contains the following 6 diagnoses: {fault(c7,extLeak)}, {fault(c6,obstr), fault(c1,obstr)}, {fault(c6,obstr), fault(c2, obstr)}, {fault(c6,obstr), fault(c3,obstr)}, {fault(c6,obstr), fault(c4,extLeak)}, {fault(c6,obstr), fault(c5, extLeak)}.

8 FORMAL VALIDATION OF DIAGNOSTIC KNOWLEDGE

The axioms employed by the diagnostic system have been validated on the basis of fundamental balance equations. In this section, we first introduce the balance equations used in the proofs, and then we present the detailed proofs of three diagnostic axioms.

8.1 Balance equations

In the following, we briefly present the conservation equations for mass and energy which have been used in the validation of axioms. A detailed description of these equations can be found in any fundamental textbook on process fluid mechanics, e.g. Denn.[19]

The *mass conservation equation* (continuity equation) for incompressible fluids states that in a system (or control volume), the inlet mass flow rate is equal to the outlet mass flow rate. In a generic system with n inlet flows and m outlet flows, the continuity equation is:

$$\sum_{i=1}^{n} w_{\text{in},i} = \sum_{j=1}^{m} w_{\text{out},j} \tag{2}$$

where w is the flow rate, defined as

$$w = vA\rho \tag{3}$$

in which v is the fluid velocity, A is the flow cross-section, and ρ is the fluid density. Applying equation (2) to the adopted SPS tree representation, we obtain for each node N in the tree:

$$\tilde{F}_{\text{in}}(N) = \tilde{F}_{\text{out}}(N) \tag{4}$$

While equation (4) always holds, $F_{\text{in}}(N) = F_{\text{out}}(N)$ holds only under the assumption of absence of leaks in N.

The form of the *energy conservation equation* we will use is the Bernoulli equation, which is normally employed to solve piping systems and holds under the following broad hypotheses: (1) steady flow; (2) Newtonian fluid (i.e. fluid with constant viscosity); (3) application along a flow tube (i.e. in a network, it has to be applied to components characterized by a uniform, possibly averaged, diameter). The Bernoulli equation for an incompressible fluid applied to a flow tube reads:

$$\frac{1}{2}\left(v_{\text{out}}^2 - v_{\text{in}}^2\right) + \frac{p_{\text{out}} - p_{\text{in}}}{\rho} + g\left(h_{\text{out}} - h_{\text{in}}\right) + \Phi w^{\mu} + \phi w^{\lambda} = 0 \tag{5}$$

The first term represents the difference between the outlet and the inlet kinetic energy, the second term represents the pressure gradient, the third term is the gravity head (where h is elevation), while the fourth and fifth terms are dissipation terms. The term Φw^{μ} is the energy dissipated by *friction over pipe walls*, where Φ is a positive coefficient, function of the overall geometry of the pipe (diameter, length, and roughness of the walls) and fluid properties (density and viscosity), and μ is a coefficient between 1 and 2. In the present context, the coefficient Φ can change only due to external leaks. The term ϕw^{λ} represents all energy losses due to the presence of *localized flow variations*, such as curves, valves, flow reductions or enlargements, and obstructions; the coefficient λ is usually considered equal to 2, and ϕ is represented by:

$$\phi = \sum_i k_i$$

where the k_i are empirically derived positive coefficients each one accounting for a different localized energy loss.

If localized energy losses, for instance those due to obstructions, arise, they can be accounted for by additional k_i coefficients, thus varying the value of the coefficient ϕ from nominal conditions. In the present work, all axioms are derived under the reasonable assumption that fluid properties do not change except locally. The effect of local variations can be thus suitably represented by a change of the ϕ coefficient.

