Proceedings of the 17th World Congress
The International Federation of Automatic Control
Seoul, Korea, July 6-11, 2008

Sensor Placement for Fault Isolation in Linear Differential-Algebraic Systems

Mattias Krysander [*], **Erik Frisk** [*], **and Jan Åslund** [*]

[*] *Department of Electrical Engineering, Linköping University SE-581 83 Linköping, Sweden. {matkr,frisk,jaasl}@isy.liu.se.*

Abstract: An algorithm is proposed for computing which sensor additions that make a diagnosis requirement specification regarding fault detectability and isolability attainable for a given linear differential-algebraic model. Restrictions on possible sensor locations can be given and if the diagnosis specification is not attainable with any available sensor addition, the algorithm provides the solutions that maximize specification fulfillment. Previous approaches with similar objectives have been based on the model structure only. Since the proposed algorithm utilizes the analytical expressions, it can handle models where structural approaches fail. A Mathematica implementation of the algorithm can be downloaded from `http://www.fs.isy.liu.se/Software/LinSensPlaceTool/`.

Keywords: Fault isolation, diagnosis, sensor placement, linear differential-algebraic equations

1. INTRODUCTION

Systematic methods for fault diagnosis and process supervision are important in many industrial applications. To be able to perform model based supervision, some redundancy is needed and this redundancy can be provided by some sensors together with a model description of the process behavior. Scientific attention has mainly been devoted to design of a diagnosis system given a model of a process equipped with a set of sensors. Not as much attention has been devoted to decide which sensors to include in the process. The topic of this paper is to, based on a linear differential-algebraic model, decide where to put sensors so that a given fault isolation performance specification is attainable.

Examples of related previous works are [1] where sensor location for optimal detection performance is studied, or [5] where an optimization problem related to sensor selection is studied. Another example is [14] where a PCA-based monitoring technique is optimized by suitable sensor selection. These papers have a rather different objective and do not address the fault isolation problem. More closely related are the works [2,11,13] who all have a similar objective but, contrary to this paper, utilizes a structural description of the model instead of the analytical equations.

The basic principles of the algorithm developed in this paper are the same as in [6] which is a structural algorithm. The objective here is the same, but since we now consider analytical models, other theoretical tools have to be applied and basic algorithmic steps are fundamentally different. The motive for this analytical approach is that structural methods might give incorrect answers for some models. The example in Section 5 is taken from [8] where the reasons for shortcomings of structural methods are investigated. The paper [6] includes a discussion on how different structural approaches for sensor placement relate to each other and this comparison is relevant also here.

2. PROBLEM FORMULATION

Before the main objective of the paper is formally presented, a small example is discussed that illustrates the fundamental problems in sensor placement for fault diagnosis. The example is modeled by a fifth order linear system of ordinary differential equations. This example will be used throughout the paper and consists of the following equations:

$$\begin{aligned} e_1: &\quad \dot{x}_1 = -x_1 + x_2 + x_5 \\ e_2: &\quad \dot{x}_2 = -2x_2 + x_3 + x_4 \\ e_3: &\quad \dot{x}_3 = -3x_3 + x_5 + f_1 + f_2 \\ e_4: &\quad \dot{x}_4 = -4x_4 + x_5 + f_3 \\ e_5: &\quad \dot{x}_5 = -5x_5 + u + f_4 \end{aligned}$$

where x_i are the state variables, u a known control signal, and f_i the faults we want to detect and isolate.

Faults are modeled by fault signals that are included in the model equations and $f_i \neq 0$ indicates a fault. From now on f_i will be used to denote both the fault signal and the corresponding fault mode. Let $\mathcal{F}$ denote the set of faults. A detectability performance specification is then a set $\mathcal{F}_{det} \subseteq \mathcal{F}$ specifying the detectability requirement and an isolability requirement is a set $\mathcal{I}$ of ordered pairs $(f_i, f_j) \in \mathcal{F}_{det} \times \mathcal{F}_{det}$, meaning that f_i is isolable from f_j. Note that the isolability specification is specified on the set of *detectable* faults $\mathcal{F}_{det}$. Now, we define *minimal sensor set* which is a minimal set of sensors to add to achieve a specified performance specification.

Definition 1. (Minimal sensor set). Let $\mathcal{P}$ be the set of possible sensor locations, i.e. the set of measurable variables, and let S be a multiset defined on $\mathcal{P}$. Given a detectability and isolability specification, S is a minimal sensor set if the specification is fulfilled when the sensors in S are added, but not fulfilled when any proper subset of S is added.

Note that S is a multiset, which is similar to a set but allows multiple instances of a member. Generalizations of the standard set operations like union and intersection are straightforward. Multisets are used instead of regular sets since it may be necessary to add more than one sensor measuring the same variable.

