



**HAL**  
open science

# A STRUCTURAL APPROACH FOR THE DESIGN OF FAILURE DETECTION AND IDENTIFICATION SYSTEMS

J P Cassar, M P Staroswiecki

► **To cite this version:**

J P Cassar, M P Staroswiecki. A STRUCTURAL APPROACH FOR THE DESIGN OF FAILURE DETECTION AND IDENTIFICATION SYSTEMS. Conference on Control of Industrial Systems, IFAC, May 1997, Belfort, France. 6 p. hal-01403803

**HAL Id: hal-01403803**

**<https://hal.science/hal-01403803>**

Submitted on 27 Nov 2016

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

## A STRUCTURAL APPROACH FOR THE DESIGN OF FAILURE DETECTION AND IDENTIFICATION SYSTEMS.

**J.P. Cassar, M. Staroswiecki**

*LAIL (URA CNRS 1440 D)  
UFR IEEA, Bâtiment P2  
Université des Sciences et Technologies Lille  
59655 Villeneuve d'Ascq Cedex (France)  
Téléphone : & fax (33) 03 20 43 47 43  
e-mail : cassar@univ-lille1.fr*

Abstract : this paper presents a structural approach for the study of the monitoring ability on large scale systems. The structural canonical decomposition, obtained as a result of a structural study based on graph theory, points out the monitorable part of the system and provides a way to generate residuals. From this result, some extensions are possible as direct residual generation by variable elimination or sensor implementation.

Keyword : Failure detection and isolation, structure system, graphs, sensors systems, Non linear systems.

### INTRODUCTION

Model based fault detection and isolation procedures (FDI) rest on the comparison between the actual behaviour of the system and a reference behaviour describing its normal operation. The reference behaviour is commonly expressed using a knowledge base representation or analytical models (Chow, *et al.*, 1984)

One of the most frequently used approaches is based on the use of Analytical Redundancy Relations (ARR) : the knowledge available upon the system leads to express its normal operation by a set of invariant features : the residuals of the ARR (coherence model). The fault detection amounts thus to a decision problem : is the variance of the residuals the effect of noise, of normal deviations and errors or is it the effect of a failure?

In a structural point of view, the system is modeled as a network of elementary activities, each of them processing a subset of variables. Among the set of all the variables, only some of them are known

(computed by elementary activities) or measured (a sensor performs also an elementary activity).

For a given instrumentation scheme, the canonical decomposition (Staroswiecki, *et al.*, 1989; Declerck, 1991) of the system structure exhibits a sub-system on which failure detection and identification procedures can be designed. Note that since only structural information are used, this approach applies to large scale systems described by a great number of variables, even when their analytical models are not precisely known.

The quality of the FDI procedure is then evaluated in terms of isolability of the different failure events through the set of invariant features that has been found (Cassar, *et al.*, 1994; Carpentier, *et al.*, 1996).

This paper first presents the principles of Fault Detection and Isolation. The second part tackles the structural analysis applied to the FDI systems design. In the last part, the structural principles are applied to problems related to FDI system design : sensors implementation and non linear systems monitoring.

## I. MODEL BASED MONITORING.

### I.1. System Modeling

When a model based approach is used, an operating model gives some information about the variables the plant involves. It can indicate the values that some variables should have in their simpler expression, or express some knowledge about the generating process of these variables.

The analytical model gives an explicit formulation of the operating model. It is generally made up of two parts:

- The first one describes the operation of the plant, including the actuators and the process dynamics. It expresses the way in which the controls are transformed into states. The state trajectories depend on the initial state for dynamic models.
- The second one describes the measurements that are available. It expresses the way in which the sensors transform some states of the process into output signals that can be used for control or FDI purposes.

Both parts of the analytical model depend on some parameters.

### I.2. FDI system.

Various approaches to F.D.I. using analytical redundancy have been proposed (see the surveys by P.M. Frank (1990), R. Iserman (1984), A. S. Willsky (1976)). They all consist of three main stages : in the first stage, residuals are generated using the operating model and the available information (inputs and outputs of the system). Residuals are variables whose value is zero when the plant operates normally under ideal circumstances (no noise, no modeling errors, no unknown inputs, no parameter deviation,...). Since those ideal circumstances will never be encountered, the residuals will differ from zero. This is why a decision procedure, in the second stage, is applied to the residuals. This procedure aims at discriminating those non zero values that are the result of Modeling errors, unknown inputs, measurement noises and those which reflect some abnormal behaviour in the plant (actuator, sensor, plant's component). On the basis of these results, the third stage will provide a fault or failure inference and isolate the part of the plant that is the most likely to be incriminated.

