Method for Automatic Diagnosis Used in Real-Time Control Systems

Gianina Gabor, Doina Zmaranda

Department of Computer Science, University of Oradea
1 Universitatii Street, 410087 Oradea, Romania
E-mail: gianina@uoradea.ro, Phone: (+40) 259-432830 int 226
E-mail: zdoina@uoradea.ro, Phone: (+40) 259-432830 int 204

Abstract: During the last years, the use of real-time control systems in different fields, including vital applications has considerably increased. Consequently, possible failures in such systems may cause fatal accidents or unacceptable social and environmental damage. Therefore, the dependability, i.e., the reliability and availability of these systems is of great importance and methods for constructing highly dependable real-time control systems should be identified; in this idea, elaborating diagnosis strategies becomes an issue.
The present paper indicates an approach for treating the failure diagnosis problem using top-down analysis failure localization method, emphasizing the diversity of situations that could appear in automatic real-time control systems. The proposed diagnosis strategy is illustrated considering the electric power plant, part of the Oradea geothermal system. Based on this case study, the steps that should be considered when applying the method in practical situations have been outlined.

1 Introduction

Modern and future real-time control systems must address several, and sometimes conflicting issues: functional and temporal predictability, fault tolerance, reliability, dependability and maintainability. For each of these issues, specific techniques and methods should be developed from the early stages of design process, in order to maximize as much as possible the probability of timely execution even in the presence of faults [5]. Moreover, optimization of responsiveness requirements of real-time control systems requires a good understanding of real-time, functional and fault models and their characteristics, as a whole [9].

It is now acknowledged that to move towards reliability and dependability in real-time control is essential in industrial applications [6]. In this general process, diagnosis represents an important step during the design and analysis phase; therefore developing proper diagnosis strategies and methods becomes an essential part of the entire real-time control systems development process [9].

In order to elaborate a diagnosis strategy, a hierarchical gradual analysis (top-down) of failure, until failure localization method, is needed. Diagnosis time it is known to be an important element of Mean Down Time (MDT). Consequently, it is essential to control the characteristic values in the most important points of a real time automatic control system [1].

Thus, for each characteristic value, an interval of normal functioning should be defined, between the minimum and maximum admissible values [7]. For evaluating the position of the current value in the normal functioning interval, different approaches could be used. In this idea, to each characteristic value we associated two discrete variables: a proximity variable and a threshold variable [8]. The proximity variable can take the values L or H, depending on the fact that the value of the characteristic is near to the low limit L or to the upper limit H, and it is used for generating attention signals when functioning is near these admissible limits. The threshold variables can take the values LL or HH, depending on the fact that the characteristic value is near the low threshold limit LL or near the upper threshold limit HH and it is used for generating alarm signals when functioning is going in a point close to threshold limits. The proximity and threshold values are defined as variables in the control program, and are associated with the physical values from the controlled system [4].

In the case study presented in this paper, only threshold values are considered, because the purpose is the failure localization. The paper indicates an approach for treating the failure diagnosis problem emphasizing the diversity of situations that could appear in this process.

2 Proposed Diagnosis Method

A diagnosis strategy is illustrated further, considering the electric power plant as a part of the Oradea geothermal system. The geothermal power plant is a component of the cascaded geothermal energy utilization system, and is used to convert the energy of the geothermal water into electrical energy using CO_2 as working fluid. The elements of the power plant are the following [2]: vaporizers (heat exchangers used to vaporize the CO_2), a reciprocating engine connected with the electric generator, a make-up and expansion CO_2 tank, condensers (heat exchangers used to condense the CO_2) and a CO_2 pump. The control system has to maintain constant the CO_2 pressure and temperature in all the important states of the thermodynamic cycle.

The important points of the geothermal system correspond to the points of the characteristic values that are associated to the power plant thermodynamic cycle.

The proposed diagnosis strategy considers three hierarchical levels: system level (geothermal power plant level), sub-system level (a part of geothermal power

plant) and entity level. At the entity level, the diagnosis process that determines the failed element is finished. For minimizing the diagnosis time, a systematic method of failure diagnosis based on relevant data collecting and analysis is necessary. Diagnosis time could be reduced through further implementation on PLCs of some diagnosis modules [2].

2.1 System Level

Figure 1 presents a functional diagram at geothermal power plant level, indicating 4 measurement points for CO_2 temperature. Using these points, localization of the area where, for example, the event: „the CO_2 temperature is too high", considered as a major system failure, could be realized.

