12th IMEKO TC1 & TC7 Joint Symposium on
Man Science & Measurement
September, 3 – 5, 2008, Annecy, France

DESIGN AND OPTIMISATION OF DEPENDABLE MEASUREMENT SYSTEMS

Blaise CONRARD , Mireille BAYART

Laboratoire d'Automatique, Génie Informatique et Signal (UMR 8146)
Polytech'Lille, 2 Bd Langevin, 59655 Villeneuve d'Ascq, France

Blaise.Conrard@polytech-lille.fr, Mireille.Bayart@univ-lille1.fr

Abstract: This paper deals with the use of a structural modelling in order to optimise the cost of a measurement system with dependability constraints. The aim of the proposed method is to determine the sensor placement that tolerates a given number of failures with the lowest cost. A structural model is used. It describes the links between the physical quantities and is employed in order to determine the potential analytical redundancies. With that, the optimisation problem becomes an integer linear programming (ILP) problem whose resolution provides the best reliable and lowest-cost system.

Keywords: sensor placement, structural analysis, dependability assessment, optimisation.

1. CONTEXT

Concerning production systems or embedded systems, their dependability mainly depends on the reliability of their measurement system. Indeed, if a sensor fails and does not send its measure to the control system, the whole can become unavailable and it can inflict economic losses on its owner. Another more serious case concerns a sensor that provides a false measure and that leads the system to an unsafe position for the environment or the operators that work close to it.

Consequently, the design of a measurement system is a complex and cautious activity. Indeed, two antagonist aspects have to be taken into account [1]. The system must be inexpensive thanks to the mineralization of the number of components and it must be fault tolerant thanks to the using of hardware and analytical redundancies.

This paper presents a way to optimize the measurement system in order to find the system that provides a required level of fault tolerance with the lowest cost. The aims of the paper are, firstly, to present the concepts and structural modelling used, and, secondly, to describe the optimisation method.

2. USED CONCEPTS AND MODELLING

This section describes a way to model a measurement system and to assess its dependability, during its design step.

2.1 Level of fault tolerance

Designing a dependable measurement system requires a way to assess the dependability of the system. The proposed criterion is based on the evaluation of its capacity to tolerate failures during its operating phase. Rather than a quantitative probability estimation, the paper proposes to use a semi-qualitative evaluation. It consists in assessing the capacity of tolerating failures, thanks to the maximum number of failures that the system can simultaneously have without providing any false information or without detecting an internal problem.

From a practical point of view, this method is attractive. Indeed, it enables a system to be evaluated without having lot of information about the reliability characteristics of all usable devices. These data are often difficult to find because they are not always provided by the suppliers or they are often imprecise since they concern new complex devices containing both electronic components and software elements used in a given and precise environment.

2.2 Structural modelling

A physical process can be modelled by a set of variables, each of them corresponding to a physical quantity. A set of physical equations links these variables and constitutes a set of constraints. In structural model [2,3], an incidence matrix is used to model the system and this set of constraints. Each row corresponds to an equation and each column to a variable. A 1 in position (i, j) indicates that variable j appears in constraint i.

For instance, with the following system made of3 pipes, the next matrix shows the relation between their flow and expresses that if two flows are known the last one can be evaluated.

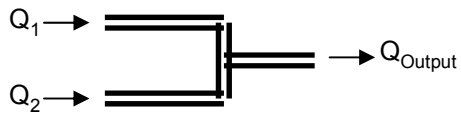

Fig. 1. 3 pipes

Table 1. Incidence matrix for 3 pipes

Q_1	Q_2	Q_{Output}
1	1	1

Thus, this model based on this incidence matrix provides a means to represent the different constraints that link physical quantities and in a second step is used to determine different ways to evaluate a physical quantity according to other ones. Another interest of this modelling is that it does not need the exact establishment of physical equations. Consequently, this makes easy the building of this model and accelerates the design phase.

