# DETERMINING A COMPONENT'S FAULT STATUS AND THE STATUS' READINESS

**Jonas Biteus*, Mattias Nyberg†, Erik Frisk*, and Jan Åslund***

* *Division of Vehicular Systems, Dept. of Electrical Engineering*
*Linköpings universitet, SE-581 83 Linköping, Sweden*
*E-mail:* {biteus,frisk,jaasl}@isy.liu.se
† *Software and Diagnostics, Power-train Division*
*Scania AB, SE-151 87 Södertälje, Sweden*
*E-mail:* mattias.nyberg@scania.com

Abstract: A diagnosis points at a set of components whose abnormal behavior could explain why a system does not function as intended, and a set of diagnoses points at different such sets of components. It would be an advantage for repair technicians if it, as a complement to the diagnoses, was possible to exactly state which components that certainly are faulty, which that are only suspected to be faulty, and which that are normal, i.e. to state the components' fault statuses. There would also be an advantage if the technicians could get an indication when a component's fault status cannot be changed by evaluating additional diagnostic tests, and the fault status is in that case said to be ready. The key contributions in the present paper are conditions that can be used to decide a component's fault status and the fault status' readiness. Conditions are stated for both centralized and distributed systems. *Copyright ©2006* IFAC.

Keywords: Fault diagnosis, fault isolation, automotive vehicles, OBD.

## 1. INTRODUCTION

In AI, the dominant methodology for fault isolation has been so called consistency based diagnosis, which has strong relationships with the methods for fault isolation used in FDI [1], [2], [3]. A consistency based diagnosis points at a set of components whose abnormal behavior could explain why a system does not function as intended, and a set of diagnoses points at different such sets of components. It would be an advantage, especially for repair technicians, if it as a complement to the diagnoses was possible to exactly state which components that certainly are faulty, which that are only suspected to be faulty, and which that are normal. This is here denoted a component's *fault status* or in short a component's *status*. In diagnostic systems designed as sets of precomputed diagnostic tests there would also be an advantage if the technicians could get an indication when a component's status cannot be changed by evaluating additional diagnostic tests, and the status is in that case said to be *ready*.

The key contributions of this paper are conditions that can be used to decide a component's status and the status' readiness. The conditions are used to state, for each component, a tuple $\langle c, s, r \rangle$ where $c$ is the component, $s$ is the status, i.e. faulty, suspected, or normal, and $r$ is ready or not-ready.

Our work has been motivated by the diagnostic systems used in automotive vehicles [4]. These systems typically store a *diagnostic trouble code* (DTC) when a component is found to be faulty. In the first generations of diagnostic systems, each diagnostic test checked exactly one component for faulty behavior. The DTCs could therefore be used to state exactly which components that where faulty and which that where normal.

Due to higher demands on diagnosis, such as reduced emission levels [5], the industry has introduced diagnostic tests that check the correct behavior of several components at the same time, denoted *multi-component* or plausibility tests. These multi-component tests are for example based on *analytical redundancy relations* (ARR) [1]. These more general tests come into conflict with the diagnostic framework based on single component tests that has previously been used in automotive vehicles. A question that has to be answered is: When and how should a DTC be set when multi-component tests are used? We propose that a DTC should be set for a component when the component's status is faulty or suspected, and that the tuple $\langle c, s, r \rangle$, described above, should be included in the DTC.

If a component's status is not ready then it would be an advantage to know which tests whose evaluation would lead the status to ready. This is especially true when not all tests can be evaluated directly due to for example limited processing power. A contribution of this paper is conditions that can be used to calculate which tests that are meaningful to evaluate.

A trend in most automotive vehicles is the inclusion of multiple *electronic control units* (ECUs), generally denoted *agents* [6], that communicate over a network [7], [8]. There might in these distributed systems exist diagnostic tests in one agent that checks components that belong to another agent. This is for example the result when there is exchange of information such as sensor values, actuator values, or calculated values. A contribution of this paper is that a component's status of faulty, suspected, and normal and the status' readiness is extended to distributed systems.

## 2. CONSISTENCY BASED DIAGNOSIS

A system consists of a set of components $\mathcal{C}$, which should be supervised by the diagnostic system implemented in a set of agents. A component is something that can be diagnosed. This not only includes components directly connected to the agents, such as sensors and actuators, but it also includes components shared between the agents, e.g. cables and pipes.