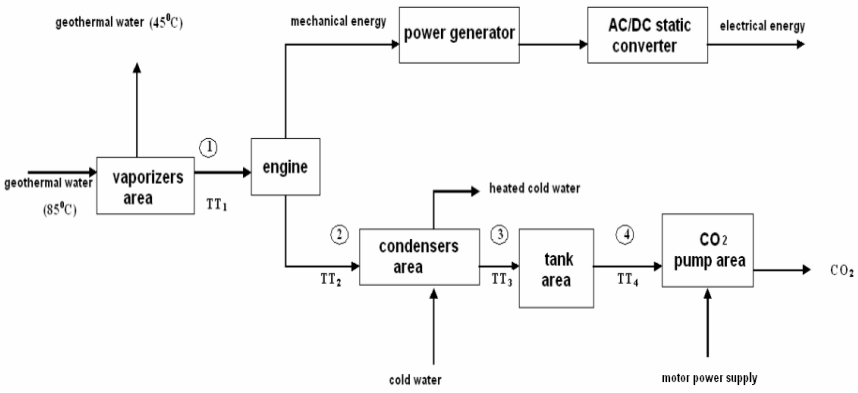

Figure 1
Functional block scheme on geothermal power plant (system) level

The area localization, also called system level failure localization, is a first step in hierarchical approach. Measurement of CO_2 temperature was realized using the temperature transducers TT1, TT2, TT3, and TT4 specified in Table 1, where only three of several possible scenarios are considered.

Sce-Nario	Point ①	Point ②	Point ③	Point ④	Failure localiza-tion area
S1	vTT1LL<vmTT1 and vmTT1<vTT1HH	vTT2LL<vmTT2 and vmTT2<vTT2HH	vmTT3>vTT3HH	vmTT4>vTT4HH	condensers area
S2	vmTT1>vTT1HH	mTT2>vTT2HH	vTT3LL<vmTT3 and vmTT3<vTT3HH	vTT4LL<vmTT4 and vmTT4<vTT4HH	vaporizers area
S3	vTT1LL<vmTT1 and vmTT1<vTT1HH	vTT2LL<vmTT2 and vmTT2<vTT2HH	vTT3LL<vmTT3 and vmTT3<vTT3HH	vmTT4<vTT4LL	tank area

Table 1
System failure localization for "the CO_2 temperature is too high" event

According to the data presented in Table 1, for each CO_2 temperature measured by TT1 – TT4 transducers, ownership in the frame of the admissible interval is verified. The measured values are generically denoted with vmTTx, the minimum threshold values with vTTxLL, and the maximum threshold values with vTTxHH. Depending on the combination obtained, the failure is localized in different areas.

For system failure detection, two principles are used:

1 any sub-system from the functional system for which the output temperature is not in the frame of admissible limits is potentially failed,

2 in a chain of successive failed sub-systems, the failure is associated to the first sub-system from the chain.

Different temperatures associated to the points from Figure 1, could be vectorial represented through:

measured values vector $t_{mCO2} = \begin{bmatrix} v_{mTT1} \\ v_{mTT2} \\ v_{mTT3} \\ v_{mTT4} \end{bmatrix}$, minimum values vector $t_{\min CO2} = \begin{bmatrix} v_{\min TT1} \\ v_{\min TT2} \\ v_{\min TT3} \\ v_{\min TT4} \end{bmatrix}$

and maximum values vector $t_{\max CO2} = \begin{bmatrix} v_{\max TT1} \\ v_{\max TT2} \\ v_{\max TT3} \\ v_{\max TT4} \end{bmatrix}$.

Functioning in the frame of admissible limits implies determining the vectors that contain the signed difference t_{mCO2} - t_{minCO2}, and t_{maxCO2} - t_{mCO2}, respectively, denoted with $(\Delta t)_s$ and $(\Delta t)_d$. When these resulting vectors have only positive signs, no failure is assumed and consequently, no diagnosis and localization is necessary. Failures appear when one ore more signs aren't strictly positive. In this case, two situations are distinguished:

- non-conflictual situations – when only one component from $(\Delta t)_s$, or $(\Delta t)_d$ respectively is negative; in this case, the failure is considered on the first principle basis and is associated to the sub-system for which the value corresponds to an output,

- conflictual situations – when two or more components from $(\Delta t)_s$, or $(\Delta t)_d$ respectively are negative.