2.3 Measurement points

A physical process has a set of points where sensors can be implemented and can provide a measure of a corresponding physical quantity. The aim of the design step consists in determining on each point the number of sensors that have to be implemented. With this goal, the proposed method consists in listing the points that we shall call here measurement points.

From this, the incidence matrix has to be completed and integrates these measurement points as new variables usable and reachable by the control system. For instance, with the previous example of 3 connected pipes, they are 3 points on which flowmeters can be implemented, and consequently 3 new variables associated to the measure of the flows.

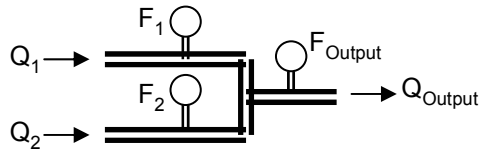

Fig. 3. 3 pipes with flowmeters

Table 2. Incidence matrix for 3 pipes with flowmeters

Q_1	Q_2	Q_{Output}	F_1	F_2	F_{Output}
1	1	1			
1			1		
	1			1	
		1			1

2.4 Establishing of measurement ways

Thanks to the incidence matrix, the various ways of measuring a given physical quantity can be found [4]. It consists in determining all the combinations of measurement points that can be used to evaluate the value of the considered quantity.

More especially, at first, it consists in searching if a measurement point can provide the considered physical quantity. Subsequently, each constraint that contains the searched quantity is used and provides an analytical way to estimate this quantity. A recursive approach is then used in order to determine the different possibilities to obtain the needed variables used in the considered constraint. Globally, a set of methods of estimating the value of a physical quantity thanks to known and reachable variables can be determined.

In the previous example, the 2 ways of obtaining the Q_{Output} quantity can be found thanks to this method. The first way is by using the F_{Output} measure, deduced from the last constraint. The second way is by using the F_1 and F_2 measures presented in the first constraint that describes that Q_{Output} can be estimated by Q_1 and Q_2 and by the two following constraints that express that Q_1 and Q_2 are provided by the F_1 and F_2 measures. Consequently, the possibility to estimate the Q_{Output} quantity can be summed up by the following relation :

$$F_{Ouput} \vee (F_1 \wedge F_2) \Rightarrow Q_{Output}$$

2.5 FTL function

In order to quantify the level of fault tolerance concerning the measure of a physical quantity q, the presented method proposes to use the function FTL(q) (Fault Tolerance Level). This function provides the minimal number of failures that can induce the unavailability of the measure of q for the control system.

According to the previous section, several ways enable the estimation of the physical quantity q. It can be obtained directly by a sensor or by an analytical relation between other measures.

If q can be obtained by a measurement point, the value of FTL(q) is equal to the number of redundancy sensors implemented on this point. Indeed, this number of sensors (n_q) gives the number of provided images of the measure q and consequently it corresponds to the minimal number of required faults to induce the unavailability of the concerned measure.

$$FTL(q) = n_q$$

If the quantity q is obtained and estimated by a combination of other measures associated with an analytical relation, its level of fault tolerance depends on the level of the used measures. It is assessed by the minimal level of all used measures. Indeed, the used measure with the lowest level defines the number of needed failures that stop the quantity estimation. For example, if the physical quantity Q can be deduced from the measures M_1 and M_2, it level can be determine from the next relation and depends on the number of redundant sensors (N_{M1} and N_{M2}) used to measure M_1 and M_2:

with $Q = function(M_1 , M_2)$

$$FTL(Q) = FTL(M_1 \wedge M_2)$$
$$= \min(FTL(M_1), FTL (M_2))$$
$$= \min(N_{M1}, N_{M2})$$

Finally, when there are several methods to estimate a quantity q, its fault tolerance level is determined by the sum of the level of each estimation way. Indeed, this set of methods forms a set of redundant measures and the minimal number of needed faults that makes all of them unavailable is equal to the sum of the minimal number of faults that makes each of them unavailable. This sum is valid with the assumption that the different methods of measuring are independent and do not use a same measurement point.

