ON-LINE QUALITATIVE MODEL-BASED DIAGNOSIS OF TECHNOLOGICAL SYSTEMS USING COLORED PETRI NETS

Adrien Leitold[1] Miklós Gerzson[2] Anna I. Pózna[2] and Katalin M. Hangos[2,3]

[1]Department of Mathematics
[2]Dept. of Electrical Engineering and Information System,
University of Pannonia
H-8201 Veszprém, P.O.B. 158,
Hungary

[3]Process Control Research Group
Computer and Automation Research Institute
H-1518 Budapest, P.O.B. 63
Hungary

E-mail: leitolda@almos.uni-pannon.hu

KEYWORDS
fault diagnosis, qualitative model, colored Petri net, HAZID tables

ABSTRACT

A novel on-line diagnosis method is proposed in this paper that uses a qualitative dynamic model of the system and its colored Petri nets model. The model contains both the normal and the possible faulty operational modes of the system. The deviation between the normal and faulty modes is characterized based on P-HAZID tables. The actual system state can be searched on the occurrence graph constructed in advance. Starting from this node the possible consequences and root causes can be determined on-line with traversing on the graph. The proposed method is illustrated on simple case studies.

INTRODUCTION

Large complex technological systems, such as manufacturing or process plants, are often characterized by a large event flow with discrete or qualitative valued variables in case of any abnormal operation. Therefore, qualitative model-based diagnosis has a large practical importance, but possesses unique theoretical challenges in the form of computational complexity at the same time.

Building the qualitative model is the most important step of the diagnosis. A method is proposed for automatic transformation of a quantitative model into its qualitative form in (Yan 2003). Another key task in prediction-based diagnosis is the prediction problem. Zhu and Tan (2010) proposed the notion of ternary qualitative function to solve effectively the qualitative prediction problem. In another approach of qualitative diagnosis, Console et al. (2007) proposed a framework for decentralized model-based diagnosis of complex systems modeled with qualitative constraints. In their methods local diagnosers are assigned to the subsystems and they are supervised by the diagnoser of the complex system.

Qualitative models used for diagnosis are given in different forms (e.g. graphs, discrete event models, qualitative difference equations), and originate not only from special purpose modeling, but also from risk and hazard analysis (HAZID). Earlier work has shown that the result of HAZID analysis given in the form of HAZID tables can be effectively used for diagnosis both in the static and dynamic cases (Németh and Cameron 2013), (Tóth et al. 2014).

Colored Petri nets (abbreviated as CP-nets) combine the modeling advantages of Petri nets and compactness of the functional programming language Standard ML (Jensen et al. 2007). The CP-nets clearly enable both the mathematical and the graph representation of a technological system to be modeled, where the signals of the system have discrete range space and time is also discrete (Fanti and Seatzu 2008). It means that CP-nets can be used to model systems characterized by signals with qualitative range space and controlled by operating procedures containing events.

The aim of this work is to develop a hybrid method for on-line diagnosis that combines the availability and flexibility of HAZID information-based diagnosis with the computational power and tools available for CP-nets.

BASIC CONCEPTS

In the following section the most important concepts are summarized on characterizing measured values in qualitative way, on hazard analysis of technological systems using P-HAZID method, and on timed CP-nets and their occurrence graph based analysis.

Qualitative Range Spaces

Measured values of a technological system do not necessary be equal to a given prescribed value, but it is often enough if they belong to a specified range. For example, for an arbitrary sensor the following ranges can be defined:

$$Q_s = \{e^-, 0, L, N, H, e^+\}$$

where 0, L, N, H refer to zero, low, normal and high measured value, respectively, while e^- and e^+ may refer to outlier value caused by a bias failure of the sensor. The state of an actuator can be described similarly.

Events, Traces and Deviations

The actions to be performed by the operators and the changes in the measured values are summarized in an

event list usually called operational procedures. In this paper it is assumed, that the elements of this list are arranged by the time, i.e. they contain the value of input and output variables in a given time stamp τ, as

$$event_\tau = (\tau, \textit{input values}, \textit{output values}).$$

The set of consecutive events is called **trace**. Based on the faultless or faulty operational course, nominal and faulty traces can be distinguished. The **nominal** trace gives the list of events under fault free conditions while faulty traces describe the events if a given fault occurs. At the recent stage of our work **it is assumed that only one fault takes place** in a modeled technological unit, and this fault is constantly present since the beginning of the operation. Comparing the trace of a given operational course (called **characteristic trace**) and the nominal trace **deviations** can be defined if a fault occurs. The most important deviation types are the following:

- *never-happened* - if the given combination of input and output variable values does not occur in the characteristic trace at any time stamp;
- *later* or *earlier* - if the given combination occurs but at a later or earlier time stamp than in the nominal trace;
- *greater* or *smaller* var_out_i – if the qualitative value of an output variable is greater or smaller in the characteristic trace than in the nominal trace at a given time instant τ.

