Model-based situation assessment of dynamic physical systems

P. Baroni, G. Guida, G. Lamperti & M. Zanella
Dipartimento di Elettronica per l'Automazione - Via Branze, 38
Università degli Studi di Brescia, I-25123 Brescia, Italy
EMail: [baroni | guida | lamperti | zanella]@bsing.ing.unibs.it

Abstract

This paper focuses on the scheduled situation assessment of dynamic physical systems to which testing is not applied. First, a set of modeling concepts as to physical system operation is introduced: such concepts stress the importance of the role played by system parameters, which are a number of physical, chemical, dimensional, structural, spatial properties of the physical system at hand. So, situation assessment is defined as the task of determining the current system parameter values of a given physical system. Since parameters are evolving over time owing to wear and tear phenomena, a set of assumptions as to the dynamic evolution of the values of system parameter is discussed. Then, a logical model for the accomplishment of the task of situation assessment is proposed and its cognitive plausibility is proven by means of a case study.

1 Introduction

Situation Assessment (SA) is a quite important task in order to improve the availability, reliability and safety of physical systems, on one hand, and to reduce their maintenance costs, on the other. Improving the availability is relevant especially for systems which are vital items of equipment in industrial plants. Improving the reliability is particularly significant for physical systems whose operation has to fulfill requirements on quality standards. Improving safety is the prime goal in the management of physical systems whose misbehaviors may have dangerous consequences for people. Reducing maintenance costs is a goal in the management of every physical system. To achieve all these goals, SA is more and more often aimed at detecting the internal problems of a given physical system possibly far

before they may have undesired consequences. Once the problems have been isolated, proper maintenance actions are planned either automatically or by the operator. The task of SA is usually carried out by engineering staff, and sometimes, for particular systems, even by special gurus. Many successful attempts to provide an automatic support for SA are registered in the literature. Nowadays, automatic SA is usually a subtask of condition monitoring, which includes a regular and consistent data collection and the interpretation or analysis of these data. This approach, however, assumes that the physical system is available to be monitored, while monitoring is not possible for all physical systems during everyday operation. The current practice for physical systems that cannot be monitored neither continuously nor periodically is scheduled SA. Such SA is the focus of this paper, which proposes a new approach for carrying out the task on dynamic physical systems. Unlike existing approaches to scheduled SA, which consist in the knowledge-based interpretation or the numeric analysis of measures, without considering any further information, our approach suggests to exploit also the record of the past history of the system whose situation has to be assessed.

The paper is organized as follows: Section 2 presents a background for the task of SA; Section 3 describes a taxonomy of modeling concepts about the physical systems taken into account by SA; Section 4 explores the laws governing the wear and tear phenomena affecting physical systems and proposes a logical model for the accomplishment of the task of SA; Section 5 presents a case study; finally, Section 6 briefly draws some conclusions.

2 Background

Situated reasoning [1][2] is an advanced approach to the SA of dynamic physical systems. State-of-the-art software products [3] for SA are on-line knowledge-based systems, endowed with a hierarchical functional architecture [4], that make use of heterogeneous knowledge representations at the different levels of the hierarchy. The lowest hierarchical level exhibits a reactive behavior, that is it takes into account the current situation of the physical system under control and makes decisions about reactions within a guaranteed response time, without relating such situation to past ones. This is quite proper for finding out pre-alarm or alarm situations and reacting to them. Upper levels, instead, perform temporal reasoning in order to relate the current situation to previous ones: their goal is to perform a diagnosis, that is to trace back a set of symptoms that have manifested during system operation to the fault/s that caused them. This goal may be achieved by the cooperation of multiple diagnostic tools, chiefly by accomplishing a model-based diagnosis [5]. By definition [6], symptoms are discrepancies between the actual and the expected behavior of a given physical system of interest. In dynamic systems, symptoms are not only static deviations from the nominal behavior, as in static systems, but also incorrect dynamic evolutions. The output of the task of diagnosis is a set of faults, that is a set of

hypotheses of abnormal behavior by one or more system components. Based on the number and on the nature of the variables considered in order to detect symptoms, diagnosis can isolate either faults at advanced stages or even minor problems.

The approach to SA described above is based on condition monitoring, that is on the continuous or periodic measurement and interpretation of data to indicate the condition of the physical system at hand. The kinds of information which are relevant to indicate the condition depend on the considered physical system and may be quite different in nature. So, for instance, there are physical systems for which it is important to make an interpretation of the results of visual inspections, and mechanical systems for which the values of measurements as to the vibrations [7] or the high frequency acoustic emissions are quite significant. However, performance monitoring, that is the acquisition and interpretation of the values of a number of selected output variables while the physical system is working, is an approach of general validity to condition monitoring.

Condition monitoring is carried out in order to determine the need for maintenance actions. So, there are situated reasoning systems where condition monitoring and condition based maintenance are coupled each other in a waterfall fashion. Condition based maintenance proposes preventive actions only when a condition (belonging to a given set) occurs, that is only as and when they are needed.

However, not all physical systems for which SA is needed can be monitored. In fact, monitoring is ineffective when measures are scarcely accurate. The results of monitoring, which is carried out with the physical system in operation, are less precise than the results of laboratory tests. Unfortunately, sometimes the imprecision of such data, which depends on the quality of the acquisition equipment, may make them useless. In these cases, either an enhanced data acquisition equipment is adopted or, if the former choice is too expensive or unfeasible, monitoring is abandoned. Besides, condition monitoring is unpractical when taking measures heavily interferes with system operation. Still more, there are cases in which condition monitoring is useless and, therefore, is not performed: this happens when the critical conditions that foretell catastrophic events can be recognized only with too short advance.

