IFAC MCPL 2007
The 4th International Federation of Automatic Control Conference on Management and Control of Production and Logistics
September 27-30, Sibiu - Romania

DIAGNOSIS FOR CONTROL SYSTEM RECONFIGURATION

Eric Deschamps and Eric Zamaï

Laboratoire des Sciences pour la Conception, l'Optimisation et la Production (G-SCOP)
INPGrenoble, UJF, CNRS,
46 avenue Félix Viallet, 38031 Grenoble Cedex, France
eric.deschamps@inpg.fr, eric.zamai@inpg.fr

Abstract: The objective of the Automated Manufacturing System reconfiguration is to react to failures such as breakdowns of actuators or sensors. Following such events, the control laws run by the control system are often blocked and thus become inadequate. Thus, it is therefore necessary to reconfigure the control system. This reconfiguration process is inevitably based on the capacities still offered by the operating part to achieve the production objectives. In this context, the paper proposes an on-line function diagnosis able to provide the required information on the capacities of the operating part. It is based on a model of the operating part in normal operation, and generic rules to obtain the possible origins and consequences of a detected symptom of failure.

Keywords: model-based diagnosis, failure and recovery, automation, real-time, manufacturing systems.

1. INTRODUCTION

Automatic Manufacturing Systems (AMS) are composed of two different parts: the controlled system and the control system (as shown in Fig. 1). The controlled system is composed of actuators which act on the product flow. It is also composed of sensors to control and monitor the actuators and the product flow although this observability on these components is only partial. To manage the complexity of such controlled systems, a hierarchical and modular control is often proposed (John, 1989). Each elementary part of the controlled system is controlled by its local control module, and these two elements are called Functional Chain (FC) as shown in Fig. 1. Thus, the purpose of the coordination level is to manage a set of FCs by using services offered by these FCs. Throughout these levels, a high level request is broken down into a sequence of elementary requests until level 1 is reached. At a considered level i, when a request is executed before the due date, sent with the request, an execution report is generated and sent to level i+1. However, at level 1, in the event of breakdown of actuators or sensors, the due date cannot always be respected and a faulty execution report is sent. On reception of such a report, level 2 tries to confine the failure before the due date of the current request to avoid sending a faulty execution report to level 2.

To ensure that the operation takes place as defined above, each module must integrate supervision, monitoring and control (SM&C) functions such as detection, diagnosis, prognosis and decision (Combacau, et al., 1990). Thus the operation of the control system is based first on collaboration between these functions and second on the exploitation of models. Here, the paper focuses on the function diagnosis. The literature proposes two kinds of approaches: first, model-free methods which are based on empirical knowledge of the controlled system as presented in (Bohez, et al. 1997); and second, model model-based methods as presented in (Ressencourt et al. 2006). The paper deals with a method for an on-line diagnosis using a model of the operating part; it is based on other classical approaches of diagnosis with an added original approach which is presented in the next sections.

This paper is organized as follows. First, section 2 focuses on the possible objectives of diagnosis. Based on the objective on which the paper focuses, section 3 presents the principle of the diagnosis. Section 4 presents an academic example, and the corresponding model is presented in section 5. Finally, section 6 details the diagnostic approach.

2. OBJECTIVE OF THE DIAGNOSIS

In the reactive hierarchical control, the diagnosis has two main objectives: first to identify the component responsible for the detected symptom with the aim of repairing it as fast as possible. The second objective is to provide information on the availability of services, to use this to confine the failure and execute the current request before the due date. The proposed diagnosis in this paper gives a solution for attaining the second objective at the coordination level. Thus, it provides information on the availability of FC services. At the coordination level, to react to a hypothetical faulty execution report sent by a FC, the control system must be reconfigured. This reconfiguration consists in designing automatically a

