# Another Point of View on Diagnosability

**Xavier Pucel, Louise Travé-Massuyès, Yannick Pencolé**
LAAS-CNRS ; Université de Toulouse ; 7, avenue du Colonel Roche, F-31077 Toulouse, France
{xpucel, louise, ypencole}@laas.fr

## Abstract

This paper provides a new definition of diagnosability, that allows one to check the diagnosability of any set of system states, and by extension of properties that depend on the system state. The existing definitions and approaches for checking diagnosability apply to faults or sets of faults, and comparison shows that the new definition generalizes the existing ones. This new definition is applied to repair preconditions, and an example shows how this brings complementary information compared to classical fault diagnosability.

## 1 Introduction

Complex and critical systems require close supervision when running, and the model-based community has produced a lot of work in this area. In particular, model-based diagnosis is an increasingly active research domain, and the problem of diagnosability analysis has been addressed many times [Sampath *et al.*, 1995; Cordier *et al.*, 2006; Bayoudh *et al.*, 2006]. In a diagnosable system, although it is impossible to know the exact state of the system, the supervisor is aware of which anticipated faults have happened and which have not. However, the information needed by a supervisor in such systems is not limited to fault presence, and fault diagnosability in a system does not guarantee that this system is easy to supervise. A system designer hence needs to verify the diagnosability of more than just the faults.

This paper presents a definition for diagnosability that can be applied to any set of states in a system. The model used in this paper is state-based, and most properties can be mapped to a set of system states. This provides the possibility to check the diagnosability of state dependent properties. When a property is diagnosable, the system supervisor is always able to assess whether the current system state verifies this property. Fault presence or absence are examples of such state dependent properties. The definition can also be used to perform diagnosability analysis for faults, in the same way as existing approaches do. But its extension to any set of states also allows to check the diagnosability of many other properties, like for example repair preconditions, which is illustrated in this paper.

The existing diagnosability approaches are presented in first place, before the new definition is introduced. This new definition is compared to existing definitions. Finally, an example illustrates the application of the new definition to repair preconditions.

## 2 Related work

Diagnosis has been an active research topic in AI for many years and numerous approaches have been proposed to cope with on-line as well as *post mortem* diagnosis [Hamscher *et al.*, 1992]. More recently a significant trend has moved the activities of the diagnosis community towards the analysis of the properties related to diagnosis. Several pieces of work deal with defining and checking diagnosability [Console *et al.*, 2000; Travé-Massuyès *et al.*, 2001; Travé-Massuyès *et al.*, 2006; Struss and Dressler, 2003; Bayoudh *et al.*, 2006] and a unified characterization bridging state based and event based modeled systems has been proposed [Cordier *et al.*, 2006]. Diagnosability guarantees that all the anticipated faulty situations of a system are discriminable one from the other, although the state of the system is partially observed. This property is quite important because it indicates that the instrumentation providing the observations about the system is well designed and sufficient to provide an explanation of what is going on. However, nowadays systems are required to run more and more autonomously and they are expected to cope with unanticipated situations by themselves, in particular when faults occur. Hence, diagnosability has been more recently addressed together with the requirements for repairability in order to provide a formal definition for self-healability [Cordier *et al.*, 2007].

## 3 Existing diagnosability approaches

This section presents diagnosability approaches existing in the literature, in order to compare them to the new approach defined in section 4. All approaches rely on a formal description of the system behaviour, in the absence and in the presence of faults.

In existing approaches, diagnosability is defined as the ability of a system to exhibit different observations for a predefined set of faults. It is based on the notion of signature, which maps faults to sets of observations.

Alban Grastien, Wolfgang Mayer, and Markus Stumptner, Editors.
Proceedings of the 19$^{\text{th}}$ International Workshop on Principles of Diagnosis (DX-08),
September 22–24, 2008, Blue Mountains, NSW, Australia.

### 3.1 System representation

The system is assumed to be described by a proposition *sd* which can be expressed in propositional logic. The set of models of this proposition is denoted $\mathcal{SD}$, it contains all variable tuples satisfying *sd* and describes the set of all the system states, faulty or non faulty. The set of variables is denoted *V*. Some of the variables characterize the presence or absence of faults, these are called *mode variables*. *O* denotes the set of *observable variables*. Generally, mode variables are not observable. The set *OBS* contains all the possible system observations. In other words, it contains the models of the restriction of *sd* to the variables in *O*.

### 3.2 Faults and fault modes

Various *faults* may occur in the system, modifying its behaviour and possibly making it unable to fulfill its function. Several faults may be present at the same time.