Returning to the example, a first question is then what are the minimal sensor sets achieving detectability of all faults? Here it is assumed that sensors measure a state-

variable or a function thereof. It can be shown, using conditions for fault detectability in linear systems, see e.g. [9], that $\{x_1\}$, $\{x_2\}$, $\{x_3, x_4\}$ are minimal sensor sets achieving detectability.

A second step is to not only require detectability, but also isolability properties. Here isolability refers to isolability as it is commonly used in FDI and the consistency based diagnosis AI community, see e.g. [3]. For details on how isolability is defined in this paper, see Sections 3 and 4. It can be shown that there are 5 minimal sensor sets that achieve maximal fault isolation: $\{x_1, x_3\}$, $\{x_1, x_4\}$, $\{x_2, x_3\}$, $\{x_2, x_4\}$, and $\{x_3, x_4\}$. Thus, adding sensors measuring all the variables in any of these sets, or a superset of the variables, achieves maximum fault isolability.

Now, it is of course the case that the new sensors may also become faulty. If we want also faults in the new sensors to be isolable from the other faults we may have to add additional sensors. In this case, if maximum fault isolability is desired also for faults in the new sensors, there are 9 minimal sensor sets where one sensor set is two sensors measuring x_1 and one for x_3, i.e. the multiset $S = \{x_1, x_1, x_3\}$ is a minimal sensor set.

The problem formulation of the paper can now be stated as:

> Given a model, possible sensor locations, and a detectability/isolability performance specification, find all minimal sensor sets with respect to the required specification.

The methods developed in sections that now follow aim at addressing this problem for general linear differential-algebraic models.

3. THEORETICAL BACKGROUND

This section will formally introduce the model class used in the paper and state some basic results on fault detectability and fault isolability for linear systems that will be used in the development of the algorithm. The results in this section are primarily based on the presentation in [10] but equivalent results exist for other model descriptions.

3.1 The Model

The class of models considered is written as

$$H(p)x + L(p)z + F(p)f = 0 \tag{1}$$

where $x(t) \in \mathbb{R}^{n_x}$, $z(t) \in \mathbb{R}^{n_z}$, $f(t) \in \mathbb{R}^{n_f}$. The matrices $H(p)$, $L(p)$, and $F(p)$ are polynomial matrices in the differentiation operator p. If discrete time systems are considered, the differentiation operator can be replaced by the time shift operator. The vector x contains all unknown signals, which includes internal system states and unknown inputs. The vector z contains all known signals such as control signals and measured signals, and the vector f contains the fault-signals corresponding to faults that need to be detected. Let the sets $\mathcal{X}$, $\mathcal{Z}$, and $\mathcal{F}$ represent the set of unknown variables, known variables, and fault variables respectively.

The theoretical development in this paper will be done under two mild assumption on the model (1). The first assumption states that if there exists a solution $x(t)$ to the model equation (1), given a fault $f(t)$ and an observation $z(t)$, then $x(t)$ is unique. In polynomial algebra this translates into that matrix $H(s)$ has full column rank. This is not a restrictive assumption since any complete physical model will, given an initial condition, have a unique solution. The second assumption is that for all columns $F_i(s)$ in $F(s)$, it holds that

$$F_i(s) \in \text{Im}\,[H(s)\ \ L(s)] \tag{2}$$

This is a mild assumption stating that for any given fault signal $f(t)$ there exist signals $z(t)$ and $x(t)$ consistent with the model equation (1).

Example 1. As an example, consider a model given by the following descriptor equations:

$$E\dot{w} = Aw + B_u u + B_d d + B_f f \tag{3a}$$
$$y = Cw + D_u u + D_d d + D_f f \tag{3b}$$

where y is the vector of existing outputs, u the inputs, w the unknown state-space variable, d unknown disturbances to be decoupled, and f the faults. Letting $E = I$ in the equations above, an ordinary state-space description is obtained. In general, E can be non-singular and even non-square.

In a sensor placement analysis there is a need to define possible sensor locations. Here the convention is used that possible sensors measure single variables in the set of unknown variables $\mathcal{X}$. For cases where there are possible sensors that measure a linear function of more than one variable, include the equation

$$y_p = C_p w$$

and let y_p be in the set of unknown variables. In matrix form, the model equations become

$$\begin{bmatrix} 0 & -(pE - A) & B_d \\ 0 & C & D_d \\ -I & C_p & 0 \end{bmatrix} \begin{pmatrix} y_p \\ w \\ d \end{pmatrix} + \begin{bmatrix} 0 & B_u \\ -I & D_u \\ 0 & 0 \end{bmatrix} \begin{pmatrix} y \\ u \end{pmatrix} + \begin{bmatrix} B_f \\ D_f \\ 0 \end{bmatrix} f = 0$$

where $\mathcal{X}$ is the set of variables in (y_p, w, d) and possible sensor locations is a subset of these variables. ◇

3.2 Basic Results on Detectability and Isolability

It will be convenient to define the set of observations z that is consistent with different fault modes. For example, the set of observations consistent with the fault-free model is written as

$$\mathcal{O}(NF) = \{z | \exists x : H(p)x + L(p)z = 0\} \tag{4}$$

and the observations consistent with the case of fault f_i

$$\mathcal{O}(f_i) = \{z | \exists x, \exists f_i : H(p)x + L(p)z + F_i(p)f_i = 0\} \tag{5}$$

With this notation, a definition on detectability is immediate.