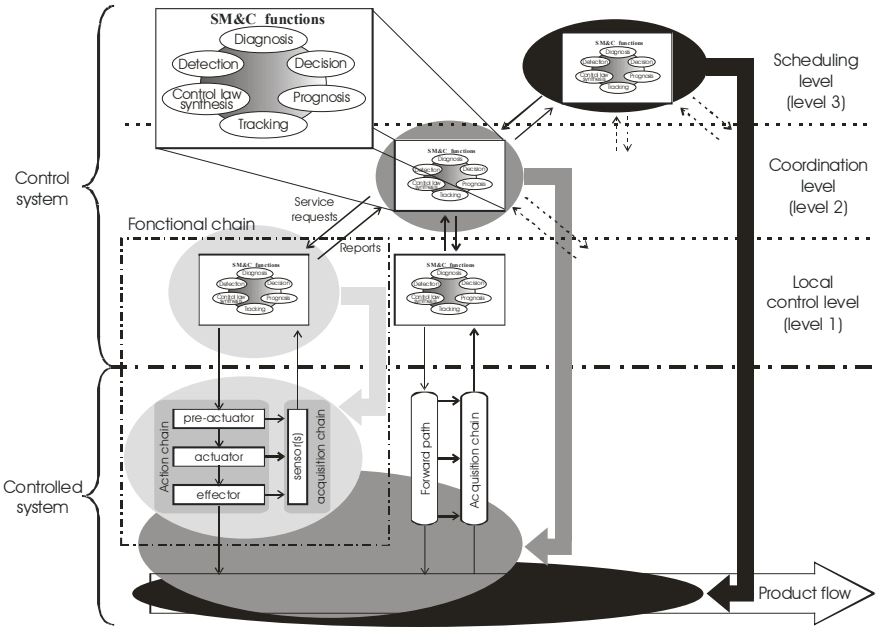

Fig. 1. Diagram of an AMS

new suitable control law (set of requests to FCs). However, to take such a decision, it is necessary to have a realistic view of the services still offered by FCs even if this view is pessimistic considering the time to react, fixed by the due date. Thus several questions must be asked. What model(s) must be used by such a function diagnosis? The objective being to reconfigure, how to link the diagnosis to the reconfiguration? And finally, how can this pessimistic view be expressed?

3. GENERAL SITUATION

In discrete event systems, methods for diagnosis are classically based on tools such as state machines (Sampath, et al., 1998), or Petri nets (Genc, et al., 2003). From detection and the partial observation of the controlled system, these methods try to identify in which state the controlled system is and what the origin of the faulty execution report is. In this kind of approach, it is generally proposed to model all the possible failures. However, due to the resulting complexity at the coordination level, it would be very difficult to predict all the failures. So, in the event of unpredicted failure, the diagnosis cannot provide a result. At this level of control, to guarantee the reactivity of the control system, the diagnosis must not be based only on a failure model.

After a failure occurrence, a method is also proposed in (de Jonge et al., 2006) to make a diagnosis based on two observations of the system which is the failed action of a plan. The method is based on the theory of diagnosis from first principles (Reiter, 1987). In fact, plan execution can be diagnosed by viewing action instances of a plan as components of a system and by viewing the input and output objects of an action as input and outputs of a component. This makes it possible to apply classical model-based diagnosis to plan execution. This idea can be exploited in the context of our work by viewing an executed service as an action. However, this approach must be extended. First, in (de Jonge et al., 2006), actions are considered as independent. This hypothesis cannot be used; several services can be carried out by the same functional chain, and so are not independent. Second, the inputs of components (corresponding to pre-conditions of action or pre-conditions, conditions, pre-constraints and constraints of services as described bellow) can have an impact on the behavior of the services but also on the operation of the functional chain. The last problem is the size of the model. In fact, the diagnosis from first principles considers a finite set of components or the plan diagnosis a finite set of action. However, due to the cyclical operation of the control system at the coordination level, the number of the past executed services is not finite. It is therefore necessary to reduce the model used by the diagnosis under hypotheses which will be explained next.

In this paper, the model for diagnosis is based on the formal description of services behavior proposed in (Henry, et al., 2004). This formal description can be used to design control laws but also to provide information on the behavior of services offered by FCs for diagnosis as explained in section 6. Thus, to reconfigure the control system after the diagnostic, it is necessary to express the diagnostic result onto the formal description proposed in (Henry, et al., 2004). Information on services is not sufficient for reconfiguring the control system. In fact, information on the state of the controlled system is also needed. More precisely, the diagnostic method provides on a rating scale a qualification of the availability of services offered by FCs. In this way the vocabulary from the safety field of research will be used. A service will be qualified as:

• Correct: observed correct (direct/indirect) in its last use.