So, in current practice, in all the cases when monitoring is unpractical or disadvantageous, the physical system is subdued to scheduled preventive maintenance and to scheduled SA. Scheduled preventive maintenance is carried out every time a fixed time interval has elapsed or a certain (quantified) amount of work has been accomplished by the considered system. This means that routine maintenance actions are conducted according to predefined plans, independently of the situation of the system. Performing a scheduled SA means checking the system situation according to a predefined timetable. Each scheduled SA session takes into account a number of results of measurements performed on the physical system. Measures may be taken passively, that is while the physical system is operating and without modifying the course of system operation, and/or actively by testing the

system, that is by applying to the system one or more input patterns and measuring the corresponding output configurations. There are, indeed, physical systems for which a preliminary SA is first carried out without performing any testing. This typically happens when testing is very expensive, since, for instance, it needs the system to be put out of service or requires a particular equipment which is not available in the working site. Only in case the preliminary SA has estimated a very critical situation of the considered physical system, a cost/risk analysis is performed in order to decide whether to carry out possible testing actions or not, so that to confirm or refute the results. Once the SA has been completed, further maintenance actions may possibly be accomplished, based on the actual, just checked, condition of the system.

The focus of this paper is on the scheduled SA of dynamic physical systems, in particular on preliminary SA, that is on SA which is carried out without performing any testing action. The authors have realized that such SA could take into account further information besides the current "passive" measures of the considered system. In particular, such SA could take advantage of information about what has happened to the system in the interval from the time when the latest SA was performed up to now as well as of the results of possible off-line measurements carried out in the same interval. This paper proposes a logical model for the accomplishment of the task according to this direction.

3 Concepts and assumptions

SA is intended to estimate the current situation of a physical system of interest. But what is indeed the "situation" of a physical system ? Our attempt to formally define the meaning of "situation" and then to say how the task of SA can be performed is based on several concepts as to dynamic physical systems and on some remarks about the concept of fault, as it is briefly summarized here below. Such concepts and remarks are abstract, in the sense that they are independent of any implementation concern, so that development problems cannot be mistaken for modeling issues.

3.1 Context graph

In our modeling approach, a physical system is described by the so-called *context graph*, since, in the authors' opinion, this concept is easy to be understood and at the same time very useful for giving an insight into physical systems. The nodes of this graph are called operating modes, the arcs are called operating transitions. An *operating mode* is a way of functioning of the physical system, owing to one physical process. We may assimilate the physical system, when it is working within an operating mode, to a virtual machine devoted to the implementation of a single physical process. The same physical system, however, may support, in different times, distinct processes, that is the same physical system may give place to several virtual machines. An *operating transition* is a way in which the physical system is

allowed to move from one operating mode to another. From a physical point of view, an operating transition is the transient of the physical process associated to the target operating mode. Then the number of physical processes supported by a physical system is equal to the number of operating modes in its context graph.

A *context graph process* is a physical process supported by the physical system: such process is described in the context graph by an operating mode and by all its entering operating transitions.

A *context* is either an operating mode or an operating transition. Each context belongs to one context graph process.

3.2 System variables

Given a physical process, three finite sets of variables are associated to it: the set *I* of *input variables*, the set *O* of *output variables* and the set *S* of *state variables*. Therefore, since each context graph process represents a distinct physical process, a distinct triple (*I*,*O*,*S*) is associated to it. The set of input variables is disjoint from those of output and state variables. Input variables include all those variables that drive, regulate, and affect system operation from the outside, while output variables are variables whose values are produced at any moment by the operation of the physical system. State variables are the variables whose values at a given instant t_0 are absolutely necessary, together with the values of input variables over the interval from t_0 to t, in order to determine the values of output variables at any instant t later than t_0. From this definition of state variables, it descends that

a) the values of output variables at any given instant t, indicated by $O(t)$, depend on the values of input variables and state variables at that instant, indicated by $I(t)$ and $S(t)$ respectively, that is
$O(t) = f(S(t),I(t))$; *(1)*

b) the values of state variables at any given instant t depend on the values of state variables at a generic previous instant t_0 and on the values of input variables over the interval from t_0 to t, indicated by $I[t_0,t]$, that is
$S(t) = g(S(t_0),I[t_0,t])$. *(2)*

Note that relations *(1)* e *(2)* are expressed in an analytic way just for the sake of clarity while explaining our view of dynamic physical systems: the adoption of the analytic language does not mean at all that this is the formalism we propose for describing the operation of physical systems in order to carry out the task of SA.

Each physical process supported by the physical system is characterized by its own couple of relations *(1)* and *(2)* and, vice versa, each distinct couple *(relation (1), relation (2))* corresponds to only one physical process. So, there is a distinct couple of relations (1) and (2) for each context graph process. Each context inherits the (*I*,*O*,*S*) triple and the *(relation (1), relation (2))* couple of the context graph process it belongs to.

The union of the sets of input variables of all the context graph processes in the context graph is the set of all the input variables of the physical system, indicated by $\Im$. The union of the sets of output variables of all the context graph processes in the context graph is the set of all the output variables of the physical system, indicated by Ω. The union of the sets of state variables of all the context graph processes in the context graph is the set of all the possible state variables of the physical system, indicated by Σ.