A *fault mode* characterizes the behaviour of the system under a given combination of faults. It assesses the presence of some faults as well as the absence of the other faults. The normal mode is one of the many fault modes, it assesses the absence of all faults. The occurrence of a permanent fault changes the fault mode of the system.

A fault is characterized by one mode variable, whose value indicates whether the fault is present or not. A *fault mode* is identified by a value for the tuple of all mode variables. $\mathcal{SD}_f$ is the description of the fault mode $f$, i.e. the set of states in which the fault mode is verified. As any state belongs to exactly one fault mode, the set of all $\mathcal{SD}_f$ is a partition of $\mathcal{SD}$, as illustrated in Figure 1.

### 3.3 Projection on observable variables

An operation called projection on observable variables and noted $\mathcal{P}_{OBS}$ is used. It takes as input a system state expressed as a variable value tuple, and outputs the tuple of observable variable values obtained in this state. For example, if *V* contains 5 variables, and if the first and third are observable, then:

$$\begin{array}{rccc} \mathcal{P}_{OBS}: & \mathcal{SD} & \rightarrow & OBS \\ & (v_1, v_2, v_3, v_4, v_5) & \rightarrow & (v_1, v_3) \end{array}$$

The inverse projection $\mathcal{P}_{OBS}^{-1}$ is defined from *OBS* to $2^{\mathcal{SD}}$ as follows:

$$\mathcal{P}_{OBS}^{-1}(\sigma) = \{s \in \mathcal{SD}, \mathcal{P}_{OBS}(s) = \sigma\}$$

The projection $\mathcal{P}_{OBS}$ associates a system state to the observation that is received under this state. The inverse projection associates an observation to the set of all states that may have originated this observation. When applied to fault modes, this projection is the base of the classical diagnosability analysis approaches.

### 3.4 Fault mode diagnosability

The classical definition for fault signature and diagnosability is provided now. The definition of diagnosability states that the system cannot produce a common observation under two different fault modes [Cordier *et al.*, 2006].

**Definition 1 (Fault mode Signature and Diagnosability)** *The* signature *of a fault mode $f$ is the set of all possible observations when the system state belongs to the mode $f$.*

$$Sig(f) = \{\mathcal{P}_{OBS}(s), s \in \mathcal{SD}_f\}$$

*A system is* diagnosable *if and only if, $f_1$ and $f_2$ being fault modes:*

$$\forall f_1, f_2 \quad f_1 \neq f_2 \Rightarrow Sig(f_1) \cap Sig(f_2) = \emptyset$$

When diagnosability according to definition 1 holds, the observations emitted by the system always allow one to decide which faults have happened, and which faults have not. But when the signatures of two fault modes intersect, this means that there exists at least one observation that can be emitted by the system under two different fault modes. There are two possible explanations for this observation, and a diagnosis process would output two diagnostic candidates.

### 3.5 Macrofault diagnosability

Another definition of diagnosability is given in [Cordier *et al.*, 2007] as an extension of definition 1. It is based on the notion of *macrofault*, which is a set of fault modes. It is based on the idea that not all pairs of fault modes need to be discriminable: fault modes that do not need to be discriminated one from another are gathered into a macrofault. The set of states in which the macrofault $F_i$ is present is noted $\mathcal{SD}_{Fi} = \bigcup_{f \in F_i} \mathcal{SD}_f$.

This raises a significant difference compared to the previous approach. Whereas fault modes are disjoint, macrofaults may overlap. In the macrofault approach, it is considered that when the system state belongs to several macrofaults, it belongs to an overlapping fault mode, and identifying only one of the macrofaults with certainty is enough for the system to be diagnosable.

In this approach, only covering sets of macrofaults are considered, i.e. sets of macrofaults such that every fault mode belongs to a macrofault. Consequently, there is always at least one present macrofault, whatever the system state is.

**Definition 2 (Macrofault, Characteristic signature)** *A* macrofault *$F_i$ is a set of fault modes. $F_i$ is present if and only if the system is in one of the fault modes $f_j \in F_i$.*

*A* characteristic signature *$cSig(F_i)$ is a set of observations that allow one to assess with certainty that the macrofault $F_i$ is present.*

$$cSig(F_i) \subseteq \Big( \bigcup_{f_j \in F_i} \big(Sig(f_i)\big) \setminus \bigcup_{f_k \notin F_i} \big(Sig(f_k)\big) \Big)$$

Note that there are several possible characteristic signatures for each macrofault. If $O$ is a characteristic signature for a macrofault $F_i$, then any $O' \subseteq O$ is also a characteristic signature for $F_i$.