Definition 2. Fault f_i is detectable in (1) if

$$\mathcal{O}(f_i) \nsubseteq \mathcal{O}(NF) \tag{6}$$

In [10] the following detectability condition, directly related to the model matrices, is given:

Theorem 1. Fault f_i is detectable in (1) if and only if

$$F_i(s) \notin \text{Im}\ H(s)$$

Detection is a special case of isolation, i.e. a fault is detectable if the fault is isolable from the no-fault mode. By noting this similarity the following definition is natural.

Definition 3. Fault f_i is isolable from fault f_j in (1) if

$$\mathcal{O}(f_i) \nsubseteq \mathcal{O}(f_j) \tag{7}$$

Similarly as for detectability, a condition for fault isolability directly related to the model matrices is given by

Theorem 2. Fault f_i is isolable from fault f_j in (1) if and only if

$$F_i(s) \notin \text{Im}\,[H(s)\ \ F_j(s)] \tag{8}$$

Proof. The result follows from Theorem 1 and observing that

$$\mathcal{O}(f_j) = \{z|\exists x, \exists f_j.[H(p)\ F_j(p)] \begin{pmatrix} x \\ f_j \end{pmatrix} + L(p)z = 0\}$$

which is in the form (4) with $H(p)$ replaced by $[H(p)\ F_j(p)]$. □

Note that both detectability and isolability are defined as model properties and not properties of a given set of residual generators. Later in the paper, we will use that fault isolability on the set of detectable single faults is a symmetric relation and this is proved next.

Corollary 1. Let fault f_i and f_j be two detectable faults. Fault f_i is isolable from fault f_j if and only if fault f_j is isolable from fault f_i.

Proof. Assume that $F_i(s) \in \text{Im}[H(s)\ F_j(s)]$, i.e. there exist rationals $x_1(s)$ and $x_2(s)$ such that

$$F_i(s) = H(s)x_1(s) + F_j(s)x_2(s)$$

Since f_i is detectable, $x_2(s) \not\equiv 0$ according to Theorem 1 and

$$F_j(s) = F_i(s)x_2^{-1}(s) - H(s)x_2^{-1}(s)x_1(s)$$

The above proves that $F_i(s) \in \text{Im}[H(s)\ F_j(s)]$ implies that $F_j(s) \in \text{Im}[H(s)\ F_i(s)]$ and by symmetry the converse implication follows analogously. □

4. SENSOR PLACEMENT ANALYSIS

The objective of this section is to give theoretical results and an algorithm to solve the problem posed in Section 2.

4.1 Sensor placement for detectability

A basic building block in the final algorithm will be to find all minimal sensor sets that achieve detectability of faults in a set of equations where the matrix $H(s)$ in (1) has full column rank. A key step in determining which sensors to add is formalized in the following lemma in a constructive and algorithmic fashion.

Lemma 1. Let $\mathcal{X}$ be the set of unknown variables, $f_i \in \mathcal{F}$ a non-detectable fault, and $X(s)$ the unique solution to

$$H(s)X(s) = F_i(s) \tag{9}$$

Then fault f_i becomes detectable if and only if any unknown in the set $\{x_j \in \mathcal{X}|X_j(s) \neq 0\}$ is measured.

Proof. It is straightforward to show that extended system, with the sensor equation $y_{\text{new}} = Cx$ added, also fulfills condition (2). The set of possible sensors locations are the set of unknowns $\mathcal{X}$ and C is therefore a selection matrix. According to Theorem 1, fault f_i becomes detectable if and only if

$$\begin{bmatrix} F_i(s) \\ 0 \end{bmatrix} \notin \text{Im} \begin{bmatrix} H(s) \\ C \end{bmatrix} \tag{10}$$

Hence, f_i becomes detectable if and only if there is no solution $X(s)$ to the equations

$$\begin{aligned} H(s)X(s) &= F_i(s) \\ CX(s) &= 0 \end{aligned}$$

If $X(s)$ the unique solution of (9), then $CX(s) \neq 0$ if and only if any unknown in the set $\{x_j \in \mathcal{X}|X_j(s) \neq 0\}$ is measured. This proves the Lemma. □