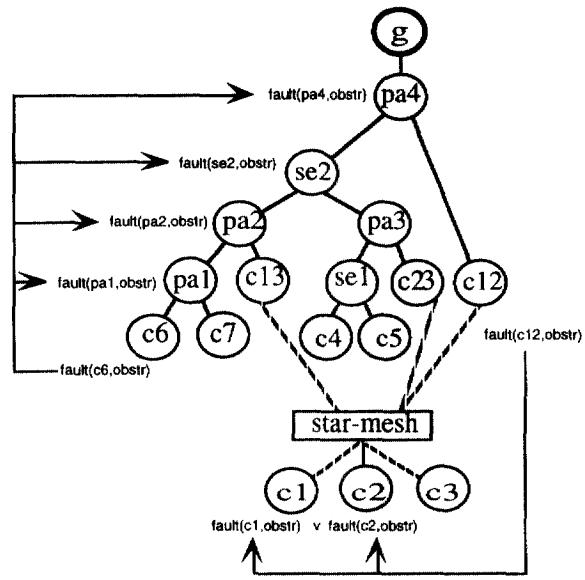

Fig. 10. Refinement of partial candidate fault(c6,obstr).

8.2 Proofs of correctness

The axioms employed by the diagnostic system have been validated on the basis of the previously introduced equations. As an example of how the validation has been performed, we present in the following, the proofs of correctness for FG1, FG7, and FG8.

Since balance equations refer to real-valued quantities, they cannot be directly applied to the qualitative-valued quantities used in the axioms. Therefore, we need to consider in every proof the relation between the qualitative and quantitative values of variables.

Instead of translating the quantitative laws into their qualitative counterparts and then trivially showing their consistency with the qualitative axioms, we choose to maintain them in their quantitative form. This approach allows us to detect and point out where and how the qualitative

representation is a source of incompleteness: in these cases, since the quantitative equations take into account a number of possibilities larger than their qualitative counterparts, it becomes necessary to explicitly state the restrictions imposed by the qualitative representation in order to proceed with the proof.

8.3 Axiom FG1

This is an interesting case where qualitative information is sufficient to conclude that a fault is necessarily present, and the proof does not require any restriction to the scope of quantitative laws:

$$\text{fault(N,extLeak)} \Leftarrow \text{node(N)} \wedge [\Delta F_{in}(N)] > [\Delta F_{out}(N)] \quad \text{(FG1)}$$

Proof

The observation $[\Delta F_{in}(N)] > [\Delta F_{out}(N)]$ obviously implies $\Delta F_{in}(N) > \Delta F_{out}(N)$, i.e.

$$F_{in}(N) - \tilde{F}_{in}(N) > F_{out}(N) - \tilde{F}_{out}(N)$$

Applying equation (4), we simplify the inequality, obtaining:

$$F_{in}(N) > F_{out}(N)$$

which indicates a mass deficit, necessarily due to an external leak inside N.

8.4 Axiom FG7

This is a case where qualitative information restricts the number of possible hypothesizable faults, and the proof thus requires a restriction to the scope of quantitative laws:

$$\begin{aligned}\text{fault(N2,obstr)} \Leftarrow\ & \text{parallel(PA,N1,N2)} \\ \wedge\ & \neg\text{barrier(N1)} \\ \wedge\ & \neg\text{barrier(N2)} \wedge [\Delta F_{in}(N1)] = [\Delta F_{out}(N1)] \\ \wedge\ & [\Delta F_{in}(N2)] = [\Delta F_{out}(N2)] \\ \wedge\ & [\Delta F_{in}(N1)] > [\Delta F_{in}(N2)] \quad \text{(FG7)}\end{aligned}$$

Proof

The application of equation (5) to the parallel of two flows gives:

$$\begin{aligned}&\frac{1}{2}\left(v_{N1,out}^2 - v_{N1,in}^2\right) + \frac{p_{PA,out} - p_{PA,in}}{\rho} \\ &\quad + g\left(h_{PA,out} - h_{PA,in}\right) + \Phi_{N1}F(N1)^{\mu} + \phi_{N1}F(N1)^{\lambda} \\ &= \frac{1}{2}\left(v_{N2,out}^2 - v_{N2,in}^2\right) + \frac{p_{PA,out} - p_{PA,in}}{\rho} \\ &\quad + g\left(h_{PA,out} - h_{PA,in}\right) + \Phi_{N2}F(N2)^{\mu} + \phi_{N2}F(N2)^{\lambda}\end{aligned}$$

