

Design of control architecture based search algorithm for fault—tolerant control system.

Zine-eddine Meguetta, Blaise Conrard and Mireille Bayart

Abstract—This article focuses on the design of the control system instrumentation. It proposes an algorithm for determining the architecture of a control system. This algorithm is based on a structural model that links the physical variables, the measures and the control variables. A method to optimize the system according to its cost as a criteria and its dependability as constraints are presented. This constraint uses a Fault Tolerant Level (*FTL*) that specifies the dependability and fixes the number of failures that can induce the unavailability of system. In this context, the optimization consists in finding the instrumentation that satisfies *FTL* as the constraints and that has the lowest financial cost. The main contributions of this paper are: i) The development of an algorithm for finding all paths of the control $u(t)$ according to the measures provided by the sensors and actuators and based on the constraints of structural model. ii) Formalization of the optimization problem that takes into account the costs of instruments and a specified *FTL*. The speed control system of an electrical vehicle is used as an illustrative example.

I. INTRODUCTION

Associated with an increasing demand for high performance control as well as for more dependability and control instrumentation of dynamical systems, and a natural trend toward system automation, structural modeling and Fault Tolerant Level (*FTL*) is becoming a strategic necessity as a result of increasing economic and environmental demands.

Over the past few years, there has been significant research effort in the analysis of dynamics systems, namely structural analysis [1]-[3]. Reference [2] presents the structural analysis to determine all the possible ways to estimate an unknown quantity from the known ones such as measurements or control signals.

The structural analysis model is presented in [1] in order to take into account different operating cases slope of the road constant and variable and their specific features, also the problem of disturbance rejection using graph techniques are given. Reference [4] shows that the structural analysis is a good tool for approximation of unknown physical quantity to control with a lack of precise model. Reference [3] gives how different levels of knowledge about faults can be incorporated in a structural fault isolability analysis; it is also shown the structural analysis which is a powerful tool for early determination of detectability and isolability possibilities of the diagnosis system.

Zine-eddine MEGUETTA, LAGIS UMR CNRS 8219, University of LILLE 1, Avenue Paul Langevin, Villeneuve d'Ascq, 59650, France.
zine-eddine.meguetta@ed.univ-lille1.fr

Alternatively, Fault Tolerant Control (*FTC*) is studied by many researchers [2],[5],[6]. In [2] presented *FTC* systems that can maintain an acceptable level of control even after the occurrence of faults. A more formal definition of a *FTC* system is given by [2] as "a control system where a fault is accommodated with or without performance degradation, but a signal fault does not develop into a fault on subsystem level". Current needs of developing autonomous vehicles and multitasking favored orientation control systems and the automotive industry is committed to offering manufacturers maintaining solutions for creating embedded reliable vehicles.

In the last decade, there has been significant research effort in the design of control systems [7]-[8]. The objective of designing a good control system is to determine the best control instrumentation scheme, that is to say, a set of sensors and actuators that allows the system to perform its mission despite the disturbance of one or several of its components. Designing a dependable control system is studied by many researchers [7]-[11]. Reference [14] has presented a methodology for designing a safe control system that tolerates a single critical fault. Reference [12] shows the design of control systems a method to optimize the instrumentation and uses financial cost and dependability as criteria. In [4] the robust design approach of the control system is presented using a structural analysis and study the Quality of Control *QoC* with the cost criterion thanks to the quantification of variables in graphical trees, it also aims to obtain the optimum instrumentation with lower cost for the system of the electric vehicle which provides good *QoC*, despite the influence of disturbance following the slope of the road and uncertainties sensors and the load mass of the vehicle.

The design problem is formalized as an optimization problem [5] that consists in searching for a subset of instruments that provides the best reliable system with the lowest cost.

The aim of designing a dependable control system is to determine the best control instrumentation scheme, that is to say, a set of sensors and actuators that, with the lowest cost, allows the system to perform its mission despite the failure of one or several of its components [5].