**Definition 3 (Macrofault Diagnosability)** *A covering set of macrofaults $\{F_i\}$, i.e. a set of macrofaults that cover all the fault modes, is diagnosable if and only if there exists a set of characteristic signatures for these macrofaults that form a partition of OBS.*

Alban Grastien, Wolfgang Mayer, and Markus Stumptner, Editors.
Proceedings of the 19th International Workshop on Principles of Diagnosis (DX-08),
September 22–24, 2008, Blue Mountains, NSW, Australia.

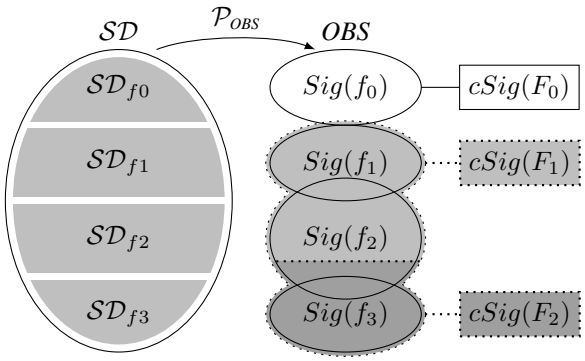



Figure 1: The fault modes $f_0, f_1, f_2, f_3$ are not diagnosable. The set of macrofaults $\{F_0, F_1, F_2\}$ is diagnosable.

When such a partition is established as illustrated in Figure 1, it is always possible to find out at least one present macrofault. As a state may belong to several macrofaults, an observation can also correspond to several macrofaults. However, it is only needed, for each observation, to assess with certainty that one macrofault is present.

This definition is a generalization of definition 1, since fault modes are particular macrofaults. Because macrofaults may overlap when they contain the same fault mode, this definition applies to a greater range of sets of states than the fault mode definition.

This definition is also less constrained than fault mode diagnosability (definition 1), in the sense that in a system verifying fault mode diagnosability, any set of macrofaults is diagnosable.

# 4 Diagnosability revisited

This section presents a new definition of diagnosability, which applies to any state dependent property. It is based upon the analysis of the set of states in which a property holds. It is a generalization of existing diagnosability definitions which only apply to sets of states characterized by the presence or absence of some faults. Comparisons show that this new definition is consistent with the existing ones.

## 4.1 Diagnosability of a property

**Definition 4 (Diagnosable block)** *Let $=_{OBS}$ be the equivalence relation defined on $\mathcal{SD}$ by:*

$$\forall s_1, s_2 \in \mathcal{SD}, s_1 =_{OBS} s_2 \Leftrightarrow \mathcal{P}_{OBS}(s_1) = \mathcal{P}_{OBS}(s_2)$$

*Each equivalence class of $=_{OBS}$ is called a* diagnosable block *of the system. The set of diagnosable blocks of the system is the quotient set of $\mathcal{SD}$ by $=_{OBS}$.*

**Definition 5 (Diagnosability)** *A property or its corresponding set of states $S \subseteq \mathcal{SD}$ is diagnosable if and only if $S$ is exactly a union of diagnosable blocks.*

Figure 2 depicts a system with 7 states and 4 possible observations. The diagnosable blocks are represented by white sets with dashed lines. Observation $o_2$ is received in two different states, one inside $S_1$ and one outside. Thus, when observing $o_2$, a supervisor is unable to decide whether the system is in $S_1$ or not. On the other hand, it is always possible to decide from the observations whether the system state belongs to $S_2$ or not.

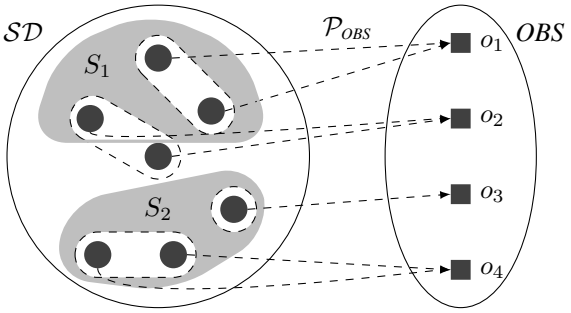



Figure 2: The set of states $S_1$ is not diagnosable. $S_2$ is diagnosable.

## 4.2 Comparison with fault mode diagnosability

Since definition 5 applies to any set of states, it applies in particular to fault modes. It is shown now that when applied to fault modes, this definition is equivalent to definition 1.