To reduce the complexity of the diagnostic system, it is sometimes preferable to only consider the abnormal $AB$ and the not abnormal $\neg AB$ mode, where the $AB$ mode does not have a model. This means that the minimal diagnosis hypothesis is fulfilled [9], and therefore the notation in for example GDE will be employed [10]. It will here be studied how the components status and the status' readiness will be defined and their properties analyzed under the minimal diagnosis hypothesis.

A *diagnosis* is a set of components $D \subseteq \mathcal{C}$, such that the components' abnormal behaviors, the remaining components' normal behaviors, the system description, and the observations are consistent. Since the minimal diagnosis hypothesis is fulfilled and $D$ is a diagnosis, all supersets of $D$ are also diagnoses. Further, a diagnosis $D'$ is a minimal diagnosis if there is no proper subset $D \subset D'$ where $D$ is a diagnosis [9].

An evaluation of a diagnostic test results in a conflict if some components, checked by the test, have been found to behave abnormal. A *conflict* is a set of components $\pi \subseteq \mathcal{C}$, such that the components' normal behaviors, the system description, and the observations are inconsistent. A set $D \subseteq \mathcal{C}$ is a diagnosis if and only if it has a nonempty intersection with every conflict in a set of conflicts. A consequence of this is that the set of minimal diagnoses is exactly determined by the set of minimal conflicts [9].

A single-component diagnostic test generates a conflict $\pi = \{c\}$ if it detects that component $c$ behaves abnormal. A more general multi-component test will generate a conflict $\pi \subseteq \mathcal{C}$ if it detects that any component in $\pi$ behaves abnormal. If no abnormal behavior is detected then a test does not generate any conflict.

## 3. MULTI-COMPONENT TESTS, COMPONENT STATUS, AND STATUS' READINESS

This section will focus on centralized diagnostic systems, while Section 5 will focus on distributed systems, described in Section 4. Here, the status of a component will first be explored in Section 3.1, and this will then be used when readiness is discussed in Section 3.2.

### 3.1 *Component Status: Faulty, Suspected, and Normal*

The following definitions states when a component's status is faulty, suspected, and when it is normal.

*Definition 1.* Let $\mathcal{D}$ be the set of minimal diagnoses. The status of component $c$ is *faulty* if and only if

$$\forall D \in \mathcal{D} : c \in D.$$

*Definition 2.* Let $\mathcal{D}$ be the set of minimal diagnoses. The status of component $c$ is *suspected* if and only if

$$\exists D_1, D_2 \in \mathcal{D} : (c \in D_1 \wedge c \notin D_2).$$

*Definition 3.* Let $\mathcal{D}$ be the set of minimal diagnoses. The status of component $c$ is *normal* if and only if

$$\forall D \in \mathcal{D} : c \notin D.$$

The possible status for a component is exhaustive, i.e. a component is either faulty, normal, or suspected. From the definitions follow that when only single-component diagnostic tests are used, it is only possible for a component's status to be faulty or normal. However, when general diagnostic tests are introduced then a component's status might also be suspected.

*Example 1.* Consider a system consisting of the set of components $A$, $B$, $C$, $D$, and $E$. Let there exist diagnostic tests such that the set of possible conflicts is $\{A\}$, $\{B, C\}$, $\{C\}$, and $\{B, D\}$. If the present set of conflicts is $\{A\}$, and $\{B, C\}$ then the corresponding set of minimal diagnoses for these conflicts is the set

$$\mathcal{D} = \{\{A, B\}, \{A, C\}\}.$$

The status of component $A$ is faulty, and the status of $B$ and $C$ are suspected. The rest of the components' statuses, i.e. $D$ and $E$, are normal. ◇

3.1.1. *Component Status Related to Conflicts* The status of faulty, suspected, and normal where defined in Section 3.1 with respect to the set of minimal diagnoses. This requires that the set of minimal diagnoses has been computed from the set of conflicts. To reduce the need to compute the minimal diagnoses, there would be an advantage if it instead was possible to decide the status of a component based on the set of conflicts themselves. The following three propositions give such relations between the conflicts and the status of faulty, suspected, and normal.

*Proposition 1.* Let $\mathcal{D}$ be a set of minimal diagnoses determined by the set of minimal conflicts $\Pi$. The status of component $c$ is *faulty* if and only if

$$\exists \pi \in \Pi : \pi = \{c\}.$$

*Proposition 2.* Let $\mathcal{D}$ be a set of minimal diagnoses determined by the set of minimal conflicts $\Pi$. The status of component $c$ is *suspected* if and only if

$$(\nexists \pi \in \Pi : \pi = \{c\}) \ \wedge \ (\exists \pi \in \Pi : c \in \pi).$$

*Proposition 3.* Let $\mathcal{D}$ be a set of minimal diagnoses determined by the set of minimal conflicts $\Pi$. The status of component $c$ is *normal* if and only if

$$\forall \pi \in \Pi : c \notin \pi.$$

The proofs follow directly from the definitions in Section 3.1.