In reference [10], the problem of co-design of control systems through a Wireless Network (*WNCS*), integration of wireless network (*WN*) in the control loop influences the (*QoS*) system in terms the Quality of Service (*QoS*) of the

wireless network which presents an approach to co-design based on distributed Bayesian networks is presented. This approach allows decisions to ensure good *QoC* for the mobile vehicle, and when will face more stations.

This paper is an extension of the results presented in [1] and [4]; the application used is an electrical vehicle that moves on a road with a variable slope. The step of design concerns the ability to guarantee the performance and robustness of a system of the vehicle in design phase; it essentially depends on the control algorithm which consists in finding all paths of the control $u(t)$ based on a structural model that link the physical variables for electrical vehicle.

This paper is organized as follows: Section 2 provides concept of the design of a control system, section 3 describes algorithm of research control and sections 4 and 5 explain application the algorithm on the vehicle. Section 6 presents the result of optimization. Finally, concluding remarks are made in section 7.

II. CONCEPT OF THE DESIGN OF A CONTROL SYSTEM

A. Dependable control system and its instrumentation

The instrumentation of a control system is composed by sensors and actuators that allow performing specified missions. These missions are not limited to the control of the process with respect to some specifications but include also supervision activities. A controlled system can be modeled by a set of physical variables linked by a set of constraints, that is to say, a set of mathematical relations between these variables. The structural modeling is used to qualitatively represent the interaction between these variables without explicitly knowing the constraints, despite the few information of this model[11]. Classically, the design process of a control system is a closed-loop scheme. After finding a first solution of potential hardware architecture, the designer assesses its characteristics (costs, reliability) in order to determine its weak points and the possible improvements. A new potential hardware architecture is deduced and the cycle goes on until a satisfactory solution is found according to the different technical and economical criteria[11]. The design of hardware control systems is characterized by a lack of available and precise information. Indeed, since this activity takes place early in the design process, a lot of choices are not fixed, such as the maintenance policies, the final choice about the suppliers, device sizing. The precise and accurate dependable characteristics of the instruments are often unknown. Getting precise values would require a disproportional investment compared with the current objectives. In this article, the structural model offers an appropriate answer to model a system despite the lack of information.

III. DESIGNING A DEPENDABLE INSTRUMENTATION SYSTEM

A. Instrumentation system design

The reference [11] deals with the structural model used in order to obtain various ways for measuring required physical quantities for a given process. This research is used by the

presented design method for determining the best hardware architecture of an instrumentation system according to a dependability constraint and a cost criterion. The design process consists of inventorying all missions that the instrumentation system has to perform. A mission is here, a set of required physical variables needed by the control system in a particular context specified by an operating mode. For each required variable, a level of dependability is set thanks to a value that specifies the number of possible tolerated faults. From this, and thanks to the results of the structural analysis, the best set of sensors and actuators, that is to say with the lowest cost and that satisfies the required dependability level, can be determined from a combinatorial optimization algorithm.

B. Dependability evaluation

Since the proposed method concerns the first steps of designing, an accurate evaluation of dependability parameters such as reliability value or failure rate is not needed. In this way, the concept of (*FTL*) is proposed to evaluate the dependability of an instrumentation system or of the fulfillment of one of its mission, even in a degraded version. For a given hardware architecture and for a given mission, the *FTL* expresses the minimal number of fault components that prevent the mission to be performed. There is no combination of usable components that allows the mission to be performed. For example, the value 1 for the *FTL*, expresses that a single failure is sufficient to make unavailable a mission, while with the value 2, despite one fault component, the mission can be performed.

C. Function *FTL* properties

The function $FTL(q)$ is used to specify the dependability and to fix the number of failures that can induce the unavailability of the control system. This function has the following properties [12]:

If a quantity q_1 can be estimated from the two quantities q_2 and q_3 , its fault tolerant level is given by the following relation:

$$\begin{aligned} FTL(q_1) &= FTL(q_2 \wedge q_3) \\ &= \min(FTL(q_2), FTL(q_3)) \end{aligned} \quad (1)$$

This relation expresses that for a given variable, the number of faults that can induce its unavailability is the minimum of faults that induce the unavailability of one of the variables required for its evaluation.