Thus, S1 scenario corresponds to a conflictual situation because two negative signs appear; the values v_{mTT3} and v_{mTT4} overcome the admissible values.

$$(\Delta t)_S = \begin{bmatrix} >0 \\ >0 \\ >0 \\ >0 \end{bmatrix} \text{ and } (\Delta t)_d = \begin{bmatrix} >0 \\ >0 \\ <0 \\ <0 \end{bmatrix}$$

The conflict is solved by applying the second principle. According to Figure 1, failure is associated to the condenser group.

For the S2 scenario, there are also two values v_{mTT1} respective v_{mTT2} that overcome the admissible limits. In this situation, based on the same principle, the failure is localized in the vaporizers area.

$$(\Delta t)_S = \begin{bmatrix} >0 \\ >0 \\ >0 \\ >0 \end{bmatrix} \text{ and } (\Delta t)_d = \begin{bmatrix} <0 \\ <0 \\ >0 \\ >0 \end{bmatrix}.$$

A non-conflictual situation is the one considered in scenario S3 from Table 1. For this case, the only value that overcome admissible limit is v_{mTT4}, measured by TT4 transducer at point ④. Based on the first principle, the failure is localized at the tank zone level.

$$(\Delta t)_S = \begin{bmatrix} >0 \\ >0 \\ >0 \\ >0 \end{bmatrix} \text{ and } (\Delta t)_d = \begin{bmatrix} >0 \\ >0 \\ >0 \\ <0 \end{bmatrix}.$$

In the above presented context, automatic diagnosis strategy implies creating an application:

∂_S: $((\Delta t)_s, (\Delta t)_d) \rightarrow \delta_S$,

where: ∂_S is „diagnosis”application symbol

$((\Delta t)_s, (\Delta t)_d)$ is the set of al sign vectors pairs

δ_S is the set of failure at system level.

The application could be modeled and implemented in its simplest form, as a correspondence table. Practically, a program that operates with current, minimum (LL) and maximum (HH) values vectors and calculates the sign vectors is necessary.

2.2 Subsystem Level

For illustrating the sub-system diagnosis strategy, we assume the conditions of S2 scenario, where failure were localized at vaporizers level [2]. Consequently, the diagnosis procedure continues at subsequent level: the vaporizers level.

Figure 2 presents the functional block scheme at failure area level, in order to continue the diagnosis activity and identify the failed entity. The scheme includes also the control loop of the temperature t_1 of CO_2.

The scheme indicates the important points where measurements should be done for diagnosis (Table 2): real vaporizers output temperature t_1 (t_1), temperature t_1 measured by TT1 (t_{m1}) temperature transducer, power supply of the PLC (v), the control value (output of the RA1 controller, u_{t1}) and the geothermal water flow (q_{ac}).

Unlike the previous level, at vaporizers level we have a close loop structure that arises specific diagnosis problems, the principles 1 and 2 being non applicable.

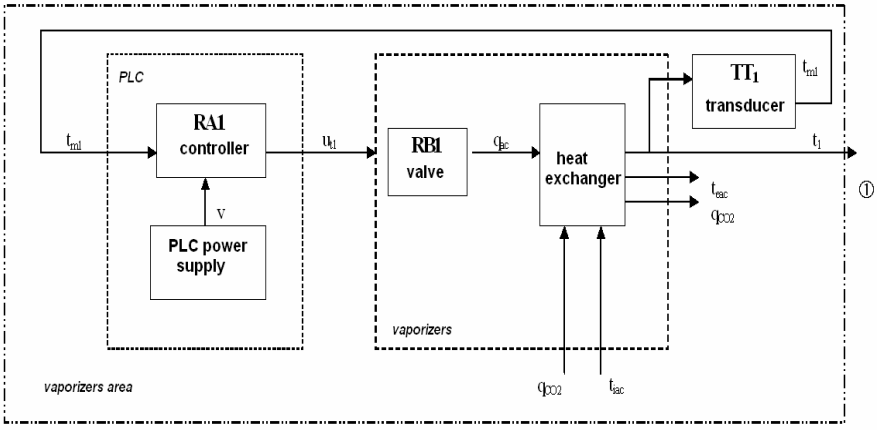

Figure 2
Functioning block scheme at vaporizers level

However, some useful remarks for diagnosis could be made:

1 the value of t_{m1} is visible modifying, while u_{t1} remains practically fixed, and is not reaching the limit values; consequently, the controlling algorithm implemented through RA1 is not functioning correctly and the failure is localized at controller level,

2 power voltage corresponding to the PLC, v, overcomes one of the admissible limits; it is likely that the PLC functioning to be incorrect and an automatic blocking to appear. Thus the failure is localized at the PLC power source.