In summary: Definition 1, 2, and 3, alternatively the conditions in Proposition 1, 2, and 3 can be used to decide if a component's status is faulty, suspected, or normal.

### 3.2 *The Status' Readiness*

If only single-component diagnostic tests, i.e. conflicts with only one component, are used, then a component's status is ready if the diagnostic test that checks the component has been evaluated. In the general case where multi-component tests are used, there does not exist such a simple relationship between when a test is finished and when the status is ready.

When discussing readiness, the set $\mathcal{D}$ is the set of minimal diagnoses consistent with the present minimal conflicts $\Pi$. The set of non-finished tests could in the future give the set of conflicts $\Pi^f$. Let $\bar{\Pi} \subseteq \Pi^f$ be a set of conflicts, and let the set $\bar{\mathcal{D}}$ be the set of possibly future minimal diagnoses consistent with the set of conflicts $\Pi \cup \bar{\Pi}$.

*Definition 4.* The status of component $c$ is *ready* if and only if the status of $c$ is faulty, normal, or suspected, considering the present diagnoses $\mathcal{D}$, and for all future diagnoses $\bar{\mathcal{D}}$ the status of $c$ is still faulty, normal, or suspected, respectively.

The readiness of a component is defined with respect to the diagnoses, and in a similar manner as in Section 3.1.1, it is possible to instead calculate the readiness from the conflicts. For faulty, the following simple relation holds.

*Proposition 4.* Let the status of component $c$ be faulty, then the status of $c$ is *ready*.

*Proof.* There exists a conflict $\pi = \{c\}$ since the status of $c$ is faulty, Proposition 1, and since $\pi$ is always a minimal conflict, the status is always faulty, and the status of $c$ is therefore ready. $\square$

The proposition shows that the definition of readiness follows the intuitive meaning of faulty, i.e. if a status is faulty, then it cannot in the future be not faulty.

There are not such a direct relationship between status for normal and suspected and readiness, as shown by the following two propositions.

*Proposition 5.* Let $\Pi$ be the set of present minimal conflicts, let $\Pi^f$ be the set of all possible future conflicts, and let $\bar{\Pi} \subseteq \Pi^f$. Let the status of component $c$ be suspected, then the status of $c$ is *ready* if and only if

$$\text{(1a)} \qquad (\nexists \pi^f \in \Pi^f : \pi^f = \{c\}) \wedge$$

$$\text{(1b)} \qquad (\nexists \bar{\Pi}, \bar{\pi} \in \bar{\Pi}, (\forall \pi \in \Pi : c \in \pi) : (c \notin \bar{\pi} \wedge \bar{\pi} \subset \pi)).$$

*Proof.* The status of $c$ is ready if and only if its status is neither normal nor faulty for all $\bar{\Pi}$. The status is not faulty exactly when (1a), Proposition 1. From Proposition 3 and considering minimal conflicts it follows that the status is not normal exactly when (1b). Since the status cannot be normal and not faulty for all future diagnoses it is suspected, and the status is ready. $\square$

Even though it might at first seem difficult, due to the inclusion of the existential quantification, to use the proposition above, it is in fact straightforward to construct an algorithm that test an equation such as (2). More about this in Section 3.4.

*Example 2.* Consider Example 1 where the set of conflicts is $\{\{A\}, \{B, C\}\}$, and the set of possible future conflicts is $\{\{C\}, \{B, D\}\}$. the status of components $B$ and $C$ are suspected. For the future conflict $\{C\}$ and for the present conflict $\{B, C\}$

$$B \notin \{C\} \wedge \{C\} \subset \{B, C\} \to \mathsf{True}$$

and it follows from Proposition 5 that the status of $B$ is not ready. The status of $C$ is also not ready since there exist a future conflict $\pi = \{C\}$. $\diamond$

*Proposition 6.* Let $\Pi$ be a set of present minimal conflicts, and let $\Pi^f$ be the set of all possible future conflicts. Let the status of component $c$ be normal, then the status is *ready* if and only if

$$\text{(2)} \qquad \nexists \pi^f \in \Pi^f, \forall \pi \in \Pi : (c \in \pi^f \wedge \pi \not\subset \pi^f).$$