By removing identical terms from the left and right part of the equation, we obtain the expression:

$$\begin{aligned}&\frac{1}{2}\left(v_{N1,out}^2 - v_{N1,in}^2\right) + \Phi_{N1}F(N1)^{\mu} + \phi_{N1}F(N1)^{\lambda} \\ &= \frac{1}{2}\left(v_{N2,out}^2 - v_{N2,in}^2\right) + \Phi_{N2}F(N2)^{\mu} + \phi_{N2}F(N2)^{\lambda}\end{aligned}$$

As pointed out before, when the qualitative values of the inlet and outlet flow rate for a node are equal, it is not possible to hypothesize an external leak in the node. Since in the considered case $[\Delta F_{in}(N1)] = [\Delta F_{out}(N1)]$ and $[\Delta F_{in}(N2)] = [\Delta F_{out}(N2)]$, we restrict our attention to the case where external leaks in N1 and N2 are excluded, i.e. $F_{in}(N1) = F_{out}(N1)$ and $F_{in}(N2) = F_{out}(N2)$. From equation (3), we can conclude that $v_{N1,in} = v_{N1,out}$, and $v_{N2,in} = v_{N2,out}$. Thus, we can remove the velocities from the expression. Moreover, since external leaks are excluded, Φ_{N1} and Φ_{N2} do not change with respect to nominal conditions, and we obtain:

$$\tilde{\Phi}_{N1}F(N1)^{\mu} + \phi_{N1}F(N1)^{\lambda} = \tilde{\Phi}_{N2}F(N2)^{\mu} + \phi_{N2}F(N2)^{\lambda}$$

Analogously, the application of equation (5) to the considered parallel flows in nominal condition yields:

$$\tilde{\Phi}_{N1}\tilde{F}(N1)^{\mu} + \tilde{\phi}_{N1}\tilde{F}(N1)^{\lambda} = \tilde{\Phi}_{N2}\tilde{F}(N2)^{\mu} + \tilde{\phi}_{N2}\tilde{F}(N2)^{\lambda}$$

Subtracting the two previous expressions and considering that $\phi = \tilde{\phi} + \Delta\phi$ (equation 1), we obtain:

$$\begin{aligned}&\tilde{\Phi}_{N1}\left(F(N1)^{\mu} - \tilde{F}(N1)^{\mu}\right) + \tilde{\phi}_{N1}\left(F(N1)^{\lambda} - \tilde{F}(N1)^{\lambda}\right) \\ &\quad + \Delta\phi_{N1}F(N1)^{\lambda} \\ &= \tilde{\Phi}_{N2}\left(F(N2)^{\mu} - \tilde{F}(N2)^{\mu}\right) + \tilde{\phi}_{N2}\left(F(N2)^{\lambda} - \tilde{F}(N2)^{\lambda}\right) \\ &\quad + \Delta\phi_{N2}F(N2)^{\lambda} \quad (6)\end{aligned}$$

Since it has been observed that $[\Delta F_{in}(N1)] > [\Delta F_{in}(N2)]$ and external leaks are excluded, we know that $[\Delta F(N1)] > [\Delta F(N2)]$, i.e.

$$\left[F(N1) - \tilde{F}(N1)\right] > \left[F(N2) - \tilde{F}(N2)\right]$$

Therefore, it is also

$$\left[F(N1)^{\mu} - \tilde{F}(N1)^{\mu}\right] > \left[F(N2)^{\mu} - \tilde{F}(N2)^{\mu}\right]$$

from which we derive:

$$\left[\Phi_{N1}\left(F(N1)^{\mu} - \tilde{F}(N1)^{\mu}\right)\right] > \left[\Phi_{N2}\left(F(N2)^{\mu} - \tilde{F}(N2)^{\mu}\right)\right]$$

which obviously implies

$$\Phi_{N1}\left(F(N1)^{\mu} - \tilde{F}(N1)^{\mu}\right) > \Phi_{N2}\left(F(N2)^{\mu} - \tilde{F}(N2)^{\mu}\right)$$

Similarly, we obtain:

$$\tilde{\phi}_{N1}\left(F(N1)^{\lambda} - \tilde{F}(N1)^{\lambda}\right) > \tilde{\phi}_{N2}\left(F(N2)^{\lambda} - \tilde{F}(N2)^{\lambda}\right)$$

Finally, from the last two inequalities and equation (6), we conclude:

$$\Delta\phi_{N1}F(N1)^{\lambda} < \Delta\phi_{N2}F(N2)^{\lambda}$$

This inequality is verified by additional localized energy losses (obstructions) in both nodes (i.e. $\Delta\phi_{N1} > 0$, and $\Delta\phi_{N2} > 0$) or just in node N2 (i.e. $\Delta\phi_{N2} > 0$, and $\Delta\phi_{N1} = 0$). Since the first of these two faults is not minimal, it is sufficient to generate the second one (obstruction in N2).