3 the u_{t1} value is modifying while the flow q_{ac}, without reaching the limit values, does not; results that the control valve RB1 is failed.

4 the flow q_{ac} value is significantly modifying while temperature t_1 is not; we conclude that the failure is at the vaporizers block level, in the heat exchanger.

It is obvious that, in this case, the reasoning is not similar to the one from the first hierarchic level, the situation being more complicate because of the existing close loop. For a correct diagnosis at vaporizers level, adequate techniques should be used, that could cope with all possible failure scenarios [3], [2].

For continuing the methodological undergoing, we assumed that we are in the fourth situation mentioned above (q_{ac} is significantly modifying while the temperature t_1 is not) and we have a monitoring program that monitors over a limited period of time the values of q_{ac} flow and of the t_1 temperature. We denote this scenario S2-4 (scenario that indicates failure at the vaporizers level, in the heat exchanger). Consequently, the analysis could continue at the next hierarchical level.

2.3 Entity Level

Figure 3 presents the vaporizers block functioning scheme that contains two circuits: one corresponding to the geothermal water and one corresponding to CO_2.

In the scheme are represented the values that should be measured for failure diagnosis at this level: two temperatures (measured by TT1, TTac1, and TTac2 temperature transducers), two pressures (measured by TP1, TPac pressure transducers) and a flow (measured by TDac flow transducer).

For detection of failure at this hierarchical level, two similar principles with the ones from system level are adopted:

S2-4i) any component from the functional scheme for which the measured output value is not in the frame of admissible limits is considered potentially failed

S2-4ii) in an un-interrupted chain of failed considered components, the failure is associated to the first component in the chain

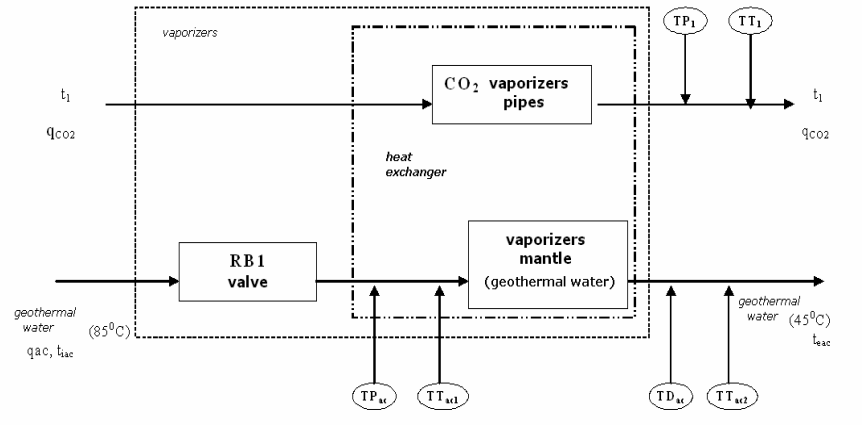

Figure 3

Vaporizers block functioning scheme

According to these principles, the values associated to the points from Figure 3 could be vectorial organized using measured values vector t_{mS2-4} and corresponding minimum and maximum values vectors $t_{minS2-4}$ and $t_{maxS2-4}$:

$$t_{mS2-4} = \begin{bmatrix} v_{mTP1} \\ v_{mTT1} \\ v_{mTTac1} \\ v_{mTPac} \\ v_{mTDac} \\ v_{mTTac2} \end{bmatrix}, \quad t_{\min S2-4} = \begin{bmatrix} v_{\min TP1} \\ v_{\min TT1} \\ v_{\min TTac1} \\ v_{\min TPac} \\ v_{\min TDac} \\ v_{\min TTac2} \end{bmatrix} \quad t_{\max S2-4} = \begin{bmatrix} v_{\max TP1} \\ v_{\max TT1} \\ v_{\max TTac1} \\ v_{\max TPac} \\ v_{\max TDac} \\ v_{\max TTac2} \end{bmatrix}$$

Functioning in the frame of admissible limits corresponding to the S2-4 scenario implies calculation of difference vectors $(\Delta t)_{S2-4d} = t_{mS2-4} - t_{minS2-4}$ and $(\Delta t)_{S2-4s} = t_{mS2-4} - t_{minS2-4}$. Failures appear when one or more of the above vector's signs are not positive.

Two possible scenarios for failure localization, in association with S2-4 scenario are presented in Table 2. They correspond to the mantle and pipes failures from inside the vaporizer heat exchanger.