The result above did not take into consideration that one may have a restriction on possible sensor locations. Thus, based on the result, let $\mathcal{P} \subseteq \mathcal{X}$ be a set of possible sensor locations and introduce the detectability set

$$D(f_i) = \{x_j \in \mathcal{P}|X_j(s) \neq 0 \wedge H(s)X(s) = F_i(s)\} \tag{11}$$

For a fault f_i that is not detectable, the set $D(f_i)$ is the set of variables such that detectability is achieved if and only if *any* variable in the set is measured. If $\mathcal{P}$ is a proper subset of $\mathcal{X}$ then $D(f_i)$ might be empty for a non-detectable fault which means that it is not possible to achieve detectability of the fault by adding any sensors in $\mathcal{P}$. For a detectable fault, there is no solution to $H(s)X(s) = F_i(s)$ and $D(f_i) = \emptyset$.

Lemma 1 characterizes which sensors to add to achieve detectability of a specific fault in case of $\mathcal{P} = \mathcal{X}$. The following theorem summarizes which sensors to add to achieve maximum fault detectability when a restriction $\mathcal{P}$ is included.

Theorem 3. Let $\mathcal{F}$ be the set of faults in the model M, $\mathcal{P} \subseteq \mathcal{X}$ the set of possible sensor locations, and M_S the equations corresponding to adding a set of sensors S. Then maximum detectability of faults $\mathcal{F}$ in $M \cup M_S$ is obtained if and only if S has a non-empty intersection with $D(f)$ for all $f \in \mathcal{F}$ with $D(f) \neq \emptyset$.

Proof. Faults f with $D(f) = \emptyset$ can not be made detectable and maximal detectability is achieved if all faults with non-empty detectability set are made detectable by adding sensors S. It follows from Lemma 1 that this is achieved if and only if $S \cap D(f) \neq \emptyset$ for all non-empty detectability sets $D(f)$. □

The above result can be summarized in an algorithm that given a model M, faults F, and a set of possible sensor locations P, computes the family of detectability sets $\mathcal{D}$.

1 **function** $\mathcal{D}$ = `Detectability`(M,F,P)
2 $\mathcal{D} = \{D(f_i)|f_i \in F \wedge D(f_i) \neq \emptyset\}$;

Our objective was not to compute the set of detectability sets $\mathcal{D}$, but rather minimal sensor sets. A hitting set for a family of sets is a set that has non-empty intersection with each set in the family. Thus, a minimal hitting set algorithm [12,4] applied to the family of sets $\mathcal{D}$ can be used to find all minimal sensor sets.

Example 2. Consider again the example from Section 2. The example model is, without any additional sensors, an exactly determined model with 5 equations and 5 unknown signals where no fault is detectable. Utilizing the results in Lemma 1 and Theorem 3, solving the equations $H(s)X^i(s) = F_i(s)$ for $X^i(s)$ give solutions with the following structure

$$\begin{bmatrix} X^1(s)\ X^2(s)\ X^3(s)\ X^4(s) \end{bmatrix} = \begin{bmatrix} \star & \star & \star & \star \\ \star & \star & \star & \star \\ \star & \star & 0 & \star \\ 0 & 0 & \star & \star \\ 0 & 0 & 0 & \star \end{bmatrix}$$

where a $\star$ indicates a non-zero element. Since, in this example, $\mathcal{P} = \mathcal{X}$ it holds according to equation (11) that the detectability sets are

$$\begin{aligned} D(f_1) &= D(f_2) = \{x_1, x_2, x_3\} \\ D(f_3) &= \{x_1, x_2, x_4\} \\ D(f_4) &= \{x_1, x_2, x_3, x_4, x_5\} \end{aligned}$$

To obtain the minimal sensor sets that achieve detectability of all faults, a minimal hitting set algorithm is applied to the detectability sets which result in the family of sets

$$\{x_1\}, \{x_2\}, \{x_3, x_4\}$$

which is consistent with the description in Section 2. ◇

The critical step in the computation of the detectability sets is to solve the equation $H(s)X(s) = F_i(s)$ and check for zero entries. If a computer algebraic tool like Maple or Mathematica is used, this is easy but if a numerical tool is used to solve the equation, care has to be taken to avoid problems due to limited precision. The step can be directly reformulated as a null-space computation. For descriptor and state-space models, i.e. at most first order derivatives in the model, the computations can be found to be numerically sound. Detailed discussions about underlying algorithms can be found in e.g. [7].

4.2 Sensor placement for isolability of detectable faults

This section describes the basic ideas of how to find the minimal sensor sets such that maximum single fault isolability is obtained under the assumption that all faults are detectable. In the next section this assumption will be removed.