*Proof.* The status of $c$ is normal for all future diagnoses if and only if $c \notin \pi^f$ for each minimal conflict $\pi^f \in \Pi^f$. The status is therefore normal if and only if $c \notin \pi^f$ or if each $\pi^f$, where $c \in \pi^f$, is non-minimal considering the set $\Pi$, equivalent with (2). The status is therefore always normal and it is therefore ready. $\square$

*Example 3.* Consider once again Example 1. the status of $D$ and $E$ are normal. The status of $D$ is not ready since for the future conflict $\{B, D\}$ and for the present conflicts,

$$D \in \{B, D\} \wedge \{A\} \not\subset \{B, D\} \to \mathsf{True}$$
$$D \in \{B, D\} \wedge \{B, C\} \not\subset \{B, D\} \to \mathsf{True}$$

and the readiness follows from Proposition 6. The status of $E$ on the other hand is ready since there does not exist any future conflict $\pi$ where $E \in \pi$. $\diamond$

In summary: The conditions in Proposition 4, 5, and 6 can be used to decide if a component's status is ready.

### 3.3 *Diagnostic Tests that Results in Ready Status*

One of the objectives for a diagnostic system is to achieve readiness for a component's status and the problem of which diagnostic tests to evaluate to achieve readiness will here be studied locally for one component. A first goal is to find which tests that are meaningful to evaluate, i.e. that can change the status, and which that are not meaningful. Within the set of meaningful tests, it is then interesting to find in which order that these tests should be evaluated such that readiness is reached as fast as possible.

3.3.1. *Meaningful Diagnostic Tests* The propositions in Section 3.1.1 can be used to decide which of the non-finished tests that should be evaluated such that readiness is achieved for a component's status.

*Definition 5* (*Meaningful diagnostic tests*). A set of diagnostic tests is *meaningful* for component $c$ if the addition of their corresponding conflicts to the set of present conflicts would result in a change in the component's status.

From the definition follows that a component's status is ready if and only if no set of meaningful tests exists. Depending on if the status of a component is faulty, normal, or suspected, different sets of tests are meaningful to evaluate.

*Proposition 7.* Let the status of component $c$ be faulty, then there exist no sets of meaningful tests.

*Proof.* Follows directly from Proposition 4. □

*Proposition 8.* Let the status of component $c$ be suspected. The sets of meaningful tests for component $c$ are the sets of tests which corresponds to the sets of conflicts

$$\text{(3a)} \quad \{\{\pi^f\} : \pi^f \in \Pi^f, \pi^f = \{c\}\} \cup$$

$$\text{(3b)} \quad \{\bar{\Pi} : \bar{\Pi} \subseteq \Pi^f, \bar{\pi} \in \bar{\Pi}, (\forall \pi \in \Pi : c \in \pi) : (c \notin \bar{\pi} \wedge \bar{\pi} \subset \pi)\}.$$

*Proof.* Proposition 5 gives both some tests that are meaningful in themselves, and sets of conflicts that only are meaningful if all tests in the set are evaluated. Equation (1a) corresponds to (3a) and (1b) to (3b). □

A conflict in a set in (3a) changes the suspected status to faulty, while a set of conflicts in (3b) changes the suspected status to normal.

*Proposition 9.* Let the status of component $c$ be normal, then the sets of *meaningful* tests are the sets that corresponds to sets of conflicts

$$\text{(4)} \quad \{\{\pi^f\} : \pi^f \in \Pi^f, (\nexists \pi \in \Pi : (c \in \pi^f \wedge \pi \subset \pi^f))\}.$$

*Proof.* Proposition 3 gives (4). □

#### 3.3.2. *Ordering Among Meaningful Tests*

After the collection of sets of meaningful tests has been found, it would be interesting to know in which order the sets of tests should be evaluated such that readiness is achieved as fast as possible. If the diagnostic system is interested in a component $c$ for which it exists a test with a conflict $\pi = \{c\}$, then this test should probably be evaluated first, since this leads to faulty status and status' readiness.

If the status for component $c$ is suspected, then the ordering depends on if it is most important to find that the status is faulty or if it is most important to return the status to normal. If faulty is prioritized, then evaluate those tests that fastest leads to faulty, i.e. tests corresponding to the conflicts in the set (3a). If the normal status is prioritized, then evaluate tests that correspond to the conflicts in (3b).