Sce-nario	Indicated value TP1	Indicated value TT1	Indicated value Tpac	Indicated value TTac1
S2-4-1	vmTP1 < vTP1LL	vTT1LL < vmTT1 and vmTT1 < vTT1HH	vTPacLL < vmTPac and vmTPac < vTPacHH	vTTac1LL < vmTTac1 and vmTTac1 < vTTac1HH
S2-4-2	vTP1LL< vmTP1 and vmTP1 < vTP1HH	vTT1LL< vmTT1 and vmTT1< vTT1HH	vmTPac < vmTPacLL	vTTac1LL < vmTTac1 and vmTTac1 < vTTac1HH

Sce-nario	Indicated value Tdac	Indicated value TTac2	Indicated value defect
S2-4-1	vTDacLL < vmTDac and vmTDac < vTDacHH	vTTac2LL< vmTTac2 and vmTTac2 < vTTac2HH	vaporizers pipes broken
S2-4-2	vTDacLL< vmTDac and vmTDac < vTDacHH	vTTac2LL < vmTTac2 and vmTTac2 < vTTac2HH	vaporizers mantle broken

Table 2

Failure localization inside the entity, at entity component level

The S2-4-1 corresponds to a non-conflictual situation. For this scenario we have:

$$(\Delta t)_{S2-4s} = \begin{bmatrix} <0 \\ >0 \\ >0 \\ >0 \\ >0 \\ >0 \end{bmatrix} \text{ and } (\Delta t)_{S2-4d} = \begin{bmatrix} >0 \\ >0 \\ >0 \\ >0 \\ >0 \\ >0 \end{bmatrix}.$$

A single value is under the admissible limit, the one measured by the TP1 (v_{mTP1}) transducer. Based on the firs principle S2-4i) this implies that the failure is localized at in CO_2 pipes level from the vaporizers heat exchanger.

The S2-4-2 contains also a non-conflictual situation, for this scenario we have:

$$(\Delta t)_{S2-4s} = \begin{bmatrix} >0 \\ >0 \\ <0 \\ >0 \\ >0 \\ >0 \end{bmatrix} \text{ and } (\Delta t)_{S2-4d} = \begin{bmatrix} >0 \\ >0 \\ >0 \\ >0 \\ >0 \\ >0 \end{bmatrix}.$$

A single value is under the admission limit, the one measured by the TPac (v_{mTPac}) transducer. Based on the first principle S2-4i) this implies that the failure is localized at the mantle level from the vaporizers heat exchanger.

Conclusions

By applying the functional block schemes implementation on various hierarchical levels in a system, and using different identification methods and information processing techniques, a failure diagnosis strategy is defined in this paper. This strategy could be applied using different scenarios for different types of failures, downward to the entity component level.

The proposed strategy outlines the idea that, if, in an automatic real-time control system, we can measure the values of characteristics in the most important points, this will create a basis for rapid failure diagnosis and diagnosis time reduction. Moreover, it is shown that, when relevant attention and alarm signals could be implemented through a control program, the time for failure awareness could be reduced, and consequently, the responsiveness and dependability of such real-time control systems being increased. The feasibility of proposed diagnosis approach is demonstrated using a practical case study.

References

[1] Bentley, J. P: Introduction to Reliability and Quality Engineering, Addison Wesley Longman, 1999

[2] Gabor, G. A: Contributions to the research on control system availability with applications for the control system of a geothermal power plant, Ph.D. theses, "Politehnica" University of Timişoara, 2005

[3] Katebi, R., Johnson, M.A., Wilkie, J: Control and Instrumentation for Wastewater Traitment Plants, Springer, 1999

[4] Goble, W: Evaluating Control Systems Reliability – Techniques and Applications, Instrument Society of America, Resources for Measurement and Control Systems, 1995

[5] Laplante, Ph. A: Real-Time Systems Design and Analysis – An Engineer's Handbook – Second Edition, IEEE Computer Society Press, 2000

[6] Liu, J: Real-Time Systems, Prentice Hall, 2000

[7] Svrcek W., Mahoney D., Young B: A Real-Time Approach to Process Control, John Wiley & Sons, 2000

[8] Smith C. A., Corripio A. B: Principles and Practice of Automatic Process Control, 2nd edition, John Wiley & Sons, New York, 1997

[9] D. Zmaranda, G. Gabor: Reliability Improvement Techniques for the Control System of a Geothermal, Power Plant, Studies in Informatics and Control, Informatics and control Publications, Volume 14, Number 1, Bucharest, Romania, March 2005, pp. 47-54