As a matter of fact, the elimination of a localized energy loss in N1 ($\Delta\phi_{N1} < 0$) could verify the inequality as well.

This third possible explanation does not belong to the five classes of considered faults, and thus is not hypothesized.

8.5 Axiom FG8

In this case, we consider an axiom which involves also efforts, and not only flows.

$$\begin{aligned}&\text{fault(N,obstr)} \Leftarrow \text{node(N)} \wedge \neg\text{barrier(N)}\\ &\wedge\ [\Delta E_{in}(N)] = [+] \wedge [\Delta E_{out}(N)] \leq [0]\\ &\wedge\ [\Delta F_{in}(N)] = [\Delta F_{out}(N)] \leq [0] \qquad \text{(FG8)}\end{aligned}$$

Proof

From the observation that $[\Delta F_{in}(N)]$ and $[\Delta F_{out}(N)]$ are equal, it is not possible to hypothesize an external leak in N. We thus restrict our attention to the case where external leaks in N are excluded, i.e. $F_{in}(N) = F_{out}(N)$. From equation (3), we derive $v_{N,out} = v_{N,in}$. Therefore, the application of the Bernoulli equation to the node gives:

$$\frac{p_{N,out} - p_{N,in}}{\rho} + g\left(h_{N,out} - h_{N,in}\right) + \Phi_N F(N)^{\mu} + \phi_N F(N)^{\lambda} = 0$$

In nominal conditions, the application of the Bernoulli equation to the node yields:

$$\frac{\tilde{p}_{N,out} - \tilde{p}_{N,in}}{\rho} + g\left(\tilde{h}_{N,out} - \tilde{h}_{N,in}\right) + \tilde{\Phi}_N \tilde{F}(N)^{\mu} + \tilde{\phi}_N \tilde{F}(N)^{\lambda} = 0$$

Since external leaks in N are excluded, Φ_N does not change with respect to its nominal value. Since significant changes of elevation in components occurring during the operation of the system are not covered by the classes of faults we are interested in, we can assume that the gravitational term in the expressions does not change with respect to nominal conditions (i.e. $\Delta h = 0$). Therefore, subtracting the two previous expressions and considering that $\phi = \tilde{\phi} + \Delta\phi$, we obtain:

$$\frac{\Delta p_{N,out}}{\rho} - \frac{\Delta p_{N,in}}{\rho} + \tilde{\Phi}_N\left(F(N)^{\mu} - \tilde{F}(N)^{\mu}\right) + \tilde{\phi}_N\left(F(N)^{\lambda} - \tilde{F}(N)^{\lambda}\right) + \Delta\phi_N F(N)^{\lambda} = 0 \qquad (7)$$

Reasoning as in the previous proof, it can be shown that $[\Delta F_{in}(N)] \leq [0]$ and $[\Delta F_{out}(N)] \leq [0]$ imply:

$$\tilde{\Phi}_N\left(F(N)^{\mu} - \tilde{F}(N)^{\mu}\right) \leq 0$$

$$\tilde{\phi}_N\left(F(N)^{\lambda} - \tilde{F}(N)^{\lambda}\right) \leq 0$$

Since $[\Delta E_{in}(N)] = [+]$ and $[\Delta E_{out}(N)] \leq [0]$, then the term $-\frac{\Delta p_{N,in}}{\rho}$ in equation (7) is negative, while the term $\frac{\Delta p_{N,out}}{\rho}$ is less than or equal to zero.

In order for equation (7) to be verified, it must thus be:

$$\Delta\phi_N F(N)^{\lambda} > 0$$

This inequality is verified by additional localized energy losses (obstruction) in the node (i.e. $\Delta\phi_N > 0$).