The problem of achieving maximum isolability of the set of single faults $\mathcal{F}$ can be divided into $|\mathcal{F}|$ sub-problems, one for each fault, as follows. For each fault $f_j \in \mathcal{F}$, find all measurements that make the maximum possible number of faults isolable from f_j. The solution to the isolability problem will then be obtained by combining the results from all sub-problems. The following example will illustrate the main principle.

Example 3. In Section 4.1 it was shown that $\{x_1\}$ is a minimal sensor set that achieves detectability of all faults in the example from Section 2. Thus, by adding the equation

$$e_6: \; y_1 = x_1$$

to the model, all faults become detectable. However, with only this sensor, none of the faults are isolable from each other. As stated above, the sensor placement analysis can be divided into $|\mathcal{F}|$ sub-problems and now the procedure will be illustrated for the first sub-problem; to find sensors that achieve maximum fault isolability from fault f_1. Based on Theorem 2, this is done by achieving detectability of the maximum number of faults when matrix $H(s)$ is replaced by $[H(s) \;\; F_1(s)]$. Thus, for the first sub-problem we have

$$H(s) = \begin{bmatrix} s+1 & -1 & 0 & 0 & -1 & 0 \\ 0 & s+2 & -1 & -1 & 0 & 0 \\ 0 & 0 & s+3 & 0 & -1 & -1 \\ 0 & 0 & 0 & s+4 & -1 & 0 \\ 0 & 0 & 0 & 0 & s+5 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \qquad (12)$$

For the remaining faults, the detectability sets are

$$D(f_2) = \emptyset, \; D(f_3) = \{x_3, x_4\}, \; D(f_4) = \{x_2, x_3, x_4, x_5\}$$

The detectability set for f_2 is empty because no addition of sensors will make f_2 isolable from f_1 which is due to that both faults influence the model in the same way. This also implies that the second sub-problem, i.e. finding sensors that achieve maximum fault isolability from fault f_2, gives identical detectability sets for f_3 and f_4. Note that, due to the symmetry result in Corollary 1, there is no need to compute the detectability sets for faults covered in previously handled sub-problems.

Thus, in the third sub-problem where f_3 is considered to be an unknown signal, only the detectability set for f_4 is needed

$$D(f_4) = \{x_2, x_3, x_4, x_5\}$$

Also due to Corollary 1, there is no need to iterate the procedure for the last fault f_4 and we are now finished.

The minimal hitting sets for the family of all non-empty detectability sets obtained in all sub-problem are $\{x_3\}$ and $\{x_4\}$ and since we started the example by adding a sensor measuring x_1 to make all faults detectable, two minimal sensor sets that gives maximum isolability are $\{x_1, x_3\}$ and $\{x_1, x_4\}$.

Since, as shown in Section 4.1, measuring $\{x_1\}$ was not the only possibility to achieve detectability we have to iterate the above procedure also for $\{x_2\}$ and $\{x_3, x_4\}$ to ensure that all minimal sensor sets are found and these sets where given in Section 2. ◇

Now follows a formalization of the above procedure. For this, let $M(f_j)$ denote the model that is obtained by decoupling fault f_j, i.e. column F_j is moved from matrix $F(s)$ to $H(s)$ as was done in (12) in the example.

Theorem 4. Assume that all faults in $\mathcal{F}$ are detectable in the model M. Let $\mathcal{P} \subseteq \mathcal{X}$ be the set of possible sensor locations and M_S the equations corresponding to adding the set of sensors S. For an arbitrary fault f_j, the maximum possible number of faults $f_i \in \mathcal{F} \setminus \{f_j\}$ are isolable from f_j in $M \cup M_S$ if and only if S has a non-empty intersection with all sets in $\mathcal{D} = \texttt{Detectability}(M(f_j), \mathcal{F} \setminus \{f_j\}, \mathcal{P})$.

Proof. Assume that $D(f_i) \in \mathcal{D}$ and $S \cap D(f_i) = \emptyset$. This means that fault f_i is not isolable from fault f_j. But since $D(f_i) \neq \emptyset$, S can be extended so that $S \cap D(f_i) \neq \emptyset$. Hence, maximal fault isolability from f_j implies that S has non-empty intersection with all sets in $\mathcal{D}$.

Conversely, if S has a non-empty intersection with all elements in $\mathcal{D}$, then according to Theorem 3 maximum number of faults are detectable in $M(f_j) \cup M_S$ which means that maximum number of faults are isolable from f_j in $M \cup M_S$. □

The above result gives the solution for one sub-problem, i.e. how to place sensors such that faults are isolated from a specified fault f_j. How to combine the results from all sub-problems into a solution for the complete problem is summarized in the pseudo-code function below that returns the set of minimal sensor sets.

```
1 function S = SensPlaceInDetectable(M, F, P)
2   D = ∅;
3   for f_j ∈ F
4     F_d(f_j) := {f_i | i > j};
5     D_j = Detectability(M(f_j), F_d(f_j), P);
6     D := D ∪ D_j
7   end
8   S = MinimalHittingSets(D);
```

Remember that here it is assumed that all faults in $\mathcal{F}$ are detectable and this assumption will be lifted in the next section.