### I.3. Residuals generation

Let  $\mathbf{z}(t,t-p)$  be the vector of the values of a vector  $\mathbf{z}$  on a temporal window of size  $p$  :  $\mathbf{z}(t,t-p)^T = [ \mathbf{z}(t)^T, \mathbf{z}(t-1)^T, \dots, \mathbf{z}(t-p)^T ]$  where  $^T$  means transposition.

The analytical model of the system first expresses the relations between the internal variables  $\mathbf{x}(t,t-p)$  (as the state variables) and the control variables  $\mathbf{u}(t,t-p)$

and secondly the measurement  $\mathbf{y}(t,t-p)$  as functions of the internal variables.

$$F(\mathbf{x}(t,t-p), \mathbf{u}(t,t-p)) = 0 \quad (1)$$

$$\mathbf{y}(t,t-p) = G(\mathbf{x}(t,t-p))$$

In order to be able to check on line the actual value of the residuals, their computational schemes, at a given time  $t$ , must only make use of known variables, namely the values of  $\mathbf{u}(t,t-p)$  and of  $\mathbf{y}(t,t-p)$ . The unknown variables vector  $\mathbf{x}$  has thus to be eliminated in the system (1).

For that, three main approaches have been developed : parameter estimation, state estimation and input output models.

An input output model expresses some invariance property of the system in the form :

$$\mathbf{r}[\mathbf{u}(t,t-p), \mathbf{y}(t,t-p)] = \mathbf{0} \quad (2)$$

It is re-writing of the plant and measurement models in which only known variables intervene. In the linear case, they are named Parity equations, or Analytical Redundancy Relations (A.R.R.) in a more general case.

The equality to zero in (2) will in fact never hold since the system is never under ideal circumstances ; in that sense, the Analytical Redundancy based residual vector will take the form :

$$\mathbf{r}(t) = \mathbf{r}[\mathbf{u}(t,t-p), \mathbf{y}(t,t-p)] \quad (3)$$

The following part will now present how the structural analysis is used as a guideline for unknown variables elimination and thus for residuals generation.

## II. STRUCTURAL ANALYSIS.

### II.1. Structure of the model

From the very general point of view that is that of structural analysis, the model of the system is only considered as a set of constraints that apply to a set of variables.

Let  $\mathbf{F} = \{ f_1, f_2, f_3, \dots, f_m \}$  if the set is of the constraints that represent the system model and  $\mathbf{Z} = \{ z_1, z_2, z_3, \dots, z_n \}$  be the set of the variables.

The set  $\mathbf{Z}$  contains two subsets  $\mathbf{K}$ ,  $\mathbf{X}$ .  $\mathbf{K}$  is the subset of known variables : the control variables set  $U$  and the measured variables set  $Y$ . The set  $\mathbf{X}$  is the subset of the unknown variables.

The structure of the model is a digraph  $(\mathbf{F}, \mathbf{Z}, \mathbf{AZ})$  which associates the two sets that constitute the system,  $\mathbf{F}$  and  $\mathbf{Z}$ , with the set of the links between their elements,  $\mathbf{AZ}$ .

$F \times Z \rightarrow AZ$

$(f_i, z_j) \in AZ \iff$  the constraint  $f_i$  applies to the variable  $z_j$

Let  $a$  belong to  $AZ$ , we note  $v(a)$  the extremity of  $a$  in  $Z$  and  $c(a)$  the extremity of  $a$  in  $F$ , so  $a$  can be written :  $a = (c(a), v(a))$ .