### 3.4 *Calculation of the Tuples for all Components*

In the introduction it was stated that, for each component, a tuple was wanted that included the status of the component and if the status is ready or not. Using Algorithm 1, which is designed by straightforward application of the propositions, Theorem 1 gives such a tuple for each component. In the algorithm, $X^C$ denotes the complement set of $X$ with respect to the set $\mathcal{C}$, $R$ is the set of components whose status is ready, and $F$, $S$, and $N$, are the sets of components whose statuses are faulty, suspected, and normal, respectively.

*Theorem 1.* Let $\Pi$ be the set of present minimal conflicts and $\Pi^f$ the set of possible future conflicts. Let the result from Algorithm 1 be $T$, then for each tuple $\langle c, s, r\rangle \in T$ the status for component $c$ is $s \in \{\text{faulty}, \text{suspected}, \text{normal}\}$ and the status is $r \in \{\text{ready}, \text{not-ready}\}$.

**Algorithm 1** Fault status and status' readiness

```
Input: The set of present minimal conflicts $\Pi$ and the set of possible future conflicts $\Pi^f$.
Output: The set of tuples $T$.
$F := \{c : \pi = \{c\}, \pi \in \Pi\}$    [Faulty.]
$S := \cup_{\pi \in \Pi} \pi \setminus F$    [Suspected.]
$N := (F \cup S)^C$    [Normal.]
$\bar{S}_1 := \{c : \pi^f \in \Pi^f, \pi^f = \{c\}\}$
$\bar{S}_2 := \{c \in \bar{\pi} \in \bar{\Pi} :$
        $\bar{\Pi} \subseteq \Pi^f, (\forall \pi \in \Pi : c \in \pi), c \notin \bar{\pi}, \bar{\pi} \subset \pi\}$
$\bar{N} := \{c \in \pi^f \in \Pi^f : \forall \pi \in \Pi, c \in \pi^f, \pi \not\subset \pi^f\}$
$R := F \cup (S \setminus \bar{S}_1 \setminus \bar{S}_2) \cup (N \setminus \bar{N})$    [Ready.]
$T = \{\langle c, s, r\rangle : c \in \mathcal{C}, s = \text{faulty if } c \in F, s = \text{suspected if } c \in S, s = \text{normal if } c \in N, r = \text{ready if } c \in R, r = \text{not-ready if } c \in R^C\}$
```

*Proof.* The correctness of $F$, $S$, and $N$ follows from Proposition 1, 2, and 3, respectively. The sets $\bar{S}_1$, $\bar{S}_2$, and $\bar{N}$ corresponds (1a), (1b), and (2), respectively, in Proposition 5 and 6. $R$ is therefore the set of components whose statuses are ready. The output $T$ is therefore correct. □

## 4. DISTRIBUTED SYSTEMS

First, distributed systems will be exemplified and a framework for distributed systems presented, then the status of faulty, normal, and suspected, and the status' readiness, are extended to distributed systems.

### 4.1 *An Example of a Distributed System*

Figure 1 shows a configuration of the distributed system used in the current Scania heavy-duty vehicles. It includes three separate CAN (controller area network) buses, which are connected to the coordinator ECU. Each of the ECUs is further connected to sensors and actuators, and both sensor values and control signals can be shared with the other ECUs over the network. There are between 20 and 30 ECUs in the system, depending on the type of the truck, and between 4 and 110 components are connected to each ECU.

### 4.2 *Framework for Distributed Diagnosis*

A system consists of a set of components $\mathcal{C}$, which should be supervised by the diagnostic systems implemented in a set of agents $\mathcal{A}$. A local diagnosis is determined by the conflicts in a single agent, while a global diagnosis is determined by all agents' conflicts.

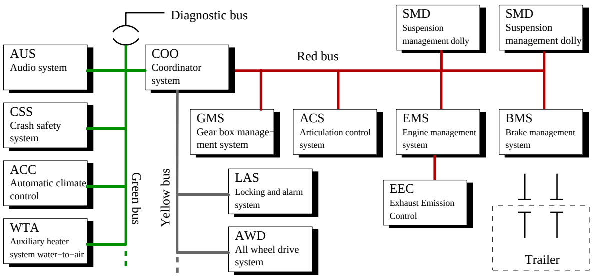
Diagnostic bus
SMD Suspension management dolly
SMD Suspension management dolly
AUS Audio system
COO Coordinator system
Red bus
CSS Crash safety system
GMS Gear box management system
ACS Articulation control system
EMS Engine management system
BMS Brake management system
ACC Automatic climate control
Green bus
Yellow bus
LAS Locking and alarm system
EEC Exhaust Emission Control
WTA Auxiliary heater system water−to−air
AWD All wheel drive system
Trailer

Figure 1. The distributed system in Scania vehicles.