3.3 Nominal behavior

The physical system was designed so that to behave in a desired way within each context. Given the (*I,O,S*) triple associated to a context, by *behavioral space* of that context we mean the $I' S \times O$ space, that is the $ni+ns+no$ dimension space defined by the *ni* distinct input variables in *I*, the *ns* distinct state variables in *S*, and the *no* distinct output variables in *O*. By *nominal behavior* of the physical system within a context we mean the behavior the system has to exhibit when operating in that context according to its design specifications. Such behavior is expressed by:

- a collection of points in the behavioral space of that context, called *nominal working points*;
- a collection of sequences of points in the $I' S$ space of that context, called *temporal paths*; the points of each sequence are ordered on a temporal basis; each sequence represents a way of navigating within the domain of the nominal behavior over time.

From a formal point of view, the way the system behaves in a given context is governed by the relations *(1)* and *(2)* of that context. Then the nominal working points have formally to belong to the *f* function of the considered context, while temporal paths have to comply with relation *(2)*. Owing to physical and teleological constraints, usually the nominal behavior is not defined on the whole $I' S$ space, but only on a domain which is included in that space. By projecting the domain of the nominal behavior of a given context on the *S* space, we obtain the domain of state variables. Each context is characterized by its own domain of state variables. The domain of state variables of a context graph process is given by the union of the domains of state variables of all the contexts belonging to that context graph process. The domain of state variables of a context graph process is disjoint from the domains of state variables of all other context graph processes.

The $\Im \times \Sigma \times \Omega$ space is called *system behavioral space*. The domain of the nominal behavior of the whole physical system is the union of the domains of the nominal behavior of all the contexts in the context graph of the physical system and can be represented in the $\Im \times \Sigma$ space.

3.4 System parameters

From a realistic perspective, to each point in the domain of the nominal behavior of a given physical system within a context, that is to each valid couple (input variable configuration, state variable configuration), does not correspond a single valid output variable configuration, but many possible configurations which are all acceptable. Therefore, in order to guarantee the nominal behavior of the physical system within a given context, each one of the parameters in the physical law synthetically expressed above by the equation *(1)* of that context is not bound to have a fixed value, instead its value may usually range over an interval. Since *O(t)* depends on *S(t)* and *S(t)* is given by function *g*, the same consideration is valid also for the parameters of function *g*. The fact that parameters may have interval values primarily accounts for the genericity related to the sample artifacts of a given series.

Each *(relation (1), relation (2))* couple, describing a physical process, univocally corresponds to a context graph process. Then, a finite set *P* of *system parameters* is associated to each context graph process: *P* is the union of P_f and P_g, where P_f is the set of parameters of relation *(1)* and P_g is the set of parameters of relation *(2)*. System parameters represent physical, chemical, structural, dimensional and spatial properties affecting system operation from inside. The set of system parameters may differ from one context graph process to another since, for instance, a parameter corresponds to a system component which is involved in the former process but not in the latter. The set $\boldsymbol{P}$ of all the parameters of the physical system is given by the union of the sets of system parameters of all the context graph processes represented in the context graph.

Each context inherits the *P* set of parameters of the context graph process it belongs to. So, given the (*I*,*O*,*S*) triple and the *P* set associated to a context of a dynamic physical system of interest, the domain of the nominal behavior of the physical system within that context is indeed included in the $I \times S \times P$ space, that is the $ni+ns+np$ dimension space defined by the *ni* distinct input variables in *I*, the *ns* distinct state variables in *S*, and the *np* distinct system parameters in *P*. To each point in this subspace, that is to each valid triple (input variable configuration, state variable configuration, system parameter configuration), corresponds in a deterministic way a single valid output variable configuration.

By projecting the domain of the nominal behavior of the physical system within a given context on the *P* space defined by the *np* parameters belonging to the set of system parameters of that context, we obtain the domain of system parameters within that context. So each context has its own domain of system parameters, placed in the *P* space defined by its own set of system parameters. The domain of the system parameters of a given context can be "transported" in the $\boldsymbol{P}$ space defined by the system parameters of the whole physical system, thus yielding the so called $\boldsymbol{P}$*_domain* of the considered context, by assuming that the domain of each *p* parameter which belongs to the difference set ($\boldsymbol{P}$*-P)* is the whole *p* axis. Based on

this assumption, the domain of system parameters of the whole context graph, that is the domain of system parameters of the physical system, is the intersection of the $\boldsymbol{P}$ _domains of system parameters of all the contexts in the graph.

3.5 Actual behavior

The behavior actually exhibited by the physical system is called *actual behavior*. At every moment, a physical system is working in a specific point of the system behavioral space, called *actual working point*.

At a given instant, the actual behavior is *normal* if *i)* the actual working point is a nominal working point, and *ii)* the past evolution of the state variable configurations followed a temporal path; otherwise, the actual behavior is *abnormal*. The causes for an abnormal behavior may be twofold: external and/or internal. External causes consist in the application of incorrect input configurations: at a given instant, assuming that the current configuration of state variables belongs to the projection of the domain of the nominal behavior of the whole context graph on the Σ space, the input configuration is incorrect if the couple (input configuration, state variable configuration) does not belong to any temporal path. External causes of misbehavior are beyond the scope of this paper.