If a quantity q_1 can be estimated from either the quantity q_2 or q_3 and if q_2 and q_3 are independent, its *FTL* is given by the following relation:

$$\begin{aligned} FTL(q_1) &= FTL(q_2 \vee q_3) \\ &= FTL(q_2) + FTL(q_3) \end{aligned} \quad (2)$$

This relation expresses that if there are several ways to estimate a quantity, its *FTL* is the sum of the levels of these ways. The assumption of independence between two required quantities expresses that there is no common quantity that allows the evaluation of these required quantities.

If a quantity q can be directly measured by sensors or actuators, its fault tolerant level is given by the following relation:

$$FTL(q) = N_{Sensor,actuator} \quad (3)$$

Where: $N_{Sensor,actuator}$ is the number of redundant sensors or actuators implemented in the system to measure q or to act on it. This relation expresses that for a quantity, its FTL is equal to the number of implemented redundant instruments. Thus, with a single sensor, a single failure entails the unavailability of the needed quantity, with two sensors, two failures are required.

D. Specifying dependability

In the proposed method, specifying this level consists in setting a limit number of tolerated failures for each of its missions. Since each mission is a set of required unknown quantities and a set of mode variable to check, it consists in setting this same limit for each of them. The function FTL is used to specify this limit that corresponds to the maximal number of failures that allows a considered quantity to be estimated. Thus, if a mission needs a quantity q and if its FTL is set to value n , the corresponding constraint is as follows:

$$FTL(mission) \geq n \Rightarrow FTL(q) \geq n \quad (4)$$

By specifying a required fault tolerant level for each mission, the designer indirectly fixes the dependability of the whole instrumentation system.

E. Building the optimization problem

The resulted optimization problem is composed by two parts. The first one is relative to the dependability constraints. It is a set of constraints on the number of sensors and actuators. This set is obtained from the dependability specification by transposing each constraint into a set of constraints on the number of sensors and actuators according to the result of the structural analysis and the properties of function FTL as explain previously.

The second part of the problem is relative to the criterion of cost. With the assumption that the cost of the instrumentation system is directly linked to the individual cost of each type of sensors and their number, the criterion to minimize is the following one:

$$Min(\sum_1^K C_{qi}) \quad (5)$$

Where K is the number of sensor or actuators implemented in the instrumentation, C_{qi} is the individual cost of this sensor or actuator.

F. Solving the optimization problem

Finally, for $i = 1 : K$ the optimization problem is the following one:

$$\begin{cases} Min(\sum_1^K C_{qi}) \\ FTL(q_1) \geq n_1 \\ \dots \\ FTL(q_i) \geq n_i \end{cases} \quad (6)$$

This problem corresponds to an Integer Linear programming (ILP) problem which is a standard optimization problem [13]. This problem can be exactly solved by current computation capacity Branch-and-Bound or Branch-and-Cut algorithms are enumeration techniques that are well suited to solve this problem and that provide the optimal solution. For larger systems, stochastic algorithms such as genetic algorithms can be used [6]. Although an optimal solution is not ensured, these algorithms provide satisfactory solutions from an industrial point of view.

IV. ALGORITHM OF RESEARCH

The following algorithm is used to search the different ways to evaluate an unknown variable.

It is based on the set theory and browses the incidence matrix built from a structural model:

Algorithm of research

% The algorithm control includes various steps that fit together as follows

- 1. Let S_c be a set of constraints:

$$S_c = \{S_{ci} \mid S_{ci} \in S_c\}$$

where: v_i is variable in the constraint S_{ci}

$$S_{ci} = \{v_i \mid v_i \in C_i\}$$

- 2. Let v_0 is the variable to search
- 3. If $S_c \neq \emptyset$

For $i = 1 : k$

If $v_i = v_0$

do

3.1 Choose S_{ci0} where:

$$S_{ci0} = \{v_0 \mid v_0 \in C_{i0}\}$$

% select the constraints that contain the factor v_0

3.2 Replace v_0 by its expression:

$$S_{c0} \leftarrow v_0$$

$$v_0 = \{v_i \mid v_i \in S_{c0}\}$$

3.3 Remove the constraint used in S_c :

$$S_{c0} \leftarrow S_c$$

- 4. Go to step 3

%Go to the other variable close(v_i) to the first variable(v_0)