4.3 Sensor placement for both detectability and isolability

Section 4.1 described how to place sensors to achieve detectability and Section 4.2 how to achieve isolability in models where faults are detectable. The algorithms in these two sections will now be combined to achieve maximum isolability in a general model.

Below is an algorithm that, given a model M that fulfills the assumptions in Section 3.1, the faults $\mathcal{F}$, and the possible sensor locations $\mathcal{P}$, computes the set $\mathcal{S}$ of all minimal sensor sets that achieve maximum isolability.

```
1 function S = SensorPlacement(M, F, P)
2   D = Detectability(M, F, P);
```

```
3   if D = ∅
4     F_d = detectable faults in M;
5     D = SensPlaceInDetectable(M, F_d, P);
6     S = MinimalHittingSets(D);
7   else
8     S = ∅;
9     S_det = MinimalHittingSets(D);
10    for s_det ∈ S_det
11      Create the extended model M_e = M ∪ M_{s_det};
12      F_e = the detectable faults included in M_e;
13      D = SensPlaceInDetectable(M_e, F_e, P);
14      S_isol = MinimalHittingSets(D);
15      S := S ∪ {s_det ∪ s_isol | s_isol ∈ S_isol};
16    end
17    Delete non−minimal sensor sets in S;
18  end
```

4.4 Adding sensors with faults

Until now, we have assumed that new sensors cannot fail but this is of course not true for many applications. How to cope with new sensors that may become faulty will be treated next.

Example 4. Consider the example from Section 2. If new sensors are fault free, it has been shown in Section 4.1 that a minimal sensor set achieving maximum fault isolability is $\{x_1, x_3\}$. However, if the sensors measuring x_1 and x_3 have faults f_5 and f_6 respectively, the maximum fault isolability is not achieved when considering both the faults $f_1, \dots f_4$ in the original model and the faults f_5 and f_6 introduced by new sensors. For example f_3 is not isolable from f_5. By adding another sensor measuring x_1 and thereby introducing a new sensor fault f_7, maximum fault isolability is achieved when considering all faults $f_1, \cdots, f_7$. The sensor set $\{x_1, x_1, x_3\}$ is a minimal sensor set achieving maximum isolability when new sensors may become faulty. ◇

The following two theorems concerning detectability and isolability properties of faults in new sensors will be sufficient results for extending the algorithm to include these faults.

Theorem 5. Let $\mathcal{X}$ be the set of unknown variables in the model M and $x_i \in \mathcal{X}$ measured with a sensor described by an equation $e \notin M$. Then, a fault in the new sensor will be detectable in $M \cup \{e\}$.

Proof. Let $H_e(s)$ correspond to the $H(s)$ matrix for $M \cup \{e\}$ and F_e the column vector corresponding to the new sensor fault. According to Theorem 1 the fault in equation e is detectable if and only if $F_e \notin \text{Im } H_e(s)$, i.e. the equation

$$H(s)\xi(s) = 0$$
$$\xi_i(s) = 1$$

has no solution. The result follows immediately since $H(s)$ has full column rank. □

A consequence of this result is that we need not consider sensor faults related to sensors s_{det} in the detectability step when we extend the algorithm to include faults in new sensors.

Theorem 6. Let $\mathcal{X}$ be the set of unknown variables and $\mathcal{F}$ a set of detectable faults in the model M. Furthermore, let M_S be a set of equations describing additional sensors and $\mathcal{F}_S$ the associated set of sensor faults. Then for any sensor fault $f_i \in \mathcal{F}_S$ and for any fault $f_j \in (\mathcal{F} \cup \mathcal{F}_S) \setminus \{f_i\}$, it holds that f_i is isolable from f_j in $M \cup M_S$.

Proof. Let x_i be a variable measured by a new sensor described by equation e and with a fault f_i. Furthermore, let f_j be an arbitrary fault in $M \cup M_S$ such that $f_j \neq f_i$ and $H(s)$ and $F_j(s)$ matrices corresponding to the equations $M \cup M_S \setminus \{e\}$. Then Theorem 2 gives that a fault $f_i \in \mathcal{F}_S$ in new sensor is isolable from $f_j \in \mathcal{F} \cup \mathcal{F}_S \setminus \{f_i\}$ if and only if the set of equations

$$H(s)\xi(s) + F_j(s)f_j(s) = 0 \quad (13)$$
$$\xi_i(s) = 1 \quad (14)$$

has no solution. Fault f_j is detectable since by assumption, all faults in $\mathcal{F}$ are detectable and by Theorem 5 all faults in $\mathcal{F}_S$ are detectable in $M \cup M_S \setminus \{e\}$. It then follows that $F_j(s) \notin \text{Im } H(s)$, which together with (13) yields that $\xi(s) = 0$. This contradicts (14) which ends the proof. □

For the function `SensorPlacement`, this theorem implies that full isolability is achieved for all sensor faults introduced by the new sensors s_{isol} in the isolability step for free.