**Proposition 1** *A system is diagnosable according to definition 1 if and only if for every fault mode $f$, $\mathcal{SD}_f$ is diagnosable according to definition 5.*

**Proof**

The signatures of two fault modes $f_i$ and $f_j$ intersect if and only if there exists a state $s_i \in \mathcal{SD}_{fi}$ and another state $s_j \in \mathcal{SD}_{fj}$ leading to the same observation. These two states obviously belong to the same diagnosable block, say $d$, and, since $\mathcal{SD}_{fi}$ and $\mathcal{SD}_{fj}$ are disjoint, none is a superset of $d$. Since diagnosable blocks form a partition of $\mathcal{SD}$, $s_i$ (resp. $s_j$) does not belong to any other diagnosable block than $d$. Hence, $\mathcal{SD}_{fi}$ (resp. $\mathcal{SD}_{fj}$) is not a union of diagnosable blocks.

If one fault mode $f_i$ is not a union of diagnosable blocks, then since fault modes form a partition of $\mathcal{SD}$, there exists a diagnosable block $d$ contaning a state $s_i$ of $f_i$ and at least one state $s_j$ belonging to another fault mode $f_j$. These two states lead to the same observation $o$, which necessarily belongs to both $Sig(f_i)$ and $Sig(f_j)$. Consequently the signatures of all fault modes are not disjoint. ■

## 4.3 Signature and preemptability

Definition 5 expresses the diagnosability of a single property. This definition is now extended to a set of properties. For this, the classical notion of signature is extended and the notion of preemptability is introduced. The new definition of the signature applies to sets of states as opposed to definition 1 that applies to fault modes.

**Definition 6 (Signature of a set of states)** *The signature of a set of states $S$, or of the property $p$ mapped to $S$, is the set of observations that can be obtained when the system is under one of these states :*

$$Sig(S) = \{\mathcal{P}_{OBS}(s), s \in S\}$$

Alban Grastien, Wolfgang Mayer, and Markus Stumptner, Editors.
Proceedings of the 19th International Workshop on Principles of Diagnosis (DX-08),
September 22–24, 2008, Blue Mountains, NSW, Australia.

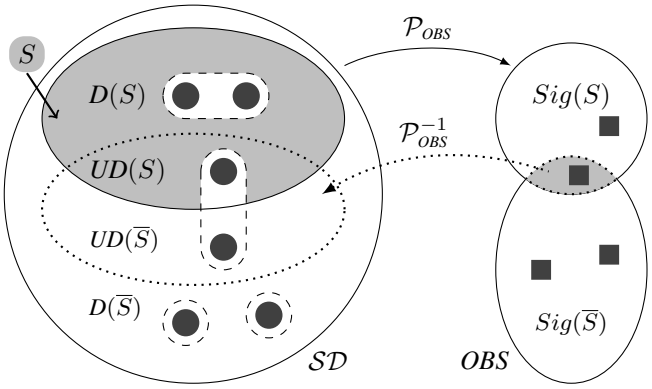



Figure 3: Signature $Sig(S)$, diagnosable space $D(S)$ and undiagnosable space $UD(S)$ of a set of states $S$.

This definition applies equally to the complement set $\overline{S}$. As sets of states generally overlap, comparing their signatures with one another does not bring much information. It is worthy to compare their signatures with the signatures of their respective complements. Indeed, if a set of states corresponds to a given property of the system, its complement corresponds to the negation of the property.

**Definition 7 (Diagnosable space, Undiagnosable space)** *The* diagnosable space $D(S)$ *(resp.* undiagnosable space $UD(S)$*) of a set of states $S$ mapped to a property $p$ is the subset of $S$ in which it is possible (resp. impossible) to assert whether the property $p$ holds.*

$$UD(S) = S \cap \mathcal{P}_{OBS}^{-1}\big(Sig(S) \cap Sig(\overline{S})\big)$$
$$D(S) = S \setminus UD(S)$$

As illustrated in Figure 3, $D(S)$ can also be defined as the union of the diagnosable blocks included in $S$. The diagnosable blocks that intersect but are not included in $S$ form $UD(S) \cup UD(\overline{S})$. The intersection of this set with $S$ gives $UD(S)$. Hence, when a set of states is diagnosable, its undiagnosable space is empty.

When a property $p$ is undiagnosable, it can be preemptable if its undiagnosable space is included in the diagnosable space of other properties. In this case these other properties may preempt $p$ in the sense that when the validity of $p$ is uncertain, one of these other properties is valid, which makes $p$ unnecessary.

**Definition 8 (Preemptability)** *A property or its corresponding set of states $S$ is* preemptable *if and only if:*

$$UD(S) \subseteq \bigcup_{S' \neq S} \big(D(S')\big)$$

Figure 4 illustrates a set $S_0$ whose undiagnosable space is included into two diagnosable sets $S_1$ and $S_2$.

### 4.4 Diagnosability of a set of properties

This section presents a definition of diagnosability for a set of properties that accounts for the mutual influence that properties may have with one another by the means of preemptability.