## II.2. Monitorable Subsystems

### a. Subsystems

Let  $P(E)$  be the set of the subsets of a given set  $E$ ; we define constraint and variable structures using the following applications:

$Q: P(F) \rightarrow P(Z)$

$F \rightarrow Q(F) = \{ z_j \mid \exists f_i \in F, \text{ such that } (f_i, z_j) \in AZ \}$

**Definition:** A subsystem is a pair  $(F, Q(F))$  where  $F$  is a subset of  $F$ .

Let  $Q(F) = Q_k(F) \cup Q_x(F)$ , where  $Q_k(F)$  is the subset of the known variables in  $Q(F)$  while  $Q_x(F)$  is the subset of the unknown ones. The constraints that define the subsystem may be then written as:

$$F(Q_k(F), Q_x(F)) = 0 \quad (4)$$

### b. Monitorable subsystems.

**Definition:** A subsystem is monitorable if it is equivalent to analytical redundancy relations of form (2).

This property can be expressed as follows : the system is  $(F, Q(F))$  monitorable if and only if a transformation  $T$  can be found such that  $T[F, Q(F)] = (F', Q(F'))$  with  $K = Q(F')$

The analytical relation is then expressed as :

$$F'(Q(F')) = 0 \quad (5)$$

## II.3. Canonical decomposition.

According to the consideration given above, the problem of finding monitorable subsystems is equivalent to the problem of finding the subsystem in which  $Q_x(F)$  can be eliminated.

This part exhibits how the analysis of system structure with regard to the unknown variables set  $X$  can be a guideline for researching these subsystems.

### a. Complete matching.

Let us consider the graph  $G(F_X, X, AX)$ , which is the restriction of the system structural graph to the set of vertices  $X$ .

$AX$  represents the subset of the arcs of  $A$  which only link  $F$  to  $X$ .

$F_X = \{f_j \mid \exists x_i \in X \text{ such that } (f_j, x_i) \in AX\}$

**Remark:** in the sequel of the paper, we will consider that  $F_X = F$ . Indeed if the complement  $\bar{F}_X$  of  $F_X$  in  $F$  only involve known variables. The expression (4) becomes then :  $\bar{F}_X(Q_k(\bar{F}_X)) = 0$  which directly constitutes analytical redundancy relations. Thus, the subsystem  $(\bar{F}_X, Q_k(\bar{F}_X))$  is not worth being studied.

### Definitions:.

•  $G(F, X, A)$  is a **matching** on  $G(F, X, AX)$  if and only if:

1)  $A \cap AX = \emptyset$

2)  $\exists a_1, a_2 \in A$  with  $a_1 \neq a_2$

$c(a_1) \neq c(a_2)$  and  $v(a_1) \neq v(a_2)$

• A **maximal matching** on  $G(F, X, AX)$  is a matching  $G(F, X, A)$  such that:

$\nexists A' \subset A, A' \neq A$   $G(F, X, A')$  is not a matching.

• A matching on  $G(F, X, AX)$  is **complete** with regard to  $F$  ( respectively with regard to  $X$ ) if and only if:

$\forall f \in F, \exists a \in A$  such that  $c(a) = f$

(resp.  $\forall x \in X, \exists a \in A$  such that  $v(a) = x$ )

The problem of finding a maximal matching has been intensively addressed (Berge, 1973; Minoux, *et al.*, 1986; Roy, 1970), in order to propose algorithms whose complexity is only polynomial instead of exponential.

The basic condition for the existence of a complete matching is given by the Kőnig-Hall theorem (Berge, 1976):

a complete matching with regard to  $F_X$  exists on  $G(F, X, AX)$  if and only if :

$$\forall F' \subset F \quad |Q_X(F')| \geq |F'|$$

The dual result can be stated for the existence of a complete matching with regard to  $X$ .

### b. Decomposition

It has been demonstrated by P. Declerck (1991) that a system can be decomposed according to a canonical form using a maximal matching. The figure 1 exhibits this decomposition on the incidence matrix of the structure. The oblique straight line symbolises a maximal matching  $G(F, X, A)$  Some other results concerning digraph decomposition and algorithms in

order to find the canonical components can be found in (Dulmage, 1958; Murota, 1987).

The matching  $G(F, X, A_X)$  is complete with regard to  $X$ .

The matching  $G(F, X, A_X)$  is complete with regard to  $F$ .

The matching  $G(F, X, A_X)$  is complete with regard to  $X$  and  $|F| > |X|$ .