In conclusion, first the detectability step is performed as before, then new faults introduced by sensors in the detectability step are included in the model, and finally the isolability step is performed as before. The new faults introduced by sensors in the detectability step are included in the creation of the extended model M_e on line 10 in `SensorPlacement`.

4.5 Fault isolability performance specification

We have discussed sensor placement for achieving detectability and maximum isolability. Since fault isolability performance is gained at the expense of adding more sensors, it is important that the algorithm can handle more precise fault isolability specifications. In Section 2 it was stated that a detectability requirement is a set $\mathcal{F}_{det} \subseteq \mathcal{F}$ and an isolability requirement is a set $\mathcal{I}$ of ordered pairs $(f_i, f_j) \in \mathcal{F} \times \mathcal{F}$, meaning that f_i is required to be isolable from f_j. As stated in Section 2 it is assumed that all faults in $\mathcal{I}$ are also included in $\mathcal{F}_{det}$.

It is straightforward to modify the proposed algorithm with a detectability and isolability specification. Two modifications have to be made, one for each specification. First, on line 2 in function `SensorPlacement`, change $\mathcal{F}$ to $\mathcal{F}_{det}$. Second, on line 4 in function `SensPlaceInDetectable`, change

$$\mathcal{F}_d(f_j) := \{f_i | i > j, (f_i, f_j) \in \mathcal{I} \vee (f_j, f_i) \in \mathcal{I}\}; \quad (15)$$

Using $\mathcal{F}_{det}$ and $\mathcal{I}$ as above it is possible to give a detailed specification. However, it is often more natural and convenient to use other representations of the isolability specification. A simpler, but less general, specification is illustrated in the following example

Example 5. For the example given in Section 2, assume that we want to compute sensor placements such that faults in $\{f_1, f_2\}$ are isolable from faults in $\{f_3, f_4\}$ and vice verse, but for example fault f_3 need not be isolable from f_4. The family $\{\{f_1, f_2\}, \{f_3, f_4\}\}$ can then be used to represent the isolability specification.

It is straightforward to verify that this specification is equivalent to the isolability requirement

$$\mathcal{I} = \{(f_1, f_3), (f_1, f_4), (f_2, f_3), (f_2, f_4)\}$$

◇

5. EXAMPLE

In this section, the sensor placement algorithm will be demonstrated by applying it to the electrical circuit shown

in Figure 1. The circuit has 5 components, a voltage source $z(t)$, two resistors R_1 and R_2, an inductor L, and a capacitor C and they can fail independently of each other. The input signal $z(t)$ is assumed to be known. The branches are enumerated $k = 1, 2, \ldots 5$ and $f_1, \ldots, f_5$ denote faults in the corresponding components. The current through branch k is i_k and the voltage across is u_k. The behavior of the fault free system is given by

$$\begin{array}{lll} u_1 = z & u_2 = R_1 i_2 & u_3 = R_2 i_3 \\ u_1 = u_5 & u_5 = u_2 + u_3 & u_3 = u_4 \\ i_1 = i_2 + i_5 & i_1 = i_3 + i_4 + i_5 & \\ u_4 = L\dfrac{d}{dt} i_4 & i_5 = C\dfrac{d}{dt} u_5 & \end{array}$$

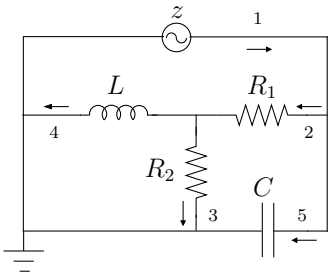

Fig. 1. An electrical circuit.

Assume that all added sensors can fail. For this case there are 7 minimal sensor sets achieving full isolability where 4 sensor sets has cardinality 3 and 3 sensor sets has cardinality 4. One of the minimal cardinality sensor sets is $\{i_1, i_1, i_4\}$, i.e. current i_1 is measured twice. For the case where new sensors can not fail, $\{i_1, i_4\}$ is a minimal sensor set but this does not give maximum isolability when sensor faults are considered. When only measuring i_1 once, the fault in the sensor measuring i_1 is not isolable from the capacitor fault. Interestingly, all minimal sensor sets include only current measurements meaning that any voltage measurement will be superfluous.