For example, in the previous example with 3 pipes, there are 2 means to estimate the flow Q_{Output}, either directly thanks to the measurement point F_{Output}, or thanks to a relation using the measurement points F_1 and F_2. According

to the number of sensors (N_x) implemented in each measurement point, the fault tolerance level is deduced:

$$F_{Ouput} \vee (F_1 \wedge F_2) \Rightarrow Q_{Output}$$
$$FTL(Q) = FTL(F_{Ouput} \vee (F_1 \wedge F_2))$$
$$= FTL(F_{Ouput}) + FTL(F_1 \wedge F_2)$$
$$= FTL(F_{Ouput}) + \min(FTL(F_1), FTL(F_2))$$
$$= N_{F\,Ouput} + \min (N_{F1}, N_{F2})$$

To sum up, the properties for the FTL function are the following ones, in which q_n represents a physical quantity and the operators $\wedge$ an association of them in order to estimate another quantity:

$$FTL(q_1 \wedge q_2) = \min (FTL(q_1) , FTL(q_2))$$
$$FTL (q) = N_{Sensor\ q}$$

And with the assumption that q_1 and q_2 are independent methods that is to say they not use a same measurement point:

$$FTL(q_1 \vee q_2) = FTL(q_1) + FTL(q_2)$$

2.6 Particular constraints

In certain cases, some considered variables cannot be evaluated from the other ones due to the nature of the equation that links them. For example, it is the case of variables whose derivation only appears in the equation and that forbids their evaluation from the other ones. Another case concerns the Boolean variable whose state depends on a condition about another one; the first one can be evaluated from the second, but not the contrary.

The structural modelling takes this situation into account by using the value of -1 instead of the previous 1. When this value of -1 appears, the concerned constraint expresses that the corresponding variable cannot be determined by the other variables.

In the previous example, if the control system needs to know only if the output flow is nil. A corresponding Boolean variable ($Q_{Output=0}$) is added. In the incident matrix the value -1 is placed for Q_{Output} in order to express that the value of $Q_{Output=0}$ can be deduced from the quantity Q_{Output} but not the contrary. The next figure shows this configuration in where a flow detector is proposed (FD_O).

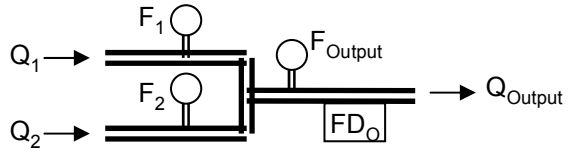

Fig. 2. 3 pipes with a flow dectector

Table 2. Incidence matrix for 3 pipes with flowmeters

Q_1	Q_2	Q_{Output}	$Q_{Output=0}$	F_1	F_2	F_{Output}	FD_O
1	1	1					
		-1	1				
1				1			
	1				1		
		1				1	
			1				1

When the incident matrix has values -1, the method of establishing of measurement ways (section 2.4) is modified. When different ways of estimate a variable are research, the constraints that have a value -1 for this variable are not considered.

2.7 Integration of operating mode

When some actuators are used, several operating modes can be defined according to the combination of active or idle actuators. The measurement system can have access to the order transmitted to each actuator and consequently can use these data in order to determine if a particular means to evaluate physical quantities can be used. The incidence matrix can be completed with this information by adding new columns that correspond to the actuators and that define if they are in a particular position.

For instance, if 2 valves are added to the previous example, the incidence matrix contains 2 new variables associated to each valve. With them, two new constraints are added and express that if a valve is close, the corresponding flow can be determined.

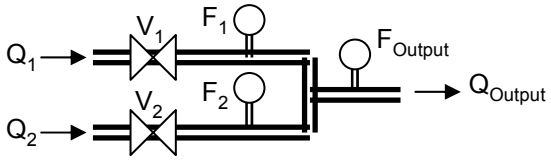

Fig. 4. 3 pipes with 2 valves

Table 3. Incidence matrix for 3 pipes

V_1	V_2	Q_1	Q_2	Q_{Output}	F_1	F_2	F_{Output}
		1	1	1			
		1			1		
			1			1	
				1			1
Close		1					
	Close		1				

With that, thanks to the first constraint, the incidence matrix allows to deduce that if a valve is closed, there is a direct relation between the two other flows. Thus, in this particular operating mode where V1 is closed, the measure of the output flow can be made by only one flowmeter, F_O or F_2 and without using the association of F_1 and F_2 as it was found previously.