#### II.4. Subsystems characterisation

##### a. Complete matching interpretation

Let us now give an interpretation of the notion of complete matching.

Let us consider a sub-system  $(F', Q(F'))$ . In the case of numerical analytical model, the set of constraints (4) applied to  $(F', Q(F'))$  can be processed as a set of equations (6) to be solved with regard to  $X' = Q_X(F')$ .

$$F'(Q_k(F'), X') = 0 \quad (6)$$

##### Proposition 1:

the existence of a complete matching with regard to  $X'$  and  $F'$  is a necessary condition for the system (6) to be solved in  $X'$ .

Proof :

1)  $|F'| = |X'|$  constitutes a necessary condition for the solving of any numerical system.

2) Let us suppose that the system  $(F', Q(F'))$  includes a subsystem  $(F'' Q(F''))$  (said under determinate).

In such a sub-system,  $X''$  can't be solved though the condition 1) holds for the whole system. Indeed, by supposing  $X_s''$  be the solution of  $X''$ , the system of equation (6) is then reduced to the system (7) to be solved in  $X'$ .

$$F'(Q_k(F') X_s'', X') = 0 \quad (7)$$

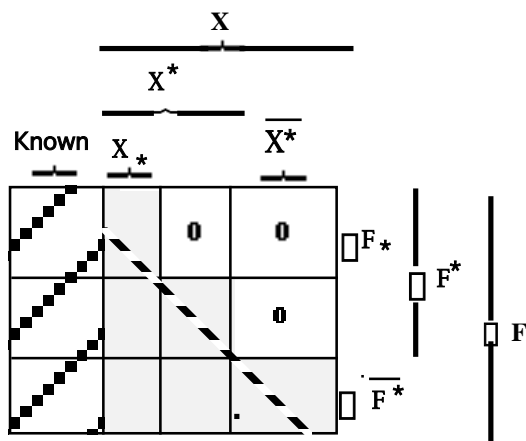


Figure 1 : Canonical decomposition of the system structure

From the definition of  $X'$  we have  $|F'| < |X'|$  and then the part 1) of the necessary condition doesn't hold.

3) Since the matching is complete with regard to both  $X'$  and  $F'$  one has obviously  $|F'| = |X'|$ . The condition 1) is verified.

From the canonical decomposition the complete matching on  $X'$  imposes that the subset  $X''$  is empty. So the case 2) can't occur and the whole set  $X'$  matched the necessary condition to be solved.

End of proof

**Remarks :** 1. In the linear static case, the existence of solution for the system of equations (6) depends on the rank of the matrix that represents the analytical model. The matrix determinant can be defined as the sum of all the complete matchings in the structure of the matrix. From this definition, the complete matching on the unknown variable is a necessary condition for the system to be of full rank.

2. In the non linear static case, the structure of the jacobian matrix of the system is the structure of the system too (Murota, 1987). So local solutions around an operating point can be considered as in the linear case.

##### b. Bad conditioned sub-system

The complete matching doesn't constitute a sufficient condition. Indeed, in some particular cases the system (6) is bad conditioned. Such a system can be transformed in an other one  $(F'', Q(F''))$  in such a way that the difference  $|F''| - |X''|$  is greater than  $|F'| - |X'|$ .

This case can be summarized by the figure 2.

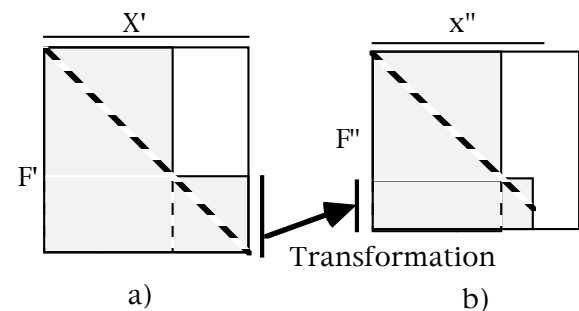


Figure 2 : bad conditioned system reduction

In this case the system of equations (6)  $(F'(Q_k(F'), X') = 0)$  can't be solved in  $X'$ , while the system  $F''(Q_k(F''), X'') = 0$  has got a solution in  $X''$ .