Internal causes are called *faults*: they are incorrect parameter configurations, that is configurations of system parameters which are outside the parameter domain of the context graph. We say that the physical system is *healthy* if the values of its parameters are within the parameter domain, is *faulty* otherwise.

3.6 Assumptions on parameters

At the beginning of its active life, every artifact is usually certified to have system parameters whose configuration of values is within the parameter domain. In this condition the physical system is healthy and, if no incorrect input configuration is applied to it, exhibits an actual behavior that complies with the nominal behavior. However, in the length of time it may happen that the behavior of the physical system does not comply with the nominal behavior any more. This can be explained only by assuming that the configuration of the values of system parameters has changed and has moved outside the parameter domain.

In previous diagnostic approaches in the literature, system parameters are considered as having fixed values in each individual system. Instead, in our approach, system parameters have not constant values, on the contrary their values are assumed to be progressively changing over time, as it happens in real life owing to wear and tear phenomena. Since parameters are not constant, they have to explicitly appear in the model of the physical system. So, the relations *(1)* and *(2)* of every given context graph process have to be corrected as follows:

$O(t) = f'(S(t),P(t),I(t)),$ *(1')*

$S(t) = g'(S(t_0),P[t_0,t],I[t_0,t]),$ *(2')*

where *P(t)* represents the configuration of system parameters at instant *t* and $P[t_0,t]$ represents the configurations of system parameters over the interval from t_0 to *t*.

We have assumed that the values of system parameters are progressively changing over time. Also the values of state variables are changing over time but relations *(1')* and *(2')* make it clear that state variables and system parameters play different roles. In fact, the evolution over time of state variables is ruled by the underlying evolution of physical processes, it is desired and instrumental in obtaining the expected behavior of the physical system. Besides, such evolution can be properly driven by means of input variable values. The evolution over time of the values of system parameters, instead, is ruled by wear and tear phenomena and is an undesired, and - to some extent - ungovernable, side effect. Such evolution can only be changed from time to time by means of maintenance or replacing actions. Another difference between state variables and parameters is that parameters represent, either directly or indirectly, properties of the physical system and of its components, while state variables are properties of the physical processes supported by the physical system.

3.7 Faults and symptoms

A physical system is faulty if its configuration of system parameters is outside the parameter domain of its context graph. This implies that there exists at least one context whose current configuration of parameters is outside its own parameter domain. Limiting our attention to relation *(1')* of this context, if one or more parameters of this relation are outside the parameter domain of the context itself, there exists at least one couple (input variable configuration, state variable configuration) such that the input variable configuration, if it is applied when the physical system is working in the state defined by that state variable configuration, produces an abnormal behavior. This means, however, that a physical system may be faulty even if no symptom has so far manifested during system operation. In fact, it may be that the physical system has so far been working in contexts belonging to context graph processes where no symptoms can manifest since, for instance, the physical parameters having incorrect values correspond to system components that do not take part in the operation within such processes. Or, it may be that, even if the physical system has so far been working in contexts belonging to context graph processes where some symptoms could potentially come out, no couple (input variable configuration, state variable configuration) which produces incorrect outputs has been encountered. Let us consider a context and a state variable configuration that belongs to the projection of the domain of the nominal behavior within that context on the *S* space. A domain of input variables corresponds to that state variable configuration: such domain includes all the input variable configurations, belonging to the projection of the nominal behavior within the considered context on the *I* space, that can be applied to the system when that is the current state variable

configuration. Such domain of input variables can be partitioned in two subdomains in relation to a given parameter configuration which is incorrect for the considered context: the subdomain of non-symptomatic input configurations and the subdomain of symptomatic input configurations. *Non-symptomatic input configurations* are particular combinations of input variables that result in a "compensation" of the anomaly of system parameters, thereby preventing the operation of the physical system from producing any symptoms. *Symptomatic input configurations*, instead, are all the other configurations of input variables in the considered input domain: they do not mask the anomaly of system parameters and therefore give rise to symptoms. This is quite analogous to what happens in software systems, where run time errors may either manifest themselves or not, depending on the values of input data.

Analogous considerations are valid also for relation *(2')*. So, knowing the current configuration of the system parameters of a physical system means knowing all its faults, have they manifested themselves as symptoms during system operation or not.

4 Situation Assessment: definition and logical model

Previous sections evidenced the importance of the role played by the system parameters of a dynamic physical system and how the current configuration of system parameters is actually a measure of the health of the physical system. We call *wear state* of a physical system at a given instant the configuration of system parameters at that instant and define SA as the task of determining the current wear state of a given physical system.

So far, we have generically stated that the evolution of the values of system parameters over time is ruled by deterioration phenomena and its course can be changed by means of maintenance or replacing interventions. This, however, is not enough for setting up a theory of SA. Then, in the next sections further concepts and assumptions on this topic are introduced.

4.1 Deterioration and maintenance

In the rationale of this paper, deteriorating a physical system means changing the values of its parameters. Also maintaining a physical system means changing the values of its parameters. Intuitively, however, deterioration phenomena tend to bring the configuration of system parameters outside the parameter domain of the physical system, while maintenance actions tend to bring it inside the parameter domain.

We call *maintenance interventions* of a given physical system all the fixing or replacing interventions that can be carried out on the system. The values of the changes a maintenance intervention produces on system parameters depends on its kind and on its "intensity".