9 DISCUSSION

A previous work[3] compared the initial version of FDef with ATMS-based diagnostic approaches, such as GDE,[14] concluding that FDef traded some generality for more simplicity and efficiency of reasoning. The new approach we have presented in this paper preserves this feature, and also succeeds in improving FDef generality, by relaxing some of the strong assumptions which underlied the initial version of FDef. The three main assumptions of the initial version of FDef were:

(i) representability of the system to be diagnosed in terms of flow structures;
(ii) restriction to presence/absence observations; and
(iii) restriction to three classes of faults (all resulting in total loss of functionality).

The novel approach we have proposed in this paper loosens the last two restrictions. First, it moves from the presence/absence quantity space to a more expressive quantity space, which increases the set of recognizable symptoms to include partial losses of functionality. Second, it introduces a fault generation mechanism based on axioms which are not only able to identify partial losses of functionality, but can also be developed and validated more easily. Indeed, while the initial version of FDef relied on axioms which had to start from a single observation and produce global explanations for it (involving the whole model), the new fault generation axioms can be developed by limiting the attention to a single node of the SPS tree and the observations which refer to it. Moreover, the axioms for the initial version of FDef were not just difficult to develop, but were difficult to validate formally, and to extend in order to cover more classes of faults. With the new axioms, we have increased the number of classes of faults handled by the approach, covering all the faults we were interested in the present research, and we have also verified that it is not difficult to formally validate them starting from fundamental balance equations (as shown previously).

As mentioned before, reasoning with the proposed approach is more efficient and simpler than the more general ATMS-based approaches. To show this in practice, we consider a situation which turns out to be problematic for ATMS-based systems: consider the system depicted in Fig. 11, and suppose that all switches are open and the bulb is on nevertheless. This problem has been proposed by Nejdl and Giefer,[20] who point out that an ATMS-based in this case generates 2^n minimal conflict sets, each one comprising n elements (one switch from each of the n branches), in order to generate the n minimal diagnoses (i.e. both switches are faulty in one of the n branches). In the following, we apply our approach to this example, showing the detailed reasoning for the case of 8 switches over 4 parallel branches ($n = 4$). Fig. 12 provides the SPS tree over which reasoning takes place.

Example C. The available observation is represented as $[\Delta F_{out}(b)] = [+]$. From this observation, value mapping

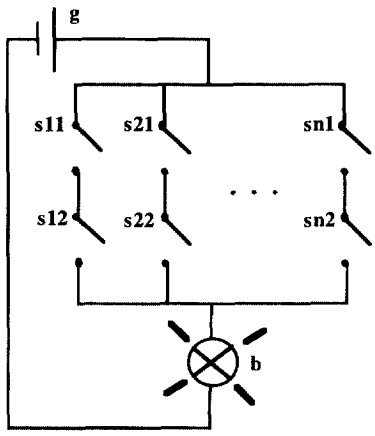

Fig. 11. Critical example.

axioms VM1 and VM7, and the propagation activity of Section 7.1, reach the following conclusions: $[\Delta F_{in}(b)] = [+]$, $[\Delta F_{out}(pa1)] = [+]$, $[\Delta F_{in}(pa1)] = [+]$, $[\Delta F_{out}(se1)] = [+]$, $[\Delta F_{in}(se1)] = [+]$, and $[\Delta F_{out}(g)] = [+]$. The applicable axioms are: FG2 to pa1 (hypothesizing an internal leak in pa1), and FG2 to se1 (internal leak in se1). Axiom FG2 applied to pa1 is preferred because it fully matches a situation where there is evidence of fault and it applies to the finest level of detail. In this way, the partial candidate fault(pa1,intLeak) is derived. Then, the obtained partial candidate is mapped by fault mapping axiom FM10, deriving its abstract counterparts at the upper level., i.e. fault(se1,intLeak). The detailed diagnoses at the component level are generated by using axioms FM8 amd FM9, obtaining the following four candidates: {fault(s41,intLeak), fault(s42,intLeak)}; {fault(s31,intLeak), fault(s32,intLeak)}; {fault(s21, intLeak), fault(s22,intLeak)}; and {fault(s11,intLeak), fault(s12,intLeak)}. The second reasoning step is now not able to choose a further node, because axiom FG2 applied to node se1 would produce candidate fault(se1,intLeak), i.e. again the same explanation for the faulty situation. As a consequence, no other axiom is applied.