Procedure HAZID

HAZOP or FMEA analysis is normally used for hazard identification of a technological system. As a combination and extension of these two methods the **procedure HAZID** (abbreviated as P-HAZID) is introduced in (Tóth et al. 2014). The result of a P-HAZID analysis is a table containing the possible deviations in the system together with their implication and causes. A cause can be a root cause if it is a non-measurable failure mode of a system element.

The diagnostic procedure based on these P-HAZID tables is as follows. As a first step the deviations between the characteristic trace and nominal trace is determined. Then the causes of the determined deviations can be deduced going backwards on the rows on the P_HAZID table until a root cause is found (Tóth et al. 2014). This means that the P-HAZID tables are processed in the backward direction of the cause-consequence relations to perform diagnosis.

Colored Petri Nets

According to the formal definition (see details in (Jensen 1997)) a CP-net model consists of places, transition, guard and arc functions, colors and tokens. For diagnostic investigations the following special choices were used in modeling of technological systems.

- **Places** refer either to the input and output variables and the **color of tokens** on them describe the variables' value, or they serve as fault and deviation places and their tokens refer to type of the fault occurring in the system and to the emergent deviation from the nominal trace.
- The main task of **transitions** is the timing of the operation. It is assumed that the operation of the system can be divided into user defined time period, and the values of variables change at the end of a period. The **guard functions** assigned to the transitions contain the fault generation function (Gerzson et al. 2012).
- **Arcs** connect places to transitions according to the logical connections between them, and the **arc functions** describe the change of colors.

The consequences of a processing step can be stochastic in a technological system. For example, the step may be completed in a normal way, or a fault occurs. The probabilistic nature of a transition t associated to a processing step can be modeled in a CP-net in such a way, that a fault function is built into its guard function. This fault function returns the logical value *true* or *false* with predefined probability, and the token values of the adjacent consequence places of transition t can be controlled by this logical value. This type of transition firing is called **stochastically fired transition** (Leitold et al. 2013).

Having the model of the investigated system the behavioral analysis can be done with the occurrence graph (Jensen 1997). The basic idea of the occurrence graph is to generate all of the reachable markings (system states) from the initial one in a form of a graph. Investigating the branches of the graph the cause and the consequences of given system state can be considered.

THE PETRI NET BASED DIAGNOSIS METHOD

The aim of this section is to introduce the proposed CP-net model-based diagnosis.

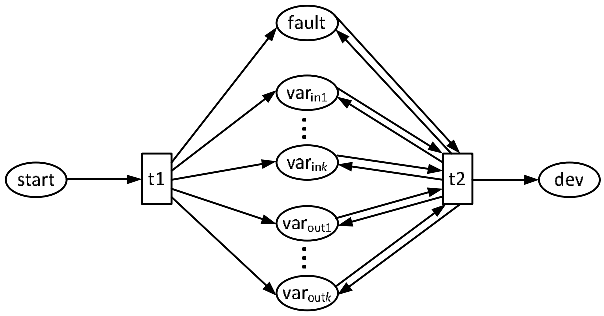
The Qualitative Model and Data Used for Diagnosis

For the general description of the proposed method let us assume that the **P-HAZID table of the modeled system is given and this table is complete and consistent**. This is, however, rarely the case of large complex dynamic systems; the handling of the partial information case is the subject of further work.

As it was mentioned before, an operational step of the system is described as an event, while the consecutive events form a trace. The nominal trace is a trace that corresponds to the fault-less operation of the system. During a real operational course a characteristic trace is observed which contains the actual measured list of events. Therefore the characteristic trace can contain fault-related or fault-free events. Comparing the nominal and the characteristic traces the list of deviations can also be obtained.