Deterioration phenomena are, of course, system dependent. The categories of causes of deterioration, however, are common to most physical systems: they are the

length of time, the operation of the physical system, the accidents occurred to the system, and the invasive diagnostic actions carried out on the system.

As time goes by, it progressively modifies the values of the parameters of a physical system. For example, the system may be made of chemical substances which are heavily affected by the length of time.

As to the operation of the physical system, it may comply with the nominal behavior or not. If the behavior of the physical system complies with the nominal behavior, it may fulfill its *technical constraints* or not. In fact, there exists a specific set of technical constraints for each context and one for the whole context graph. Such constraints state how to drive the operation of the physical system on a temporal basis so that not to overcome its constructive technical limits. For instance, a constraint regarding a single context may state that the physical system can work uninterruptedly in that context only for a limited time interval, lest the system may be damaged. It is intuitive that working in different nominal points and either fulfilling or not technical requirements is likely to produce different changes of the values of system parameters.

By definition, the *accidents* of a physical system are all the fortuitous events which may damage the system, while the *diagnostic activities* of a physical system are all the invasive activities which can be carried out on the system for diagnostic purposes. The changes of the values of system parameters produced by each single accident or diagnostic activity depends on its type and on its "gravity".

4.2 External history, state history, and internal history

The concept of external history is aimed at gathering all the exogenous actions causing changes of the values of system parameters, as they have been applied to the system over a given interval.

The record of: 1) input variable values, 2) accidents, 3) diagnostic activities, and 4) maintenance interventions, in a time interval is called *external history* of the system in the given interval. The values of input variables applied to the system determine system operation. The operation of the system, that is its working points, cannot be recorded since we are dealing with physical systems that cannot be monitored.

In the course of the life of the system, the values of state variables and system parameters are incessantly changing. The progression of state variable configurations and system parameter configurations over a given interval are called *state history* and *internal history* of the system in the considered interval, respectively.

4.3 The dynamic evolution of parameters

A basic assumption of our modeling approach to physical systems it that, given a physical system and a generic time interval, the internal history of the system in this

interval depends on the initial wear state along with both the state history and the external history of the system throughout the interval. More formally:

$P(t) = h(P(t_0),S[t_0,t],H[t_0,t]),$ *(3)*

where $H[t_0,t]$ is the external history of the system over interval $[t_0,t]$.

Roughly speaking, what happens inside the system is the consequence of what is applied to the system from the outside but depends also on the configuration of state variables at the moment each outside action is applied to the system; so, the same outside actions applied to different wear states and/or state variable configurations have different effects. In other words, the current wear state of the system is the consequence of the external history of the system throughout its life, but distinct sample systems which have had the same external history may have different current wear states, depending on their wear state at the beginning of their lives. In fact, according to our approach, the wear state of a physical system when its active life starts is different from one sample system to another, that is a physical system may be more or less worn out than another of the same type even from the very beginning. The successive evolution of the wear state is affected by the combined effect of the actions included in the system external history.

According to *(2')*, the state history of a physical system depends on the internal history and, vice versa, according to *(3)*, the internal history depends on the state history. This points out that the problem of computing in an analytic way the evolution of the wear state of a physical system over time is untractable and then such problem has to be faced by qualitative physics approaches.

4.4 A logical model of the task

The method we propose for estimating the current wear state of a given dynamic physical system (to which testing is not applied) is based on the corroboration of two distinct methods, having different input information.

The first method uses the wear state and the state variable configuration at the moment the latest SA was accomplished and the external history of the system from that instant to the current instant. Such method is founded on relation *(3)* and consists in simulating the evolution of the values of system parameters over time, from the latest time a SA was performed up to now, so that to estimate the current values of all system parameters. The simulation of the internal history requires also the simulation of the state history. Then, a simulation engine has to be available, which performs a temporal reasoning. The simulation may take advantage of the results of possible off-line measurements carried out in the considered interval.

The second method is the more traditional: it avoids considering any past information and consists in taking measures of both observable system output variables and system characteristics. Such measures have to provide, either directly or indirectly, the values of as many parameters as it is possible. At the end, the results produced by the two distinct methods have to be fused into one estimate of

the current wear state. Once the current wear state has been assessed, it has to be checked whether the current configuration of system parameters is within the parameter domain of the physical system or not. In the latter case, special warnings have to be displayed.

4.5 Knowledge sources

The task of SA, as defined in the previous sections, is knowledge intensive and, to a great extent, reasoning mechanisms are independent of the particular physical system at hand. Then SA lends itself to be faced by exploiting the knowledge-based system technology. The fundamental knowledge sources needed for performing the task are listed below.

- Modeled context graph. This is the knowledge as to the nominal behavior of the given physical system. The modeled context graph is basically the context graph introduced above wherein the nominal behavior is described by means of models. We do not make any assumptions as to the epistemological type of the models to be used: it depends on the knowledge available on a case by case basis. The triple *(I,O,S)*, the *P* set, the domain of the nominal behavior, the technical constraints, a behavioral model and a state model have to be associated to each context in the context graph. The *behavioral model* is a model that embodies equation *(1')*, that is that enables to compute/estimate the values of output variables at any instant based on those of input variables, state variables and system parameters at the same instant. The *state model*, instead, is a model that embodies equation *(2')*, that is, given an initial state variable configuration, the state model enables to compute/estimate the evolution of state variables over a time interval, based on the values of input variables and system parameters throughout the interval. Besides, the set of technical constraints regarding the whole context graph has to be associated to it.