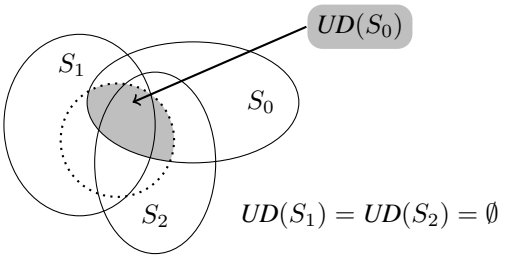



Figure 4: The set of states $S_0$ is preemptable.

**Definition 9 (Diagnosability of a set of properties)** *A set of properties is diagnosable if and only if each property is either diagnosable or preemptable.*

Considering a diagnosable set of properties, the union of all the corresponding sets of states is diagnosable.

Let $S_i$ be the set of states corresponding to the $i$-th property of a diagnosable set of properties. For each $i$, $UD(S_i)$ is either empty or included in the diagnosable sets of other sets of states. Hence, $\bigcup_i S_i = \bigcup_i D(S_i)$ is diagnosable since each $D(S_i)$ is a union of diagnosable blocks.

### 4.5 Comparison with macrofault diagnosability

Now it is shown that definition 9 is equivalent to definition 3 when applied to macrofaults.

**Proposition 2** *A covering set of macrofaults is diagnosable according to definition 3 if and only if it is diagnosable according to definition 9.*

**Proof**

First, given a macrofault $F_i$, let us consider $Sig(D(F_i))$. This set contains no observation from a state in which $F_i$ is absent, and is hence a characteristic signature for $F_i$. Let us map each macrofault $F_i$ to the set $\Sigma_i = Sig(D(F_i)) \setminus \bigcup_{j<i} Sig(D(F_j))$. $\Sigma_i$ is a characteristic signature for $F_i$ since it is a subset of $Sig(D(F_i))$.

Second, let $o \in Sig(D(F_i))$. We have either $o \notin \Sigma_i$, or $o \in \Sigma_j$ with $j < i$, and if $o \in \Sigma_i$ then necessarily $o \notin \Sigma_k$ with $k \neq i$. Hence, the set of all $\Sigma_i$ forms a partition of the set $\bigcup_i Sig(D(F_i))$.

The previous statements are now used to establish the equivalence. The covering set of macrofaults $\{F_0 \dots F_n\}$ is diagnosable according to definition 9 if and only if the set of all $D(F_i)$ covers $\mathcal{SD}$ (see section 4.4), which is equivalent to the set $\bigcup_i Sig(D(F_i))$ covering *OBS*. Consequently, from the statements above, it follows that the set $\Pi = \{\Sigma_0 \dots \Sigma_n\}$ partitions *OBS*, and the set of macrofaults is diagnosable according to definition 3. ■

## 5 Application to repair preconditions

The definition of diagnosability is now applied to sets of states that map to repair preconditions. When a repair precondition is diagnosable, it is possible to decide when to apply the repair and when not. It is a complementary approach to fault diagnosis, since knowing which fault happened and knowing what to do to repair it is not the same information, and both answers are important for monitoring a system.

Alban Grastien, Wolfgang Mayer, and Markus Stumptner, Editors.
Proceedings of the 19th International Workshop on Principles of Diagnosis (DX-08),
September 22–24, 2008, Blue Mountains, NSW, Australia.

Knowing which fault happened but being unable to decide which repair is suited is odd. On the other hand, knowing how to repair a faulty system without knowing the details of the faults is a problem for low cost maintenance or feedback to the system designers. Hence, diagnosability analysis of repair preconditions is a complement to fault diagnosability analysis.

A repair is an action or a process that puts a system back to a normal state from a faulty abnormal state. Repairs can be plans driven by goals [Friedrich *et al.*, 2005], reconfigurations [ten Teije *et al.*, 2004], or other actions. In most approaches, repairs have preconditions, which generally define a set of states. In the case of repair plans, the plan may contain actions that bring additional information about the system state, thus refining the diagnosis. Plans may also contain conditional branchings, especially in order to react to additional diangosis information.

A repair may not be executed in every state of the system for various reasons. An action or plan that repairs a system from a given state may damage it even more in some other states. For example changing a wheel is not possible if the vehicle is not at full stop. Also, it is considered in this paper that repairs being the system back in a normal state, partial repairs are not considered. For example, changing one wheel repairs a vehicle with one flat tire, but it does not repair a vehicle with two flat tires.

In most cases, non faulty states do not belong to repair preconditions, since it is not useful to repair a normal system. However, when there is an ambiguity about the presence fo a fault, some supervision policies consider that it is better to repair a normal system is better than let the system run with its fault. Consequently, normal states may belong to fault preconditions.