From the figure 2-b and the explanation above, the subsystem  $(F'', X'')$  belongs to the subsystem  $(F, X)$  of the decomposition.

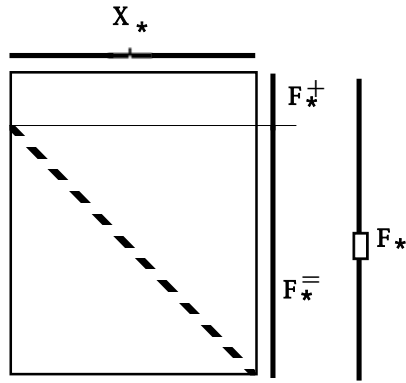


Figure 3 : monitorable sub-system

*c. Monitorable sub-systems*

Let us consider the component  $(F_{\square}, X_{\square})$  of the canonical decomposition. Let  $F_{\square}^{-}$  be  $c(A_{\square}) \square F_{\square}$  the part of  $F_{\square}$  associated with the complete matching and let  $F_{\square}^{+}$  be its complement in  $F_{\square}$ . That leads to the notations of the figure 3.

Proposition 2.

If the canonical decomposition makes a component  $(F_{\square}, X_{\square})$  appear, this subsystem constitutes a monitorable subsystem.

Proof :

We have to consider two cases :

1) The sub-system  $(F_{\square}^{-}, X_{\square})$  is well conditioned. Let  $X_s(Q_K(F_{\square}^{-}))$  be the solution of the corresponding system of equations for given values of  $Q_K(F_{\square}^{-})$ . Using the remaining relations  $F_{\square}^{+}$  leads to :

$$F_{\square}^{+}(Q_K(F_{\square}^{+}), X_s(Q_K(F_{\square}^{-}))) = 0$$

which constitutes a set of analytical redundancy relations.

2) The sub-system  $(F_{\square}^{-}, X_{\square})$  is bad conditioned. It can then be reduced as explained above and directly leads to a well conditioned sub-system corresponding to case 1.

In both cases the subsystem is monitorable.

End of proof

Remark :

In the case 2), the constraints  $f \square F_{\square}^{+}$  can only be used if  $Q_X(f)$  is included in the set of variables which can be solved from the reduced subsystem.

II.5. Residuals Generation.

The analytical redundancy relations, which are used for the residual computation, can be derived from monitorable sub-system using two approaches.

The first approach has been used in the proof given above. It decomposes the generation process into two stages : the first one is the computation of the solution with regard to the unknown variables ; in the second stage this solution is substituted into the remaining relations.

The second approach aims to eliminate the set of unknown variables in a single operation. In the linear case, the projection operation is used for this purpose and that leads to the parity techniques (Chow, *et al.*, 1984) . In the case of polynomial models, the theory of elimination can be used (Guernez, *et al.*, 1996).

III. RELATED RESULTS

III.1. Model manipulation

*a. System reduction*

As mentioned above, the redundancy relations are obtained by eliminating the unknown variables. In the case of polynomial models, the theory of elimination (Cox, *et al.*, 1992) can be used to eliminate recursively some subsets of unknown variables associated to sub-systems with appropriate structural properties (Guernez, *et al.*, 1996).

*b. Elimination guideline*

The theory of elimination leads to tools which are only able to deal with small sized system. The analysis of the structure provides guidelines which allow to decompose and to order the process of elimination (Guernez, *et al.*, 1996).

III.2. F.D.I. system performances

*a. Failure signatures*

Failures can be defined as the dysfunction a component of the system (sensors, actuator, ...) associated to a constraint relation of the operating model. The signature of a failure is defined as the set of residuals whose computation uses the constraint associated with the failure. A binary vector can be associated with each signature (Cassar, *et al.*, 1994).

*b. Performances criteria*

The ability to distinguish the effects of the failure events on the residual results defines the isolation performances derived from the set of redundancy relations. It can be evaluated by calculating the Hamming distance between each pair of signatures of failure events.

It can be shown that the isolation capability increases with the number of redundancy relations.

*b Control of the Residuals structure*

From an initial set of redundancy relations, it is possible to generate new relations leading to suitable isolation properties. In the linear case, this is achieved by appropriate linear combination of the residuals (Staroswiecki, *et al.*, 1991). In the non

linear case, the theory of elimination is used again (Guernez, *et al.*, 1996).