While simulating the evolution of the values of system parameters over a past interval, the behavioral models can be used so that to determine the values of output variables at an instant an off-line measurement was taken. Then, the actual results of such measurement can be compared with the expected ones, determined based on the values of system parameters estimated by the simulation, so that to confirm or refute the simulation.

The state models can be used so that to determine the evolution of state variable configuration which, according to relation *(3)*, in necessary in order to assess the current situation of the system.

The domain of system parameters can be used in order to find out possible system faults that have not yet manifested as symptoms.

Each nominal working point is univocally identified by a point in the domain of the nominal behavior. So, the domain of nominal behavior may be divided into regions, each one having its own associated wear model: when the physical system is working in correspondence to a point of a region, the effect produced by the

operation in that region on the values of system parameters can be estimated by using the associated model.

- Classes of accidents. This is the knowledge as to the accidents of the physical system.

- Classes of diagnostic activities. This is the knowledge as to the diagnostic activities of the physical system. Both accidents and diagnostic activities may be organized into classes, where each instance of a class is characterized by its own *gravity dimensions*. The detrimental changes of the values of system parameters produced by each instance depends on its type and on the values of its gravity dimensions.

- Classes of maintenance interventions. This is the knowledge as to the maintenance interventions of the physical system. Such intervention may be classified and each class may be characterized by one or more *intensity dimensions*. The beneficial change of the values of system parameters produced by each instance of maintenance intervention depends on its type (that is on the class it belongs to) and on the values of its intensity dimensions.

- Wear knowledge. This is the knowledge needed for estimating the changes of the values of system parameters produced by each possible action that can be applied to the system from the outside. The wear knowledge has to provide the means for associating to each possible action in the external history (that is to each possible input variable configuration or instance of the classes of accidents, diagnostic activities and maintenance interventions) the changes of the values of system parameters such action produces; these changes depend on the specific wear state and state variable configuration of the system at the moment the action was applied. Besides, the wear knowledge has to provide the means for estimating the changes of the values of system parameters produced by the simultaneous occurrence of more than one outside actions. So this knowledge, which is uncertain in nature, enables to determine the internal history of the physical system based on the external history.

5 A case study: power transformers

Power transformers are very expensive and critical components in electrical power systems. Their outage directly affects the production and generally causes a substantial economical loss. Moreover, hazardous events, such as an explosion or fire, may occur, with safety-critical consequences and a negative impact on plant availability.

Since transformers are static machines, with a very simple input/output function, there are no external symptoms useful for detecting incipient faults while they are in operation. This is why power transformers are devices which are not directly subdued to continuous monitoring: only the network fed by a power transformer is

monitored. Besides, transformer testing can be carried out only when the transformer is out of service and is therefore performed only in exceptional cases, after some suspicions about transformer situation have already arisen. For all these reasons, the SA of power transformer is a scheduled task which is usually carried out by experts (who are a very critical resource for electrical companies) without performing any testing. Domain expert use their knowledge, accumulated through years of on-field experience, in order to assess transformer situation starting from some simple measurements that can be performed while the transformer is in operation. Electrical utilities are, therefore, significantly interested in scheduled methods to assess the health of power transformers and to timely diagnose abnormal phenomena which may lead to a fault.

In the last few years two of the authors have been involved in researches about a knowledge-based system for the SA of power transformers. The approach followed in such researches, which led to the implementation of a fully working prototype [8], concentrated on the interpretation of the results of measurements performed on the working transformer. The interpretation takes into account not only the last measurement results only but also the past history of the device. Past history includes results of previous measurements, the historical record of load profiles, maintenance interventions, and external anomalous events. What experts actually do is comparing and corroborating the estimate that they may formulate based only on the device history with the estimate that can be derived from last measurement results, as it will briefly be described in Section 5.7. This is indeed the logical model for accomplishing the task of SA proposed in this paper and the authors' claim is that this approach is cognitively plausible for several classes of physical systems.

In the following the knowledge available for carrying out the task of SA for power transformers is described. Such knowledge is classified after the fundamental knowledge sources listed in Section 4.5.

5.1 Modeled context graph

This section is split into two subsection, the first dedicated to the models describing the nominal behavior and the state behavior of power transformers, and the second dedicated to the most important system parameters affecting the transformer behavior and their domains.

5.1.1 Models

Since the goal a power transformer has to accomplish is only one and very simple, namely to modify the ratio between voltage and current of electric power (ideally without any power loss), it can be modeled as a device having only one operating mode. Behavioral and state models of power transformers, however, are seldom available as far as wear and tear processes are concerned and they are not used as a primary method by SA experts.

5.1.2 System parameters

The actual structure of a large power transformer is very complex, however for the sake of this paper we can consider a simplified partial model involving the following components:

- copper windings through which current flows. In three-phase transformers there are three couples of concentric windings: the ratio between the number of turns of the couples of windings determines the transformation ratio;
- insulating paper which wrap up the turns of the windings in order to prevent short circuits;
- insulating mineral oil within which all the other components are immersed. Oil has both the goal of contributing, along with the paper, to the insulation between windings and other metallic parts, and of cooling, by natural or artificial circulation, the parts which are subject to heating due to various types of power losses.