**Definition 10 (Repair precondition)** *A repair precondition is a set of states, in which the repair can be applied, and in which the application of the repair brings the system to a normal state.*

This definition implies that if two repair preconditions are verified at the same time, only one repair needs to be applied.

No assumption is made in this paper about the relation between fault modes and repair preconditions. A repair may be applicable in only some of the states of a fault mode, while each fault mode may be repaired differently according to the current system state.

Each repair precondition is described by a logic proposition $rp_i$. The proposition $rp_i$ generally constrains mode variables as well as variables defining the operational state of the system. The set $\mathcal{RP}_i \subseteq \mathcal{SD}$ contains all the system states fulfilling $rp_i$. The set $\overline{\mathcal{RP}_i}$ is the complement of $\mathcal{RP}_i$ in $\mathcal{SD}$, it is the set of system states for which the $i$-th repair is not suited.

## 6 Example

The concepts and definitions described in the previous sections are illustrated by a simple example. It is shown that definitions 5 and 9 allow us to analyse diagnosability at different levels (faults, macrofaults, or repair preconditions) and that the returned information may be different and complementary.

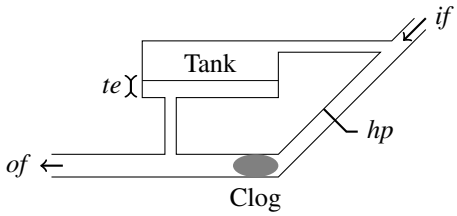



Figure 5: A pipe and a tank

**System** The system consists in a fluid pipe with variable input flow, which is supposed to provide a constant output flow. A tank is used to compensate flow variations. This tank is filled when the input flow is higher that the expected output, and provides water when the input flow is too low.

**Faults** Two faults are considered. First, the pipe may be clogged, which reduces greatly the flow capacity of the pipe. Second, the tank is supposed to be always able to deliver water, however in exceptional conditions, the tank may occur to be empty. When this occurs, the input flow is directed in priority to the tank. If the input flow is sufficiently high, it can supply both the empty tank and the output.

**Sensors** A pressure sensor is placed in the pipe, in order to detect abnormally high pressures. This happens when the pipe is clogged, and there is input flow.

**Model** The model of this system contains five variables :

- *if* describes the input flow and has 3 values : *none*, *low*, and *high*.
- *of* is Boolean and equals 1 when there is an output flow.
- *hp* is Boolean and equals 1 when the pressure inside the pipe is abnormally high.
- *pc* is Boolean and equals 1 when the pipe is clogged.
- *te* is Boolean and equals 1 when the tank is empty.

The behaviour of the system is described by the following constraints:

$$of = 1 \Leftrightarrow \big(te = 0 \vee (if = \text{high} \wedge pc = 0)\big)$$
$$hp = 1 \Leftrightarrow (if \neq \text{none} \wedge pc = 1)$$

**Observables** The variables *if* , *of* and *hp* are observable.

**Repairs** The following repairs are available:

1. It is possible to unclog the pipe thanks to a chemical action ($rp1$). This repair can be applied when the pipe is clogged. For safety reasons, it must not be applied when the pipe is not clogged. If the tank is empty, this repair is not sufficient to bring back the system in a normal state.

$$rp_1 : (pc = 1 \wedge te = 0)$$

Alban Grastien, Wolfgang Mayer, and Markus Stumptner, Editors.
Proceedings of the 19$^{\text{th}}$ International Workshop on Principles of Diagnosis (DX-08),
September 22–24, 2008, Blue Mountains, NSW, Australia.

2. It is also possible to unclog the pipe mechanically ($rp2$). The action consists in sending someone on site and clean the pipe. This repair can only be applied when the pipe is empty (no input flow), but is not sufficient if the tank is empty, since it will not bring the system to a normal state. This repair can if necessary be applied in the normal mode : once the cleaner is on site, if the pipe is not clogged, then the cleaner will do nothing.

$$rp_2 : (te = 0 \wedge if = \text{none})$$

3. Finally, if the tank is empty, it is possible to redirect the whole flow through the tank ($rp3$). This permits to mechanically unclog the pipe if needed. However, the manipulations involved in this repair require that there is no flow in the pipe.

$$rp_3 : \big(te = 1 \wedge (if = \text{none} \vee pc = 1)\big)$$

The system has 12 different states, represented in Figure 6 as well as the diagnosable blocks and their corresponding observations. The application of definitions 5 and 9 to the fault modes, macrofaults and repair preconditions are now illustrated on this system.

### 6.1 Fault mode diagnosability analysis

The system has 4 fault modes, named *normal*, *pipe clogged*, *tank empty* and *pipe & tank* that define 4 sets of states whose diagnosability is analyzed. The analysis details are described in Table 1.