Consequently, for each physical quantity, the current operating mode when this quantity is needed can be specified and allows to find new other ways to estimate it. During the establishing of measurement ways, only the constraints that match with the specified operating mode are the taken into account.

2.8 Integration of operating mode

As the operating mode, some constraints can be defined ore used only if an initial state is known. It is the case of relations that has an integration operator and that need to know the value of certain variable at a known time.

For instance, in the forward example where a tank is used, the level of fluid in it can be determined by the quantity of fluid added only if the level before its filling is known.

3. OPTIMISATION METHOD

Based on the previous considerations, this section presents the proposed method of designing a measurement system.

3.1 Principle of the proposed method

The proposed method uses the following steps:

a. The designer describes the system thanks to the various measurement points and for each of them, the cost of corresponding sensor. With this data, the method will determine the adequate number of sensor that minimise globally the cost of the system.
b. Subsequently, he describes the physical quantities required by the control system and if necessary in which operating mode, these quantities are required. Simultaneously, he sets a required fault tolerance level for each quantity. This level corresponds to the limit number of failures with which the measure can occur become unavailable. Indirectly, with this data, the designer specifies the global dependability level for the system.
c. Thirdly, he builds the structural model that forms the base to determine the different means of measuring or estimating each required physical quantity.
d. From all these data, the optimization phase can begin and will provide among every possible measurement system, one that suits the fault tolerance constraints and that has the minimal cost.

3.3 Constrains transposition

The first step of the optimization phase is the transposition of the required fault tolerance level for each needed physical quantity into a set of constraints applied on the measurement points.

The function FTL(q_i) (Fault Tolerance Level) is used to specified the fault tolerance level for each needed measure quantity (q_i), according to the importance of the considered quantity. By specifying a minimal value, the designer defines the number of failures that can render unavailability each measure provided by the measurement system. Consequently, the required dependability of the measurement system is given by a set of minimal fault tolerance levels, as it follows :

$$\begin{cases} FLT(q_1) \geq n_1 \\ FLT(q_2) \geq n2 \\ ... \end{cases}$$

Thanks to the study of the structural model, a set of methods to evaluate each needed physical quantity is determined. This set of methods is expressed by a set of required measures. Each of these measures corresponds to a measurement point where one or several sensors can be implemented. A Boolean equation is used to represent the various combinations of measures that enable the estimation of the required physical quantity. Consequently the previous system of inequations becomes the following one, in where each needed quantity has been replaced by the corresponding combination of required measures.

$$\begin{cases} FLT(p_1 \vee p_2 \wedge p_3 \vee ...) \geq n_1 \\ FLT(p_4 \vee p_5 \vee ...) \geq n_1 \\ ... \end{cases}$$

Thanks to the following properties of function FTL, the fault tolerance constraints applied to the measure of a physical quantity will be transposed into a set of inequations.

$FLT(a \wedge b) \geq n$
$\quad => FLT(a) \geq n$ and $FLT(b) \geq n$

$FLT(a \vee b) \geq n$
$\quad => FLT(a) + FLT(b) \geq n,$
if a and b are independent

To do it, we propose to change each Boolean expression by its conjunctive form, in order to simplify the transposition and in order to take into account the possible dependences between the different groups of measures.