For each of the components listed above, one or more parameters can be defined which influence transformer behavior and whose progressive variation during operation may eventually lead to the occurrence of critical faults.

- Winding parameters. For windings, the only parameter we consider here is deformation. In fact, their geometrical shape is ideally cylindrical but can be subject to progressive deformations during the operations, mainly due to severe mechanical stresses caused by external short circuits. Even though a transformer may continue normal operation in presence of partially deformed windings, the problem is that deformed windings are subject to phenomena of mechanical instability, so that the occurrence of new short circuits may eventually destroy them.

- Paper parameters. For insulating paper, the main parameter is the polymerization degree, i.e. the mean length of the polymer chains composing it. This parameter is strictly related to paper compactness and to its mechanical strength. During transformer operation, paper heating determines a progressive breaking of polymer chains, so that the polymerization degree decreases with respect to the initial value and paper tends progressively to crumble, especially when it is mechanically stressed, i.e. in presence of external short circuits. If paper around windings breaks or crumbles, windings are no more insulated and a short circuit may occur within the transformer, with dramatic consequences (fire and explosion) because mineral oil is highly inflammable.

  The initial value of polymerization degree for normal new paper is known, as well as the lowest threshold value below which the transformer should not be kept in service.

- Oil parameters. For insulating oil, two parameters, whose nominal ranges are known, are worth consideration: acidity and dielectric strength. Oil acidity increases progressively from the initial value due to chemical phenomena related to oil heating

during operation. When acidity is above a given threshold, oil begins to corrode paper and metallic parts: in these cases it has to be subjected to a complex (and expensive) treatment in order to reduce acidity.

Dielectric strength is the most important oil property, since it guarantees electric insulation. Various causes, both related to specific abnormal phenomena and to normal oil aging, may provoke a decrease of dielectric strength, so that the danger of internal short circuits increases.

5.2 Classes of accidents

Two kinds of external accidents may affect a power transformer: short circuits and overvoltages.

- Short circuits. When a short circuit happens in the external power network, the current flowing within the transformer increases abruptly: the most important consequence is that windings (and therefore also insulating paper) are subject to a sudden and strong mechanical stress, causing also violent vibrations. As mentioned above, this may cause permanent deformations of the windings, or, if the mechanical structure of the windings collapses, the destruction of the transformer. The expert is able to qualitatively classify the criticality of each short circuit based on its peak value and duration: these values are available since they are registered by suitable devices monitoring the network.

- Overvoltages. They are large increases of the voltage value over the nominal one which may happen for various reasons within the network (typically manoeuvres modifying the actual topology of the network, such as the opening and closing of circuit breakers). Overvoltages propagate through the network and may reach a transformer, so that to stress its overall insulating system: the severity of the stress is related to the voltage value, which is measured by network monitoring devices.

5.3 Classes of diagnostic activities

Many kinds of diagnostic activities can be performed on a power transformer: we list here below only those significant for the present discussion.

- Measurement of winding inductance. It is a testing action (to be performed with the transformer out of service) which does not cause any serious deterioration of the values of system parameters.
- Paper sampling. It is a testing action (to be performed with the transformer out of service) which requires that the transformer is open. If carried out correctly, it does not cause any serious consequence on the values of system parameters.
- Oil sampling. It is a diagnostic activity that can be carried out also during normal transformer service. It does not cause any serious consequence on the values of system parameters.

5.4 Classes of maintenance interventions

As far as maintenance intervention are concerned, we distinguish here only two classes of interventions:

- oil maintenance, namely the chemico-physical treatment that can be applied to the oil in order to restore its desired properties;
- mechanical maintenance, including all the interventions that involve mechanical operations on the internal transformer structure necessary to restore its initial characteristics (both winding shape and insulating paper properties). These interventions are very complex and expensive and require the transportation of the transformer to the building firm.

5.5 Wear knowledge

Detailed analytical models of the various types of phenomena (electromagnetic, thermal, chemical) occurring within a transformer, during normal operation or accidents, are seldom available or useful for the specific task of SA. Therefore experts in charge of the SA of transformers do not resort to analytical models of physical processes and rather use empirical models, derived both from general principles and from working experience, to estimate the values of parameters according to transformer history. We mention here two of such kinds of models.

- Winding aging models. They are empirical models that allow experts to estimate the current deformation of transformer windings based on the short circuits that affected the transformer. A rough sum of such short circuits has to be made (it is indeed a weighed sum, where each short circuit is multiplied by its own criticality). This sum resumes the real short circuit history to a number of equivalent "maximal criticality short circuits". If such number is above a given threshold, which depends also on specific structural features of the considered transformer, there is a reasonable suspect that transformer windings may be seriously damaged.

- Paper aging models. They are empirical models that relate the decrease of polymerization degree to paper temperature. It should be stressed that such models are neither very accurate nor universally accepted: different experts use different models and there are also experts who do not really trust in any of these models. The maximum temperature reached by the paper within the transformer can be derived, again thanks to empirical models, from the value of the power flowing through it (it has to be noted that the value of flowing power does not change very often, so that thermal transients can be practically neglected). Based on the record of values of power flowing through the transformer, it is thus possible to build an historical record of the temperature reached by the paper and then, using the paper aging model, to evaluate the current polymerization degree.