According to definition 5, none of these fault modes is diagnosable. Moreover, fault modes are by definition disjoint sets, and the notion of preemptability is not relevant when dealing with disjoint sets of states, since disjoint sets cannot preempt one another. Consequently, no fault mode is diagnosable according to definition 9 either.

### 6.2 Macrofault diagnosability analysis

Let us consider for example the set of macrofaults defined by $\{F_1, F_2, F_3\}$ with $F_1 = \{$*normal*, *tank empty*$\}$ and $F_2 = \{$*pipe clogged*$\}$ and $F_3 = \{$*tank empty*, *pipe & tank*$\}$. The diagnosability analysis is given in Table 2.

None of these macrofaults is diagnosable with respect to definition 5. Moreover, only $F_3$ is preemptable, with $UD(F_3) \subset D(F_1)$, which is not enough to make the set of macrofaults $\{F_1, F_2, F_3\}$ diagnosable according to definition 9.

### 6.3 Repair precondition diagnosability analysis

The sets of states corresponding to the repair preconditions are represented in figure 6. Diagnosability analysis provides the results indicated in Table 3.

The undiagnosable spaces of repair preconditions $\mathcal{RP}_2$ and $\mathcal{RP}_3$ are empty, which means these sets of states are unions of diagnosable blocks. They are diagnosable, according to definition 5. Moreover, $\mathcal{RP}_1$ is not diagnosable, but $UD(\mathcal{RP}_1) \subset D(\mathcal{RP}_2)$, it is preemptable. The set of repair preconditions $\{\mathcal{RP}_1, \mathcal{RP}_2, \mathcal{RP}_3\}$ is diagnosable with respect to definition 9.

## 7 Conclusion

This paper provides a new, general definition of diagnosability, that applies to any set of states and by extension to any state dependent property. Given a property that depends on the system state, it is possible to assess whether the observations are sufficient to deduce that the property holds or not. Such properties can be the presence or absence of faults, which falls back into existing diagnosability approaches. They can also be repair preconditions, which we expect to fall back into existing self-healability approaches [Cordier *et al.*, 2007]. Analysing repair preconditions diagnosability is showed to bring different information from analysing fault modes or macrofaults diagnosability.

This work covers many other kinds of properties, like for example the ability of the system to provide its function, or a given part of its function, or to respect a given quality of service. Any property that can be mapped to a set of states can be checked with this approach.

## References

[Bayoudh *et al.*, 2006] M. Bayoudh, L. Travé-Massuyès, and X. Olive. Hybrid systems diagnosability by abstracting faulty continuous dynamics. In *Proceedings of DX'06*, 2006.

[Console *et al.*, 2000] L. Console, C. Picardi, and M. Ribaudo. Diagnosis and diagnosibility analysis using pepa. In *Proceedings of the European Conference on Artificial Intelligence (ECAI'2000)*, pages 131–135, Germany, 2000.

[Cordier *et al.*, 2006] Marie-Odile Cordier, Louise Travé-Massuyès, and Xavier Pucel. Comparing diagnosability in continuous and discrete-event systems. In *Proceedings of the 17th International Workshop on Principles of Diagnosis, DX'06*, pages 55–60, 2006.

[Cordier *et al.*, 2007] M.O. Cordier, Y. Pencolé, L. Travé-Massuyès, and T. Vidal. Self-healability = diagnosability + repairability. In *Proceedings of the 18th International Workshop on Principles of Diagnosis DX'07, Nashville, TN, USA*, 2007.

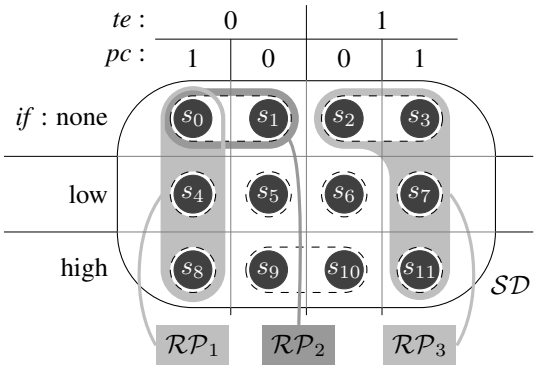
[Friedrich *et al.*, 2005] Gerhard Friedrich, Georg Gottlob, and Wolfgang Nejdl. Formalizing the repair process — extended report. *Annals of Mathematics and Artificial Intelligence*, 11(1-4):187–201, april 2005.

[Hamscher *et al.*, 1992] W. Hamscher, L. Console, and J. de Kleer. *Readings in model-based diagnosis*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 1992.