For instance, if the designer sets value 2 for the fault tolerance level of the measure of the output flow in the previous example with 3 pipes. The obtained relations are the following :

$FLT(Q_{Output}) \geq 2$ implies that
$FLT(F_{Ouput} \vee F_1 \wedge F_2) \geq 2$
since we have found: $F_{Ouput} \vee (F_1 \wedge F_2) => Q_{Output}$
On a conjunctive form, this relation becomes:
$FLT((F_{Ouput} \vee F_1) \wedge (F_{Ouput} \vee F_2)) \geq 2$
Consequently, the resulted system of inequations can be deduced and is the following one:

$$\begin{cases} FLT(F_{Output} \vee F_1) \geq 2 \\ FLT(F_{Output} \vee F_2) \geq 2 \end{cases}$$

or:

$$\begin{cases} FLT(F_{Output}) + FLT(F_1) \geq 2 \\ FLT(F_{Output}) + FLT(F_2) \geq 2 \end{cases}$$

Finally, in this system of inequations, the fault tolerant level functions are replaced by the number of sensors in order to form a system of constraints that the measurement system has to satisfy:

$$\begin{cases} N_{F_{Output}} + N_{F_1} \geq 2 \\ N_{F_{Output}} + N_{F_2} \geq 2 \end{cases}$$

3.3 Optimisation

From the structural model and from the fault tolerance level specified for each physical quantity that the measurement system has to provide, the optimisation corresponds to a problem of cost minimisation associated to a system of inequations.

Since the function FLT(P) where P is a measurement point, is equivalent to the number (N_x) of sensors placed on the corresponding point, the final problem is as follows:

$$\begin{cases} minimize(N_1.Cost_1 + ... + N_m.Cost_m) \\ N_1 + N_2 \geq n_1 \\ N_1 + N_3 \geq n_2 \\ ... \end{cases}$$

This form corresponds to a classical integer linear programming (ILP) problem. A way to solve it, is the use of a Branch and Bound algorithm [5]. It consists of a systematic enumeration of all candidate solutions, where large subsets of fruitless candidates are discarded. For very huge systems whose number of solutions is too high and that need a too long time of treatment, an exhaustive algorithm cannot be used. In this case, although an optimal solution is not ensured, the genetic algorithms can be used and provide satisfactory solutions from an industrial point of view.

4. ILLUSTRATIVE EXAMPLE

This section presents the application of the presented method on an illustrative example.

4.1 General description

The considered process is a tank whose role is the mixing of 2 fluids with the same proportion before draining off toward the rest of the system. One of the interests of this example is that a same measurement point can be used to evaluate various physical quantities according to the operating mode of the system, such as the filling of the tank with one or two fluids or as the draining. Another interest is that 2 ways of filling the tank are considered: either one fluid then the other one or simultaneously. More especially, if the physical quantities needed by the control system are the same, the operating mode differs.

4.2 Description of the process

The process is shown on figure 4. 10 physical quantities are needed to describe this system and required by the control system. There are the tank fluid level (N), and 3 fluid levels (N_L, N_I, N_U) which are Boolean variables and that express if the fluid level is at low, intermediate or upper position. The variables Q_{F1} and Q_{F2} represent the quantity of fluid 1 or 2 in the tank. Concerning the different flows, there are flows Q_1, Q_2, Q_O associated to each pipe and finally T represents the temperature of the mixture in the tank.

Concerning the measurement point, the following sensors are proposed. 5 of them (F_1, F_2, F_O, N and T) are analogical sensors and the other (D_1, D_2, D_U, D_I D_L, D_O) are digital ones. According to the method, the following step is the specification of the cost of each sensor for each measurement point. For this illustrative example, a cost of 5 is chosen for the analogical sensors and a cost of 2 for the discrete ones. Consequently, one goal of the method is the select of the best suitable type of sensor.