5.6 Conducting Situation Assessment

Limiting our scope to the system parameters introduced in Section 5.1.2, conducting the SA of a power transformer means estimating the values of four parameters, namely winding deformation, paper polymerization degree, oil acidity and oil dielectric strength. According to the logical model of the task of SA introduced in Section 4.4, the values of system parameters have to be estimated based on current (and possibly past) "passive" measures and/or past external history. The definition of the external history of a physical system, given in Section 4.2, states it consists of the record of 1) input variable values, 2) accidents, 3) diagnostic activities, and 4) maintenance interventions, in a considered time interval. By now, we have defined what are accidents, diagnostic activities and maintenance interventions in the case of power transformers. Historical records are actually created for all these events. As to the values of input variable values, what is actually recorded for power transformers is the number of operation hours, each associated with the mean value of the power flowing through the transformer.

The way experts follow for performing the SA of power transformers, which resembles quite tightly the logical model for SA proposed in this paper, is briefly described in the following. The discussion evidences also how this kind of SA, which does not need any testing, is carried out so that to have a first estimate of the current system situation. On the ground of this estimate, experts may decide to perform specific testing actions and eventually to undertake maintenance interventions.

5.7 The way experts work

Expert estimate the value of winding deformation from past short circuits by using winding aging models. This estimation, based on past external history only, is quite important since there are no means to directly measure winding deformation during transformer operation. In case the estimated winding deformations are significant, inductance measurement is required and, to this end, a suitable transformer outage is scheduled. In fact, winding deformation causes a variation of winding inductance and is therefore estimated by measuring winding inductance and evaluating its variation with respect to the nominal value, measured when transformer was initially put in service. If measured inductance values confirm the presence of significant deformations, the transformer is taken out of service, in order to prevent possibly dramatic accidents, and is fixed or replaced, according to various types of technical and economical considerations.

The value of paper polymerization degree is roughly estimated from past operation by using paper aging models. As mentioned above, however, such models are not very accurate and reliable. Moreover they can not take into account anomalous phenomena, such as local overheatings (due for instance to a bad local circulation of oil), that may lead to accelerated aging, and thus to dangerous conditions, in specific parts of the transformer. Therefore the estimation of the current

paper polymerization degree based on paper aging models is always corroborated with analyses of oil samples. In fact, polymerization degree can be estimated on the basis of the presence within the oil of some chemical substances resulting from the decomposition of paper polymer chains. If the value of the concentration within the oil of chemical substances produced by polymer decomposition is higher (or lower) than the expert expected on the basis of previous calculations, it may reveal (or refute) the presence of very aged paper.

In case the preliminary estimation of paper polymerization degree has led to suspect that the paper is very aged, final decisions about interventions to be undertaken, such as, for instance, analyzing a paper sample, are subject to a complex risk/cost analysis. Paper sampling, which requires that the transformer is out of service and open, is a very complex and expensive intervention, which is justified only in extraordinary cases.

As far as oil parameters are concerned, namely acidity and oil dielectric strength, they are measured directly through suitable tests on oil samples.

6 Conclusions

The health state of a given physical system is represented by the configuration of the values of a number of (physical, chemical, structural, dimensional, spatial) parameters. Faults in a physical system are indeed invalid configurations of these parameters. The deviation of the values of such parameters from their domain is caused by deterioration phenomena, owing to the length of time, system operation, occurred accidents, diagnostic and maintenance activities. The task of situation assessment of a physical system, besides analyzing and interpreting current measures, could take advantage of the simulation of the evolution of the values of system parameters over a past interval of interest throughout which the causes of deterioration that were applied to the system are known. The problem of simulating the evolution of the values of system parameters over time is, however, untractable and therefore is a challenge to be faced by qualitative physics approaches. The contribution of this paper has to be found in the original modeling concepts and assumptions it proposes, which give an insight into physical system behavior, both healthy and faulty, and which possibly constitute a foundation for a new theory of situation assessment.

Keywords: situation assessment, fault diagnosis, model-based reasoning

References.

1. Ingrand, F.F., Georgeff, M.P. & Rao, A.S. An architecture for real-time reasoning and system control, *IEEE Expert*, 1992, 7(6), 34-44.
2. Laffey, T.J., Cox, P.A., Schmidt, J.L., Kao, S.M. & Read, J.Y. Real-time knowledge-based systems, *AI Magazine*, 1988, 9(1), 27-45.

3. Esprit Project 6862, *Real-time situation assessment of dynamic, hard to measure systems*, Tiger Final Report D120.36, 1995.
4. Morin, M., Nadjm-Tehrani, S., Österling, P. & Sandewall, E. Real-Time Hierarchical Control, *IEEE Software*, 1992, No. 9, 51-57.
5. Hamscher, W., Console, L. & de Kleer, J. (ed). *Readings in model-based diagnosis*, Morgan Kaufmann, San Mateo, CA, 1992.
6. Reiter, R. A theory of diagnosis from first principles, *Artificial Intelligence*, 1987, 32(1), 57-96.
7. Milne, R. Amethyst: Vibration based condition monitoring, in Keyes, J. & Maus, R. (ed), *The handbook of expert systems applications in manufacturing*, McGraw Hill Inc., 1990.
8. Baroni, P., Cremonesi, F., Guida, G., Mussi, S. & Yakov, S. ASTRA: a knowledge based system for state assessment, preventive diagnosis, and intervention planning of power transformers, pp. 463 to 470, *Proc. ISAP 94 Int. Conf. on Intelligent System Application to Power Systems*, Montpellier, F, 1994.