*Example 4.* Figure 2 shows a typical layout of agents and components. The system consists of two agents, a network, and four sensor components, i.e. $S_1$ to $S_4$. The sensors $S_1$ and $S_2$ are physically connected to agent $A_1$, while the sensors $S_3$ and $S_4$ are connected to $A_2$. The diagnostic tests check the consistent behavior of the sensors, which are connected with dashed lines. The diagnostic test in agent $A_1$ collects the value of sensor $S_3$ over the network, and use this to check the consistency of the sensors $S_1$, $S_2$, and $S_3$. ◇

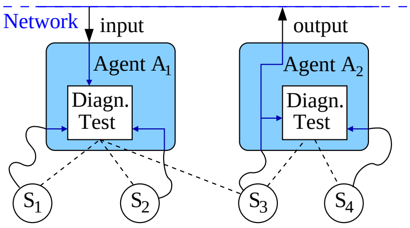

Figure 2. A typical agent, network, component, and diagnostic test layout.

## 5. STATUS AND STATUS' READINESS EXTENDED TO DISTRIBUTED SYSTEMS

A component's status and the status' readiness, which were defined and characterized in Section 3, will here be extended to distributed systems.

### 5.1 *Locally and Globally Fault Status*

Let $\Pi^A$ bet the set of minimal conflicts detected in agent $A \in \mathcal{A}$, and let $\mathbb{D}^A$ be the set of local minimal diagnoses determined by the set of minimal conflicts $\Pi^A$. Further, let $\mathcal{D}$ the set of minimal global diagnoses determined by the set of conflicts $\cup_{A \in \mathcal{A}} \Pi^A$. A component's status can, in a distributed system, be divided into two different levels, the global and the local.

*Definition 6.* The *global status* (GS) of component c is faulty, suspected, or normal if it is faulty, normal, or suspected, respectively, with respect to the global minimal diagnoses $\mathcal{D}$.

*Definition 7.* The *local status* (LS) of component c is faulty, normal, or suspected, for agent $A$ if it is faulty, normal, or suspected, respectively with respect to the local minimal diagnoses $\mathbb{D}^A$.

The GS and the LS of component c is either normal, suspected, or faulty, i.e. exhaustive. The GS has a simple relation to the LS in some agent where the LS is faulty.

*Proposition 10.* The GS of component c is *faulty* if and only if the LS is faulty for some agent.

*Proof.* The GS of component c is faulty if and only if there exist a conflict $\pi = \{c\}$, and such a conflict exists if and only if the LS of c is faulty for some agent, Proposition 1. □

The proposition shows that the definition of globally faulty follows the intuitive meaning of faulty. If the LS of a component is faulty, then its GS must also be faulty. The relation between GS suspected and the local status is not so simple.

*Proposition 11.* The GS of component c is *suspected* if and only if

$$(\nexists A \in \mathcal{A} : (\text{the LS of c is faulty in } A)) \wedge \tag{5a}$$

$$\Big(\exists A \in \mathcal{A} : \big((\text{the LS of c is suspected in } A) \wedge \tag{5b}$$

$$(\exists \pi \in \Pi^A, \forall \tilde{A} \in \mathcal{A}, \forall \tilde{\pi} \in \Pi^{\tilde{A}} : (c \in \pi \wedge \tilde{\pi} \not\subset \pi))\big)\Big). \tag{5c}$$

*Proof.* The GS of component c is suspected if and only if there exist a minimal conflict $\pi$ such that $c \in \pi$ and the LS of c is not faulty for any agent, i.e. (5a). For an agent $e$ where the LS of c is suspected, i.e. (5b), there exists a minimal conflict $\pi$, considering the set of conflicts $\cup_{A \in \mathcal{A}} \Pi^A$, such that $c \in \pi$ exactly when (5c). From this follows that the GS of c is suspected. □

An implication of Proposition 11 is that the GS of c is suspected if the LS is suspected for all agents and only if the LS is suspected for some agent. The relation between GS normal and the LS is shown by the following proposition.