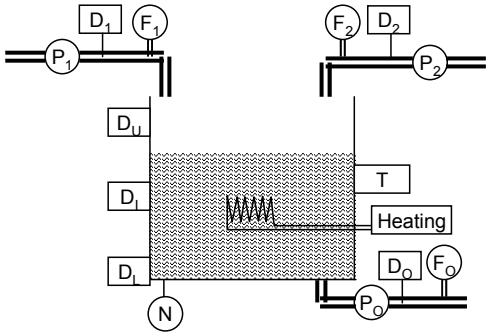

Fig. 4. 3 pipes with flowmeters

The next step deals with the structural analysis and the building of the incidence matrix. This matrix is shown on table 5. Some constraints define particular relations usable when a pump is stopped, or when the initial state (IS) is known. Indeed, if the tank is initially empty (E in the table), the quantity of each fluid in the tank can be evaluated thanks to the flow of each fluid. In the same way, if the tank fluid level is initially in a known position (E: empty, I: intermediate) and if the tank is filled by only one fluid, its quantity in the tank can be estimated from the tank level sensor.

4.3 Optimisation and result

After performing the optimisation for various required fault tolerance levels and for the 2 ways of filling, the synthesis of the results is present on the following table.

Table 4. Incidence matrix for the tank process

	sequential filling	simultaneous filling
FTL =1	cost = 10 sensors: N, T	cost = 15 sensors: N, D_2, T
FTL =2	cost = 20 sensors: 2×N, 2×T	cost = 27 sensors: N, D_1, D_2, 2×T, D_L

For the presented example, only in one case, solutions with only analogical sensors are the ones with the lowest cost. Indeed, the digital sensors are only interesting to implement a survey system that has in charge the checking of actuators' state. As we can expect, the costs of the proposed solutions are quite proportional to the required fault tolerance level. But if the designer wants to improve the speed of the process thanks to a simultaneous filling of the tank with the two fluids, the additional cost is about 50% higher than the sequential way of filling.

Table 5. Incidence matrix for the tank process

P_1	P_2	P_O	IS	N	N_L	N_I	N_U	Q_1	Q_{F1}	Q_2	Q_{F2}	Q_O	T	F_1	D_1	F_2	D_2	F_O	D_{FO}	D_E	D_I	D_U	L_F	T
				1				1		1		1												
				-1	1																			
				-1		1																		
				-1			1																	
Stop								1																
	Stop									1														
		Stop										1												
		Stop	E					1	1															
		Stop	E							1	1													
	Stop	Stop	E			1			1															
Stop		Stop	I				1				1													
								1						1										
								-1							1									
										1						1								
										-1							1							
												1						1						
												-1							1					
					1															1				
						1															1			
							1															1		
				1																			1	
													1											1

5. CONCLUSION

This paper presents a relatively easy-to-use design method. Indeed, it requires a reduced amount of data, that is to say, an incidence matrix built by a structural modelling and the cost of the potential usable sensors. With that, the method gives the sensor placement that offers a given fault tolerance level, with the lowest cost. Consequently, its main interest is that it can be used very early for the design of a measurement system and it provides a first cost estimate to the designer. Moreover, the way of using fault tolerance with a semi-qualitative point of view, is well-suited to present problems, for which the designers have at their disposal little information concerning the reliability of new sensors included electronic devices associated to embedded software.

6. REFERENCES

[1] Conrard B, Bayart M., Design of safe control system thanks to a combinatorial optimization, Proceeding of SafeProcess'03, Washington D.C., June 2003

[2] Düstegor D., Frisk E., Cocquempot V., Krysander, M., Staroswiecki M., *Structural Analysis of Fault Isolability in the DAMADICS Benchmark*, CEP. Vol 14, issue 6, June 2006, pp. 597-608

[3] Cassar J.P.C, Litwak R.G., Cocquempot V., Staroswiecki M., Approche structurelle de la conception de systèmes de surveillance pour des procédés industriels complexes, Revue Européenne de Diagnostic et sûreté de fonctionnement - Vol 4, n°2, p179-202, 1994

[4] Blanke M., Kinnaert M., Lunze J., and Staroswiecki M., Fault diagnosis and fault tolerant control, Chapter « Structural analysis », Springer-Verlag, 2003.

[5] Roucairol C., *Solving hard combinatorial optimization problems*, in: Proceeding of CESA'98, pp. 66-72, 1998