The CP-net Diagnoser

In order to use a CP-net for diagnosis we construct a special CP-net model. The input and output variables are modeled as places in this net (see Fig. 1.). The color sets belonging to these places contain the possible values of the variables. One of the other places describes the fault occurring during the operation, while a special place refers to the deviations from the normal course. At the end of the simulation this place contains all the deviations as tokens generated in the course of the system operation in case of a given fault.



Figures 1: Generalized CP-net Model for Diagnosis

Two transitions are defined in this CP-net model. The first one (t1 in Fig. 1.) is for setting the initialization values to places. For the initialization of the input and output variables the arc expression functions belonging to the arcs connecting transition t1 and the corresponding places contain the initial value of these variables. Transition t2 generates the changes taking place as time evolves. This way the above CP-net is regarded as a discrete event model of the system to be diagnosed.

The Course of the On-line Diagnosis

The proposed diagnosis method is based on the investigation of the occurrence graph of the CP-net model of the diagnosed system. The occurrence graph is generated for a given initial state of the system. Assume only those faults can occur during the operation of the system which are built in the fault function and all the consequence of these faults are known. It is also assumed that the consequences of faults appear in the token color of variables and deviation places in CP-net model. In this case the occurrence graph contains all the reachable markings (states) of the net. Therefore both the states of normal operation (i.e. the nominal trace) and the states of different faulty modes are encoded into the nodes on the graph.

Having the CP-net model of the system to be diagnosed, the occurrence graph can be constructed off-line in advance. This graph is used during the operation of the on-line diagnosis in such a way, that the operator determines the node referring to the actual system state, and starting from this node the possible consequences can be concluded. On the other hand, the possible causes of faults can be determined from this node of the graph, too. Assume that the complete characteristic trace is known from the operation of the technological system and a deviation list is generated by comparing that to the nominal trace. Then the fault can be determined by comparing the resulted deviations with the token colors of the deviation place in the terminal nodes of the occurrence graph.

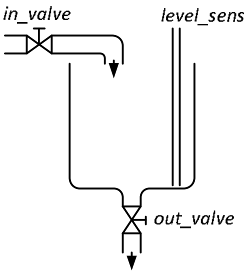
We can also consider the case, when the complete characteristic trace is not known because the operation of the system is not completed but the deviations up to a certain time instant are known. In this case **the recent deviation list has to be compared to the color of deviation place having the same time stamp in the nodes of occurrence graph**. If only one node has equality in its deviation list, then the possible faulty mode is determined. If more than one node meets this criterion, i.e. different operational modes result in the same deviations, then the possible set of faults can only be determined and further investigations are needed.

SIMPLE CASE STUDIES

Two simple case studies are presented: the first one is a simple system consisting of just a single component, while the other one is a composite system built up from three components.

Filling Process of a Tank

For the illustration of described hazard identification method the filling process of a tank is investigated. This simple technological unit consists of a tank with an input and output connection (see Fig. 2.). The control of the liquid flow is performed by magnetic valves. There is a level sensor in the tank to check the actual value of the level.



Figures 2: Scheme of Simple Tank Example

The operating procedure for the tank is as follow. In the initial state the valves are closed, the tank is empty. As a first step the input valve is opened. Then the control system waits for the filling up of tank for two time periods. Then the output valve is opened and the tank works as a continuous unit. The actual value of the level sensor is recorded in every time period but these data are used for monitoring the correct operation of the unit only.

It is assumed that the following faults can occur in the system:

– The fault of the level sensor, what can be either negative or positive bias error, i.e. the measured value is less or greater than the actual value with one qualitative unit.
– The fault of the tank, when the tank is leaked and the level of the liquid remains zero.

It is assumed only one of these faults can occur and the fault had evolved before the process starts and it remains constant during the operation.

The input variables of this system are the states of the input and output valves, while the output variable is the level value measured by the level sensor. The qualitative range spaces for the variables are as follows. For the input variables, i.e. for the valves the qualitative range space

$$Q_v = \{op, cl\}$$

is used, where *op* and *cl* refers to the open and close state of valves, respectively. For the output variable (for the measured level value) the already introduced qualitative range space Q_s is applied (see Sec. *Basic Concepts*).

An element of the event list has the following structure: $event_\tau$ = (τ, *state of input valve*, *state of output valve*, *measured value of level sensor*), where τ is the time stamp. The trace for the normal operational course is as follows:

$$T = event_0,\ event_1,\ event_2,\ event_3;$$

where

$event_0$ = (0, *cl*, *cl, 0*) – initialization;
$event_1$ = (1, *op*, *cl, 0*) – the input valve opens;
$event_2$ = (2, *op*, *cl, L*) – an intermediate state;
$event_3$ = (3, *op*, *op, N*) – the filling up is ready.