*Proposition 12.* The GS of component c is *normal* if and only if

$$\forall A \in \mathcal{A} : \big((\text{the LS of c is normal in } A) \vee \tag{6a}$$

$$\big((\text{the LS of c is suspected in } A) \wedge \tag{6b}$$

$$(\nexists \pi \in \Pi^A, \forall \tilde{A} \in \mathcal{A} \backslash A, \forall \tilde{\pi} \in \Pi^{\tilde{A}} : (c \in \pi \wedge \tilde{\pi} \not\subset \pi))\big)\big). \tag{6c}$$

*Proof.* The GS of component c is normal if and only if c is not included in any minimal conflict, Proposition 3. The LS is therefore normal, i.e. (6a), or suspected, i.e. (6b), for all agents. In an agent $A$ where the LS is suspected, the conflicts including c will be non-minimal considering the complete set of minimal conflicts exactly when (6c). Therefore c is not included in any minimal conflict in the complete set of minimal conflicts, i.e. the GS of c is normal. □

An implication of Proposition 12 is that the GS of component c is normal if the LS is normal for all agents.

*Example 5.* A system consists of two agents $A_1$ and $A_2$ which have calculated the sets of minimal conflicts $\Pi^{A_1} = \{\{A, B\}\}$ and $\Pi^{A_2} = \{\{A\}, \{C, D\}\}$. The sets of minimal local diagnoses determined by the sets of conflicts are $\mathbb{D}^{A_1} = \{\{A\}, \{B\}\}$ and $\mathbb{D}^{A_1} = \{\{A, C\}, \{A, D\}\}$. The LS of components $A$ and B is suspected in agent $A_1$, while the LS of component $A$ is faulty and the LS of C and D is suspected in $A_2$.

Proposition 10 gives that the GS of $A$ is faulty since there exist a LS where $A$ is faulty. The GS of B is normal since the LS of B is normal in $A_2$, i.e. (6a), and it is both suspected in $A_1$, i.e. (6b), and there exist no conflict $\pi \in \Pi^{A_1}$ such that $\{A\} \not\subset \pi$, i.e. (6c). The GS of C and D is suspected since they are suspected in $A_2$ and the conflict $\{A, B\} \not\subset \{C, D\}$. The set of global diagnoses is $\mathcal{D} = \{\{A, C\}, \{A, D\}\}$, which verifies the statuses. ◇

In summary: The conditions in Propositions 10, 11, and 12 can be used to decide if a components GS is faulty, suspected, or normal.

### 5.2 *Global and Local Readiness*

The definition of readiness in Section 3 is here extended to global and local readiness.

*Definition 8.* The status of component $c$ is *globally ready* if it is ready with respect to the set of present and future global minimal diagnoses $\mathcal{D}$.

*Definition 9.* The status of component $c$ is *locally ready* for agent $A$ if it is ready with respect to the set of present and future local minimal diagnoses $\mathbb{D}^A$.

Since components might be shared between agents, a component might be locally ready even though it is not globally ready, and vice versa. The relations between globally ready and locally ready are shown by the three propositions below.

The strong relationship between the faulty status and status' readiness shown in Proposition 4 also holds for global readiness, as shown by the following proposition.

*Proposition 13.* Let the GS of component $c$ be *faulty*, then it is globally ready.

*Proof.* If the GS of $c$ is faulty, then the LS of $c$ is faulty for some agent and it is therefore locally ready for some agent, Proposition 4. Since it is locally ready, the LS is faulty for all future diagnoses and therefore the GS is also faulty for all future diagnoses, i.e. it is globally ready. □

The relationship between global readiness and the GS is not as simple when the GS is suspected or normal as is shown by the following two propositions.

*Proposition 14.* Let the GS of component $c$ be *suspected*, then it is globally ready if and only if

$$\text{(7a)}\quad \left(\nexists \pi^f \in \Pi^f, \exists A \in \mathcal{A} : (\text{LS of } c \text{ is faulty in } A)\right) \wedge$$

$$\text{(7b)}\quad \Big(\nexists \bar{\Pi} \subseteq \Pi^f : \big(\forall A \in \{A : (\text{LS of } c \text{ is susp. in } A)\},$$
$$\forall \pi \in \Pi^A, \exists \bar{\pi} \in \bar{\Pi} : (c \in \pi \wedge \bar{\pi} \subset \pi)\big)\Big).$$

*Proof.* The GS of component $c$ is suspected and globally ready if and only if the GS is neither faulty nor normal for any future conflicts. It is not faulty exactly when (7a), Proposition 10. The GS is normal exactly when (7b), Proposition 12. Therefore $c$ is globally ready if and only if (7) is fulfilled. □