### c. Sensors location

All the analyses performed above rest on the basis of a given instrumentation. This has been designed for other purposes than F.D.I. and the obtained performances can be limited. The sensors location procedure starts from the definition of the failures to be processed and locates the sensors by using a structure guided recursive algorithm in order to obtain the desired performances (Carpentier, *et al.*, 1996).

## IV. CONCLUSION.

The structural decomposition of a system we have presented constitutes a good way to analyse the redundancy of the knowledge available about the system. This redundancy is used to detect and isolate eventual faults and failures.

Structural analysis appears to be a good tool for some related studies. However, the results are always subject to a limitation which rests on the possibility of bad conditioned sub-system. These cases can be detected by the structural analysis which ignores the analytical aspect of the model.

However this approach makes no hypothesis about the kind of model which should be used and can then be applied to various process models. From this point of view, it can be considered as a very powerful pre-processing of any classical residual generation method applied to large scale systems.

## REFERENCES.

- Berge, C., (1957), Two theorems in graph theory., *Proceedings of the National Academy of Science*, vol **43**, 842-844.
- Berge, C., (1973), *Graphe et hypergraphes.*, Dunod, Paris.
- Carpentier, T., R. Litwak, (1996) Algorithms for Sensor Location in view of Supervision, IEEE-SMC Conf. CESA'96, Symposium on Control, Optimization and Supervision, pp. 684-690, July 9-12 1996, Lille, France.
- Cassar, J. Ph., R. G. Litwak, V. Cocquempot, M. Staroswiecki (1994). Approche structurelle de la conception de systèmes de surveillance pour des procédés industriels complexes. *Revue Européenne de Diagnostic et Sécurité de fonctionnement*. Vol **n°2**, p. 179-202.
- Chow, E. Y., A. S. Willsky, (1984), Analytical redundancy and the design of robust failure detection system, IEEE trans. A. C., vol. AC 29 n°7, July 1984.
- Cox, D., J. Little, D. O'Shea (1992). *Ideals, Varieties and Algorithms*. Undergraduate texts in Mathematics, Springer Verlag, New York.
- Declerck, P. (1991), Analyse structurale et fonctionnelle des grands systèmes. Application à une centrale PWR 900 MW., Thèse de doctorat, Université des Sciences et Technologies de Lille, Villeneuve d'Ascq, France, 20 décembre 1991.
- Dulmage, A. L., N. S. Mendelshon, (1958), Covering of bipartite graphs., *Canadian Journal of Mathematics*, 1958, vol **10**, 517-534.
- Frank, P. M., (1990), Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy - A survey., *Automatica* vol **26**, n° 3, pp 459-474.
- Guernez, C., J. Ph. Cassar (1996), M. Staroswiecki, Fault Detection and Isolation on Polynomial systems : Analytical Redundancy Relations Generation and Residuals Structuration, IEEE-SMC Conf. CESA'96, Symposium on Control, Optimization and Supervision, pp. 690-695, July 9-12 1996, Lille, France.
- Iserman, R., (1984), Process fault detection Based on Modelling and Estimation Methods. A survey., *Automatica*, vol. **20** n°4, pp 387-404.
- Minoux, M., G. Bartnik, (1986) *Graphes Algorithmes Logiciels.*, Dunod Informatique, Paris.
- Murota, K., (1987), *System analysis by graphs and matroids.*, Springer Verlag.
- Roy, B., (1970), *Algèbre moderne et théorie des graphes.*, Dunod, Paris.
- Staroswiecki, M., V. Cocquempot, J. Ph. Cassar, (1991), Optimal design of FDI systems via parity space and observer based approaches., Proceedings of IECON'91, Kobe, Japan, October 28-November 1 1991, 143,148.
- Staroswiecki, M., P. Declerck, (1989), Analytical redundancy in non linear interconnected systems by means of structural analysis. AIPAC'89 IFAC Symposium on Advanced Information Processing in Automatic Control, Nancy, France, 3-5 July, 1989, pp II 23-27.
- Willsky, A. S., (1976), A survey of design methods for failure detection in dynamic systems., *Automatica* vol **12** pp 601-611.