As it can be seen in this and the previous examples, unlike ATMS-based systems, our approach skips completely conflict generation (and thus does not generate conflicts at all), and directly identifies the fault at the most appropriate level in the tree, mapping it into the correct candidates. This mapping activity is not exponential, but linear in the number of parallel branches of the example.

Incidentally, the discussed case provides also an example of application to a non-hydraulic system. The application is correct as long as the battery is considered as a generator of current, because the fault generation axioms presented in this paper deal with generators of flow.

Another important advantage of the diagnostic reasoning of our proposed approach, is that, unlike ATMS-based systems, it remains close to the expert way of reasoning. Indeed, a simple trace of the axioms actually applied by the system to reach its conclusions is easily understood by the expert. Consider again example C: first, the system concludes that since the bulb is lit, there must be an internal leak in the parallel of the four branches; then it maps this conclusion at the most detailed level, determining that both switches of one of the branches must be internally leaking.

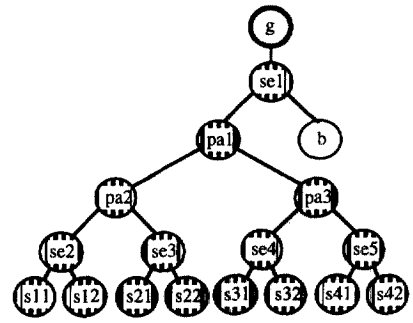

Fig. 12. SPS tree for the four parallel branches case.

Finally, we would like to note that the adoption of the hierarchical SPS model representation improves reasoning with respect to both the initial version of FDef and to traditional model-based approaches, by allowing for a more focused diagnostic process. The proposed control algorithm is indeed able to focus its attention on those subparts of the system where the fault is likely to be located, also choosing the more appropriate level of granularity. This is again evident in example C, where, regardless of the number of branches in the system, FDef will always identify the fault at the node which abstracts all the branches.

10 CONCLUSIONS

In this paper, we have shown first the results of our experiments in functional diagnosis of a real-world case study (the HFOTS) with binary presence/absence observations about flows and efforts. Then, we have analysed critically those results, and shown how the approach can be significantly improved by representing and reasoning about deviations of variables. The new approach is both more general and more competent than the previous one. We have also exploited a proper organizing structure to reason about the model, and formally validated the diagnostic knowledge. These activities have been partly discussed in the paper.

The new version of FDef presented in this paper has been implemented in PROLOG and is currently being tested not only on the HFOTS, but also on case studies of FTS taken from hydraulics textbooks.

Our current research work focuses on further improving the approach and is mainly concentrated on three goals.

First, we are working at removing the restriction to volumetric pumps. As we have seen, volumetric pumps deliver the same flow rate regardless of the pressure drop they have to face. Volumetric pumps are used in the oil industry because they can handle fluids of extremely high viscosity, as in the application which prompted our initial study. However, extension of the approach to other types of pumps is relatively easy, and requires the formulation of new fault generation axioms which could take into account pumps

which act as generators of pressure. Such axioms would also cover other components in other domains (such as electrical voltage generators).

Second, besides verifying the correctness of the fault generation axioms (as shown in the paper), we are studying the problem of completeness (i.e. ensuring that a given set of axioms is able to produce all the candidates belonging to the considered classes of faults, which are detectable using the adopted quantity space).

Third, we aim at extending the approach to other relevant aspects of FTS, such as heat transfer (for example, in the HFOTS case study, a possible cause of solidification of fuel is a fault in a connected heating system). This development will be achieved through the introduction of influences (i.e. relations between interacting primitives belonging to different flow-structures) in the representation, and through the exploitation of the reasoning-about-influences technique we presented elsewhere.[11] However, since the technique is able to handle influences only with presence/absence observations, it needs to be generalized to handle the deviation quantity space adopted in this paper.