In the second run all inputs are the same as in the first run with the exception that only voltages can be measured because voltage measurements can be performed without disconnecting wires in the circuit. With this restriction full isolability cannot be achieved. The maximum isolability is that the voltage source fault can be isolated from all other faults, faults in the resistors and in the inductor are not isolable from each other, and the capacitor fault can even not be detected, i.e. $\{\{f_1\}, \{f_2, f_3, f_4\}\}$. There are 10 minimal sensor sets achieving this isolability and $\{u_2, u_3\}$ and $\{u_2, u_4\}$ are the ones with minimal cardinality.

In the third and final run, we input the isolability specification $\{\{f_1\}, \{f_2, f_3, f_4\}, \{f_5\}\}$, assumes that all voltages and currents can be measured, and sensors do not fail. This time there are 13 minimal sensor sets, all with cardinality 2. In this case the isolability achieved by different minimal sensor sets are not the same. For example, the set $\{i_1, i_4\}$, returned also in the first run, achieves full isolability, but for instance the minimal sensor set $\{i_2, i_5\}$ achieves exactly the specified isolability. Hence, some minimal sensor sets might achieve better isolability than specified but the retraction of any sensor in any minimal sensor set will take the isolability performance below the specified.

This example has been used in [8] to illustrate problems with structural approaches for determining the index of a DAE. Using the structural approach for sensor placement in [6], a non-trivial reformulation of the model equations are needed to obtain a characterization of all sensor sets.

6. CONCLUSIONS

An algorithm has been developed that computes a characterization of all sensor additions that makes a fault isolability specification attainable for a given linear differential-algebraic model. It may be the case that the fault isolation specification is not attainable, for example due to a restriction on possible sensor locations. In such a case, the algorithm then provides solutions that are as close to the specification with the available sensors. The new sensors added to make fault isolation possible may also become faulty. These additional sensor faults need to be considered in the analysis and it has been shown that it might be necessary to add more than one sensor measuring the same variable. Since the approach is analytical, the method can handle models where structural approaches fail.

REFERENCES

[1] M. Basseville, A. Benveniste, G.V. Moustakides, and A. Rougée. Optimal sensor location for detecting changes in dynamical behavior. *IEEE Transactions on Automatic Control*, 32(12):1067–1975, 1987.

[2] C. Commault, J. Dion, and S.Y. Agha. Structural analysis for the sensor location problem in fault detection and isolation. In *Proceedings of IFAC Safeprocess'06*, Beijing, China, 2006.

[3] M.O. Cordier, P. Dague, F. Levy, J. Montmain, M. Staroswiecki, and L. Travé-Massuyès. Conflicts versus analytical redundancy relations: a comparative analysis of the model based diagnosis approach from the artificial intelligence and automatic control perspectives. *IEEE Transaction on Systems, Man, and Cybernetics – Part B*, 34(5):2163–2177, 2004.

[4] J. de Kleer. Diagnosing multiple faults. *Artificial Intelligence*, 32(1):97–130, 1987.

[5] R. Debouk, S. Lafortune, and D. Teneketzis. On an optimization problem in sensor selection. *Discrete Event Dynamic Systems: Theory and Applications*, (12):417–445, 2002.

[6] Erik Frisk and Mattias Krysander. Sensor placement for maximum fault isolability. 18th International Workshop on Principles of Diagnosis (DX-07), pages 106–113, Nashville, USA, 2007.

[7] D. Henrion and M. Sebek. An algorithm for polynomial matrix factor extraction. *International Journal of Control*, 73(8):686–695, 2000.

[8] K. Murota. *Matrices and Matroids for System Analysis*. Springer-Verlag, 2000. ISBN 3-540-66024-0.

[9] M. Nyberg. Criterions for detectability and strong detectability of faults in linear systems. *International Journal of Control*, 75(7):490–501, May 2002.

[10] Mattias Nyberg and Erik Frisk. Residual generation for fault diagnosis of systems described by linear differential-algebraic equations. *IEEE Transactions on Automatic Control*, 51(12):1995–2000, 2006.

[11] R. Raghuraj, M. Bhushan, and R. Rengaswamy. Locating sensors in complex chemical plants based on fault diagnostic observability criteria. *AIChE*, 45(2):310–322, 1999.

[12] R. Reiter. A theory of diagnosis from first principles. *Artificial Intelligence*, 32(1):57–95, 1987.

[13] L. Travé-Massuyès, T. Escobet, and X. Olive. Diagnosability analysis based on component-supported analytical redundancy relations. *IEEE Transaction on Systems, Man, and Cybernetics – Part A*, 36(6):1146–1160, 2006.

[14] H. Wang, Z. Song, and H. Wang. Statistical process monitoring using improved PCA with optimized sensor locations. *Journal of Process Control*, (12):735–744, 2002.