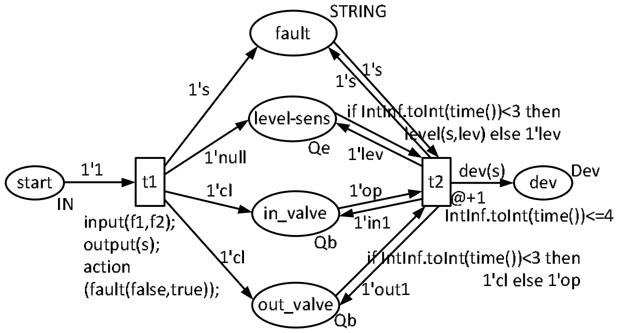
This event list is modified if a fault occurs. If the tank leaks, the following trace is generated:
T' = (0, *cl*, *cl, 0*), (1, *op*, *cl, 0*), (2, *op*, *cl, 0*), (3, *op*, *op, 0*)
As a consequence of the leak the tank remains empty. In case of negative bias error of level sensor:
T'' = (0, *cl*, *cl*, e^-),(1, *op*, *cl*, e^-),(2, *op*, *cl, 0*),(3, *op*, *op*, *L*).
The value shown by the sensor is less with one qualitative value than in the normal trace.

Comparing these traces to the nominal trace, the deviations from the normal operational mode can be determined and the P-HAZID table can be set up. A part of this table is shown in Table 1.

Table 1: Part of P-HAZID Table of Tank Filling Example

Cause	Deviation	Implication
Tank_leak	NH(2, *op*, *cl*, *L*)	NH(3, *op*, *op*, *N*)
Tank_leak	SML(2, *op*, *cl*, *L*)	SML(3, *op*, *op*, *N*)
Neg_bias	LAT(1, *op*, *cl*, *0*)	LAT(2, *op*, *cl*, *L*)
LAT(1,*op*, *cl*, *0*)	LAT(2, *op*, *cl*, *L*)	NH(3, *op*, *op*, *N*)

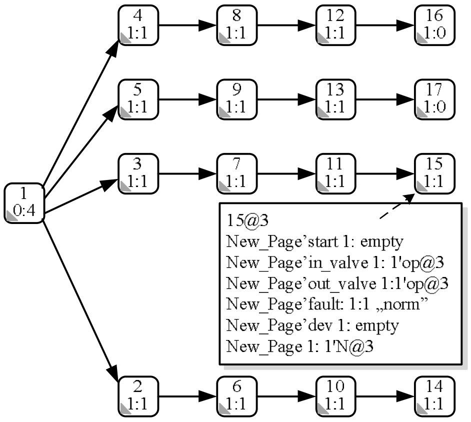
The software package CPNTools (CPNTools) was used for implementing the proposed hazard identification method, and for the generation and investigation of occurrence graph. The CP-net model of the simple tank can be seen in Fig 3. The places 'in_valve' and 'out_valve' refer to the input variables while the place 'level_sens' to the output variable. The color sets belonging to these places correspond to the defined qualitative range spaces. In case of fault, the token on place 'fault' contains its type and the tokens on place 'dev' give the deviations from the normal course. Transition 't1' initializes the system. The fault initialization function in the guard function of transition 't1' determines the type of the fault.



Figures 3: The CP-net Model of the Simple Tank System

Transition 't2' models the operation of the system. This transition fires as many times as many events are in the event list. As result of a firing the following can happen in the system:

– state of input and output valves can change;
– the measured value of the level sensor can change according to faultless or faulty operational mode;
– in case of fault the generated tokens on place 'dev' describe the deviations from the normal course based on P-HAZID table.

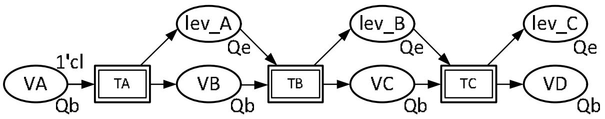


Figures 4: The Occurrence Graph of Simple Tank Example

The occurrence graph of the simple tank example can be seen in Fig 4. In this case the graph is a tree which has four branches according to four operational modes (normal and three different faults) of the system. In case of normal operational mode the work of the system ends properly (Node 15). There is no token on place 'dev', i.e. the system works in a normal, faultless way. In this simple example the complete deviation lists in every operational case are different, therefore comparing the resulted deviation list with terminal nodes the fault can be identified unambiguously. In case of on-line fault identification it can be stated if there is any deviation at the first time instance then based on its character the negative bias or positive bias can be determined. If the deviation appears at the second time instant only, then the fault must be a leak.