*Proposition 15.* Let $\Pi^f$ be the set of possible future conflicts. Let the GS of component $c$ be *normal*, then it is globally ready if and only if

$$\text{(8)}\quad \nexists \pi^f \in \Pi^f : \Big(\big(\exists A \in \mathcal{A} : (\text{LS of } c \text{ is faulty})\big) \vee$$
$$\Big(\exists A \in \mathcal{A}, \forall \tilde{A} \in \mathcal{A}, \forall \tilde{\pi} \in \Pi^{\tilde{A}} :$$
$$\big((\text{LS of } c \text{ is suspected in } A) \wedge \tilde{\pi} \not\subset \pi^f\big)\Big)\Big).$$

*Proof.* The GS of component $c$ is normal if and only if it does not exist a conflict such that the GS becomes faulty or suspected. This is equivalent to

$$\nexists \pi^f \in \Pi^f : (\exists A : \text{LS of } c \text{ is faulty for } A),$$

Proposition 10, and that

$$\nexists \pi^f \in \Pi^f : \Big(\big(\nexists A : (\text{LS of } c \text{ is faulty in } A)\big) \wedge$$
$$\Big(\exists A : \Big(\big(\text{LS of } c \text{ is suspected in } A\big) \wedge$$
$$\big(\forall \tilde{A}, \forall \tilde{\pi} : (c \in \pi^f \wedge \tilde{\pi} \not\subset \pi^f)\big)\Big)\Big)\Big),$$

Proposition 11, which is equivalent with (8). Therefore $c$ is globally ready if and only if (8) is fulfilled. □

In summary: The conditions in Propositions 13, 14, and 15 can be used to decide if a components GS is ready.

### 5.3 *Test to Achieve Readiness*

The set of meaningful tests can be calculated by following the same procedure as was done in Section 3.3.

## 6. CONCLUSIONS

Motivated by applications used in automotive vehicles, a component's status has been defined as faulty, suspected, or normal. Also defined is the status' readiness, i.e. when the evaluating of additional diagnostic tests could not change the status. Conditions useful for calculating the set of diagnostic tests that has to be evaluated to reach readiness of a component's status was stated exactly. Necessary and sufficient conditions to determine the status and the status' readiness have been derived. A result of the analysis is that a component's status can be faulty if and only if there exist a diagnostic test that only detects a fault in that specific component. A consequence of this is that the status of a component that only is included in multi-component tests, based on for example ARR's, can never become faulty, only suspected. From the derived conditions, it was straightforward to construct an algorithm that computes the status and the status' readiness for all components. The output of the algorithm is a set of tuples, where a tuple $\langle c, s, r \rangle$ states the status $s$ and the status' readiness $r$ for a component $c$. The results for centralized systems were extended to distributed systems.

## References

[1] G. Biswas, M.O. Cordier, J. Lunze, L. Trave-Massuyes, and M. Staroswiecki. Diagnosis of complex systems: Bridging the methodologies of the FDI and DX communities. *Systems, Man and Cybernetics, Part B,* IEEE *Transactions*, 34(5), Oct 2004.

[2] J. de Kleer and J. Kurien. Fundamentals of model-based diagnosis. In *Proceedings of* IFAC *Safeprocess'03*, Washington, U.S.A., 2003.

[3] M. Nyberg and M. Krysander. Combining AI, FDI, and statistical hypothesis-testing in a framework for diagnosis. In *Proceedings of* IFAC *Safeprocess'03*, Washington, U.S.A., 2003.

[4] SAE. *On-Board Diagnostics for Light and Medium Duty Vehicles Standards Manual*. Society of Automotive Engineers, Warrendale, U.S.A., 2003.

[5] European Union. Emissions of atmospheric pollutants from motor vehicles, 2005.

[6] C. C. Hayes. Agents in a nutshell-a very brief introduction. *Knowledge and Data Engineering, IEEE Transactions on*, 11(1):127–132, 1999.

[7] J. Biteus. Distributed diagnosis and simulation based residual generators. Technical report, Linköpings Universitet, 2005.

[8] D. Hristu-Varsakelis and W. S. Levine. *The Handbook of Networked and Embedded Control Systems*. Springer, 2005.

[9] J. de Kleer, A. K. Mackworth, and R. Reiter. Characterizing diagnoses and systems. *Artificial Intelligence*, 56, 1992.

[10] J. de Kleer and B. Williams. Diagnosing multiple faults. *Artificial Intelligence*, 32, Apr 1987.