Else

% final step

End of the algorithm

V. APPLICATION OF ALGORITHM ON THE VEHICLE

This section presents the use of this search algorithm control on a case study.

A. Description of the process

The considered process is an electrical vehicle, as shown in figure 1 of the reference [1]. The available instruments for this vehicle are: Electrical motor, Wheel encoder, GPS sensor, Inclinator. The considered variables are the following ones: a is the acceleration of the vehicle, v is the speed of the vehicle, x is the position of the vehicle, U is the control signal of the motor, and α is the angle of slope, I is the measure given by the inclinometer, C_v is the measure given by the encoder placed on the wheel.

Thanks to the following equations, the search algorithm control can be applied on the case study. In these equations, the period of sampling is known and constant δt .

$$a_t = g \sin(\alpha_t) - \frac{F_r}{m_t} + \frac{U_t}{m_t} \quad (7)$$

$$a_t = \frac{v(t + \delta t) - v(t)}{\delta t} \quad (8)$$

$$\alpha_t = \alpha_{t-\delta t} + \Delta \alpha_t \quad (9)$$

$$c_v^t = v_t + \varepsilon_v^t \quad (10)$$

$$I_t = \alpha_t + \varepsilon_I^t \quad (11)$$

$$m_t = M + \Delta m_t \quad (12)$$

$$m_{t-\delta t} = M + \Delta m_{t-\delta t} \quad (13)$$

$$a_{t-\delta t} = \frac{v(t) - v(t - \delta t)}{\delta t} \quad (14)$$

$$c_v^{t-\delta t} = v_t - \varepsilon_v^{t-\delta t} \quad (15)$$

$$a_{t-\delta t} = g \sin(\alpha_{t-\delta t}) - \frac{F_r}{m_{t-\delta t}} + \frac{U_{t-\delta t}}{m_{t-\delta t}} \quad (16)$$

In these equations, the following parameters are used: M is a fixed parameter used corresponding to the assumed mass of the vehicle, m_t is a real mass quantity of the vehicle, Δm_t is the variation of the mass due to the various transported loads, c_v^t is the measured speed provided by speed sensor, ε_v^t is the uncertainty of the measurement error while v_t is the real speed, I_t is the measured slope provided by inclinometer, ε_I^t is the uncertainty of the measurement error of inclinometer, α_t is the real slope.

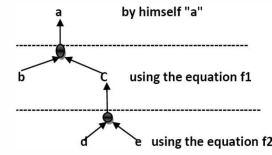


Fig. 1. Paths to evaluate the variable a

B. Result of the algorithm on the electrical vehicle

1) *General principle:* In this basic example, the objective is to find a based on equations (f_1 and f_2), given the following equations:

$$\begin{aligned} f_1 &= a \wedge b \wedge c \\ f_2 &= c \wedge d \vee e \end{aligned} \quad (17)$$

TABLE I
GENERAL PRINCIPAL

a				
x	b	c		
x	b	x	d	e

The solution: to find a is direct by himself a , or equation f_1 where $a = f(b, c)$, or by f_2 where $a = f(b, d, e)$ because $c = g(d, e)$, the corresponding graphical representation is in figure 1. Each node of the tree is associated to an algebraic formula (f_i) and can be read as arithmetic operator for the evaluation of a variable.

Applying search algorithm, the different paths to evaluate the control signal $u(t)$ are obtained and are shown in table 2. At each row of this table, a variable is replaced by other ones that allow its evaluation.