ACKNOWLEDGEMENTS

One of the anonymous referees provided very useful comments to the preliminary version of this paper. We are also indebted to Joaquín López Cortés (Department of Energy Systems and Marine Engineering, Technical University of Hamburg-Harburg), who provided the HFOTS case study, and many clarifications about its functioning.

REFERENCES

1. Chittaro, L., Fabbri, R. & López Cortés, J. Functional diagnosis goes to the sea: applying FDef to the heavy fuel oil transfer system of a ship. In *Proceedings of FLAIRS-96*, Key West, FL, USA. Florida Artificial Intelligence Research Society, 1996, pp. 419–423.
2. Chandrasekaran, B. Functional representation and causal processes. *Advances in Computers*, 1994, **38**, 73–143.
3. Chittaro, L. Functional diagnosis and prescription of measurements using effort and flow variables. *IEE Control Theory and Applications*, 1995, **142**, 420–432.
4. Hawkins, R., Sticklen, J., McDowell, J. K., Hill, T. and Boyer, R. Function-based modeling and troubleshooting. *Applied Artificial Intelligence*, 1994, **8**, 285–302.
5. Hunt, J., Pugh, D. and Price, C. Failure mode effects analysis: a practical application of functional modeling. *Applied Artificial Intelligence*, 1995, **9**, 33–44.
6. Kumar, A. N. and Upadhyaya, S. J. Function based discrimination during model-based diagnosis. *Applied Artificial Intelligence*, 1995, **9**, 65–80.
7. Larsson, J. E. Diagnosis based on explicit means-end models. *Artificial Intelligence*, 1996, **80**, 29–93.
8. Lind, M. Modeling goals and functions of complex industrial plants. *Applied Artificial Intelligence*, 1994, **8**, 259–284.
9. Chittaro, L., Guida, G., Tasso, C. and Toppano, E. Functional and teleological knowledge in the multimodeling approach for reasoning about physical systems: a case study in diagnosis. *IEEE Transactions on Systems, Man, and Cybernetics*, 1993, **23**, 1718–1751.
10. López Cortés, J. & Michaelsen, A. A methodological framework for modelling complex technical marine systems for diagnostic purposes. In *Proceedings of the 2nd IEE Intelligent Systems Engineering Conference*, Hamburg, Germany. IEE Press, Stevenage, UK, 1994, Part D, pp. 298–303.
11. Chittaro, L. & Ranon, R. Augmenting the diagnostic power of flow-based approaches to functional reasoning. In *Proceedings AAAI-96: 13th Conference of The American Association for Artificial Intelligence*, Portland, OR, USA. MIT Press, Cambridge, MA, 1996, pp. 1010–1015.
12. Rasmussen, J. *Information Processing and Human–Machine Interaction. An Approach to Cognitive Engineering*. North-Holland, Amsterdam, 1986.
13. Paynter, H.M. *Analysis and Design of Engineering Systems*. MIT Press, Cambridge, MA, 1961.
14. de Kleer, J. and Williams, B. C. Diagnosing multiple faults. *Artificial Intelligence*, 1987, **32**, 97–130.
15. Malik, A. & Struss, P. Diagnosis of dynamic systems does not necessarily require simulation. In *Proceedings DX-96: 7th International Workshop on Principles of Diagnosis*, Val Morin, Canada. NRC-CNRC, 1996, pp. 147–156.
16. Williams, B. C. and Nayak, P. P. Immobile robots: AI in the new millenium. *AI Magazine*, 1996, **17**, 17–35.
17. Chen, W. K. *Applied Graph Theory: Graphs and Electrical Networks*. North Holland, 2nd Revised Edition, 1976.
18. Mauss, J. & Neumann, B. Qualitative reasoning about electrical circuits using series-parallel-star trees. *Proceedings ECAI-96: Workshop on Model-based Systems and Qualitative Reasoning*, ECCAI, Budapest, Hungary. 1996.
19. Denn, M. M. *Process Fluid Mechanics*. Prentice Hall, Englewood Cliffs, NJ, 1980.
20. Nejdl, W. & Giefer, B. DRUM: reasoning without conflicts and justifications. In *Proceedings DX-94: 5th International Workshop on Principles of Diagnosis*, New Paltz, NY, USA. 1994, pp. 226–233.