[Sampath *et al.*, 1995] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis. Diagnosability of discrete event system. *IEEE Transactions on Automatic Control*, 40(9):1555–1575, 1995.

[Struss and Dressler, 2003] P. Struss and O. Dressler. A toolbox integrating model-based diagnosability analysis and automated generation of diagnostics. In *Proceedings of DX'03*, 2003.

[ten Teije *et al.*, 2004] A. ten Teije, F. van Harmelen, and B. Wielinga. Configuration of web services as parametric




| States | Observation | | |
|---|---|---|---|
| | *if* | *hp* | *of* |
| $s_0, s_1$ | none | 0 | 1 |
| $s_2, s_3$ | none | 0 | 0 |
| $s_4$ | low | 1 | 1 |
| $s_5$ | low | 0 | 1 |
| $s_6$ | low | 0 | 0 |
| $s_7$ | low | 1 | 0 |
| $s_8$ | high | 1 | 1 |
| $s_9, s_{10}$ | none | 0 | 1 |
| $s_{11}$ | high | 1 | 0 |

Figure 6: States, diagnosable blocks and repair plans of the system.

| Fault mode | States | Intersected diagnosable blocks | *UD* |
|---|---|---|---|
| $\mathcal{SD}_{normal}$ | $\{s_1, s_5, s_9\}$ | $\{s_0, s_1\}$ and $\{s_9, s_{10}\}$ | $\{s_1, s_9\}$ |
| $\mathcal{SD}_{pipe\ clogged}$ | $\{s_0, s_4, s_8\}$ | $\{s_0, s_1\}$ | $\{s_0\}$ |
| $\mathcal{SD}_{tank\ empty}$ | $\{s_2, s_6, s_{10}\}$ | $\{s_9, s_{10}\}$ and $\{s_2, s_3\}$ | $\{s_2, s_{10}\}$ |
| $\mathcal{SD}_{pipe\ \&\ tank}$ | $\{s_3, s_7, s_{11}\}$ | $\{s_2, s_3\}$ | $\{s_3\}$ |

Table 1: Fault modes diagnosability results.

| Macrofault | States | Intersected diagnosable blocks | *UD* |
|---|---|---|---|
| $F_1$ | $\{s_1, s_2, s_5, s_6, s_9, s_{10}\}$ | $\{s_0, s_1\}$ and $\{s_2, s_3\}$ | $\{s_1, s_2\}$ |
| $F_2$ | $\{s_0, s_4, s_8\}$ | $\{s_0, s_1\}$ | $\{s_0\}$ |
| $F_3$ | $\{s_2, s_3, s_6, s_7, s_{10}, s_{11}\}$ | $\{s_9, s_{10}\}$ | $\{s_{10}\}$ |

Table 2: Macrofaults diagnosability results.

| Repair precondition | States | Intersected diagnosable blocks | *UD* |
|---|---|---|---|
| $\mathcal{RP}_1$ | $\{s_0, s_4, s_8\}$ | $\{s_0, s_1\}$ | $\{s_0\}$ |
| $\mathcal{RP}_2$ | $\{s_0, s_1\}$ | none | $\emptyset$ |
| $\mathcal{RP}_3$ | $\{s_2, s_3, s_7, s_{11}\}$ | none | $\emptyset$ |

Table 3: Repair preconditions diagnosability results.

In each table, the column "Intersected diagnosable blocks" lists the diagnosable blocks that intersect but are not subset of the corresponding set of states.

Alban Grastien, Wolfgang Mayer, and Markus Stumptner, Editors.
Proceedings of the 19th International Workshop on Principles of Diagnosis (DX-08),
September 22–24, 2008, Blue Mountains, NSW, Australia.

design. In E. Motta, N. Shadbolt, A. Stutt, and N. Gibbins, editors, *Proceedings of the 14th International Conference, (EKAW-2004)*, number 3257 in Lecture Notes in Artificial Intelligence, pages 321–336, Whittleburry Hall, UK, October 2004. Springer Verlag. ISBN 3-540-23340-7.

[Travé-Massuyès *et al.*, 2001] L. Travé-Massuyès, T. Escobet, and R. Milne. Model-based diagnosability and sensor placement application to a frame 6 gas turbine subsystem. In *Proceedings of the Seventeenth International Joint Conference on Artificial Intelligence, IJCAI'01*, volume 1, pages 551–556, 2001.

[Travé-Massuyès *et al.*, 2006] L. Travé-Massuyès, T. Escobet, and X. Olive. Diagnosability analysis based on component supported analytical redundancy relations. *IEEE Transactions on Systems, Man and Cybernetics, Part A : Systems and Humans*, 36(6), 2006.