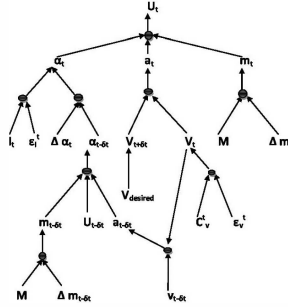
The set of constraints are provided by the structural analysis of electrical vehicle. The slope α_t appears in two constraints as following :

$$\begin{aligned} \alpha_t &= \alpha_{t-\delta t} + \Delta \alpha_t \\ I_t &= \alpha_t + \varepsilon_I^t \end{aligned} \quad (18)$$

Due to that, we used two way in the table, once we replaced by first constraint in equation 18 and other time by the second equation.

The graphical representation, each node of the tree code an algebraic formula f_i and can be read as arithmetic operator, it is labeled by variables (arrows) according to the algebraic equation associated. As the figure 2 shows, and this tree we can associate an incidence matrix in [1]. In the set of constraints based of the structural analysis of the system, the slope α_t appears in two constraints in the S_c . It is for this in the table that we divided the work of two sub-algorithms 1 and 2 because α_t appears in two equations is shown in table 2.

For this reason, we must search to rewrite the formulas, i.e. simplifying database (algebraic constraints), before using the search algorithm control.

[illegible]

$$\begin{cases} \begin{aligned} &Min(Ci_{Cv} + Ci_I + Ci_U) \\ &min(N_{\alpha_t}, N_{U_t}, N_{v_t}) \end{aligned} & \geq n_1 \\ \begin{aligned} &min(N_{U_t}, N_{\alpha_t}) + min(N_{x_t}, N_{t_{descent}}) + min(N_{v_t+\delta t}, N_{v_t}) \end{aligned} & \geq n_1 \end{cases} \quad (23)$$

The optimization problem for the case of the road slope α_t is too great as following:

$$\begin{cases} \begin{aligned} &Min(Ci_{Cv} + Ci_I + Ci_U) \\ &min(N_{\alpha_t}, N_{U_t}, N_{v_t}) \end{aligned} & \geq n_2 \\ \begin{aligned} &min(N_{U_t}, N_{\alpha_t}) + min(N_{x_t}, N_{t_{descent}}) + min(N_{v_t+\delta t}, N_{v_t}) \end{aligned} & \geq n_2 \end{cases} \quad (24)$$

The table 3 summarizes the values of fault tolerance levels for different instruments Cv, I, u . N_{Cv} is fault tolerance level for speed sensor, N_I for inclinometer, N_u for the motor. The chronometer component Ch , it is not important in the set of instruments in electrical vehicle, so this component has less need for fault tolerance $N_{ch} = 0$ and the *GPS* has to be tolerant to one failure $N_{gps} = 1$. We chose arbitrarily the values of the costs associated to each sensor and actuator, Ci_u for the cost motor, Ci_{Cv} cost for the speed sensor, Ci_I for the cost inclinometer.

TABLE III
THE NUMERICAL VALUES FOR THE PARAMETERS OF THE INSTRUMENTATION

number of instrumentation	1	2	3	4	5
$FTL(v_{t+\delta t})$	2	3	1	1	2
$FTL(a_t)$	4	6	4	3	5
N_{Cv}	2	3	3	2	3
N_I	2	3	2	1	2
N_u	2	4	1	1	3
Ci_{Cv}	3	4	5	2	4
Ci_I	2	3	4	3	2
Ci_u	10	11	12	11	11

The result of the optimization problem has a global cost of 16 with the following architecture for the case of the road slope α_t is too small : A cost of 11 for a motor, a cost of 3 for inclinometer, a cost of 2 for speed sensor, The control of the speed $FTL(v_{t+\delta t})$ is tolerant to one failure, while the control of the acceleration $FTL(a_t)$ is tolerant to three failures.

The result of the optimization problem has a global cost of 15 with the following architecture for the case of the road slope α_t is too great as following: A cost of 10 for a motor, a cost of 3 for inclinometer, a cost of 2 for speed sensor, The control of the speed $FTL(v_{t+\delta t})$ is tolerant to two failures, while the control of the acceleration $FTL(a_t)$ is tolerant to four failures.

VII. CONCLUSION

In this paper, a control algorithm has been proposed to find the control $u(t)$, using structural model

describing qualitatively different relations linking the physical quantities for an electrical vehicle.

This paper presents robust design approach of the control system. Indeed, it requires a reduced amount of data, that is to say, an incidence matrix built using structural modeling, the cost of the instruments implemented like sensors and actuators and a set of fault tolerant level constraints. After optimizing, the method gives the instruments (sensors, actuators) that offers a given fault tolerance level for the variables to control, with the lowest cost. Consequently, the capacity of fault tolerance is presented to determine instrumentation architecture that can perform their mission despite one or several failures.

The further works concern the simplification of the set of constraints (algebraic constraints) using algorithm of [9] and the extension for the multicontrol signal systems.

REFERENCES

- [1] Z-E. Megatta and B. Conrard, M. Bayart, *Instrumentation for electrical vehicle model on road slope using structural analysis*, 20th Mediterranean conference on control and automation(MED), Barcelona, Spain, july 3-6, 2012.
- [2] M.Blanke, M.Kinnaert, J.Lunze, and M.Staroswiecki. *Diagnosis and Fault tolerant* (2nd ed.), Springer-Verlag,. Berlin Heidelberg, 2006
- [3] D.Dustegor, E.Frisk, V.Cocquempot, M.Krysander, M.Staroswiecki. *Structural Analysis of Fault Isolability in the DAMADICS Benchmark*, In:Control Engineering Practice. Vol 14, issue 6, pp. 597-608, 2006.
- [4] Z-E. Meguetta and B. Conrard, M. Bayart, *Conception de l'instrumentation d'un véhicule grâce à une modélisation structurale sous un critère d'optimisation de la qualité de commande et du coût*, QUALITA'2013, 10ème Congrès International Pluridisciplinaire Qualité et Sécurité de Fonctionnement, Compiègne, France, 19-22 mars, 2013.
- [5] B.Conrard and M.Bayart. *Design of safe control system thanks to a combinatorial optimization*, proceeding of SafeProcess'03, Washington D.C, 2003.
- [6] C.Roucairol, *Solving hard combinatorial optimization problems*, in: Proceeding of CESA'98, pp. 66-72, 1998.
- [7] B. Conrard and M. Bayart, *Design of safe control system thanks to a combinatorial optimization*, proceeding of SafeProcess'03. Washington D.C, 2003.
- [8] B. Conrard and M. Bayart, *Design and optimization of dependable measurement systems*, 12th IMEKO TC1 & TC7 joint symposium on Man science & measurement. Annecy, France, 2008.
- [9] M.Nikolskaia, *Decision diagrams and applications to reliability analysis*. Thèse de doctorat de l'université Bordeaux 1(LABRI), page 167, France, janvier 2000.
- [10] A. Mechraoui and J-M. Thiriet, *Co-conception de robots mobiles commandés en réseaux sans fil*, 9 ème congrès international pluridisciplinaire en qualité et sureté de fonctionnement, France: Angers, 2011.
- [11] B. Conrard, V. Cocquempot and S. Mili, *Fault Tolerant System Design in Multiple Operating Modes using a Structural Model*, Confrence ESREL European Safety & Reliability Conference. Troyes, France, 18-22 September 2011.
- [12] B. Conrard, V. Cocquempot and M. Bayart, *Sensor and actuator placement with dependability constraints and a cost criterion*, IFAC Safeprocess . Barcelona, Spain, June 30 - July 3, 2009.
- [13] J.Mitchell. *Branch-and-cut algorithms for combinatorial optimization problems*. Oxford University Press, New York, 2002.
- [14] M.Blanke, J-S. Thomsen. *Electrical steering of vehicles - fault-tolerant analysis and design* Original Research, Article Microelectronics Reliability, Volume 46, Issues 9–11, 2006, Pages 1421-1432.