Series of Three Tanks

The developed method gives possibility to diagnose complex composite systems, too. Exploiting the hierarchical modeling feature of CPNTools, a CP-net model of complex system can be constructed form the known CP-net model of simple technological units.



Figures 5: The Hierarchical CP-net Model of the Serial Tank System

To show this, the example of three tanks in serial is investigated. The upper level of the CP-net model can be seen in Fig. 5. The upper level contains the logical connections among the elements which are necessary for the right timing and the fault propagation. The models of the tanks, which are embedded as subnets, are very similar to the model in Fig. 3, some modification of arc expressions and an extra place for fault propagation are needed only. For the hazard investigations it is assumed that fault can occur at any of the system element but only one fault can occur at an element. The occurrence graph of whole system can be used for fault detection as it was described at the single tank example.

Although the serial tank system is relatively simple system but its occurrence graph contains more than 200 nodes. Searching on a large graph is a computationally hard problem. In (Tóth et al, 2014) is proved that complex system can be structurally decomposed and the diagnosis can be performed on the component elements separately. This can be used in our case so that the occurrence graph of the subsystems is applied for the diagnosis first, then the search can be spread out to the other parts or to the whole occurrence graph, if necessary.

CONCLUSION

A novel on-line diagnosis method is introduced for hazard identification of technological systems. The method is a hybrid procedure for on-line diagnosis that combines the availability and flexibility of HAZID information-based diagnosis with the computational power and tools available for CP-nets. The deviations between the nominal and characteristic traces stem from the technological system can be identified on the occurrence graph of CP-net model. The occurrence graph of the system to be diagnosed can be constructed in advance and with the on-line searching on the graph the possible fault can be determined. The proposed methods and tools were illustrated using two simple case studies.

ACKNOWLEDGEMENT

This research is partially supported by the Hungarian Research Fund through grant No. K-83440. We also acknowledge the financial support of the Hungarian State and the European Union under the TAMOP-4.2.2.A- 11/1/ KONV-2012-0072.

REFERENCES

Console, L.; C. Picardi and D.T. Dupré 2007. "A Framework for Decentralized Qualitative Model-Based Diagnosis." *International Joint Conference on Artificial Intelligence IJCAI-07*, Hyderabad, India, 286-291

Fanti, M.P. and C. Seatzu. 2008. "Fault diagnosis and identification of discrete event systems using Petri nets" *9th International Workshop on Discrete Event Systems* WODES 2008, 432-435

Gerzson, M.; B. Márczi and A. Leitold. 2012. "Diagnosis of Technological Systems based on their Coloured Petri Net Model" *ARGESIM Report* Eds: Troch, I., Breitenecker, F. no. S38 358/1-6.

Jensen, K. 1997. "Coloured Petri Nets: Basic Concepts, Analysis Methods and Practical Use" Springer-Verlag

Jensen, K.; L.M. Kristensen and L. Wells. 2007. "Coloured Petri Nets and CPN Tools for Modelling and Validation of Concurrent Systems" *Int. J. of Software Tools for Technology Transfer* 9. 3-4. 213-254

Leitold, A.; B. Márczi; A. I. Pózna and M. Gerzson. 2013. "Investigation of manufacturing systems using timed colored Petri nets *Factory Automation Conference*, Veszprém, Hungary

Németh, E. and I. T. Cameron. 2013. "Cause-implication diagrams for process systems: Their generation, utility and importance." *Chemical Engineering Transactions*, 31:193–198.

Tóth A.; K.M. Hangos and A. Werner-Stark. 2014. "A structural decomposition-based diagnosis method for dynamic process systems using HAZID information." *J. of Loss Prevention in the Proc. Ind.* 31:(1) pp. 97-104.

Yan, Y. 2003. Qualitative Model Abstraction for Diagnosis, *17th Int. Workshop on Qualitative Reasoning*, Brasilia, Brazil, Aug. 20-22, 171-179.

Zhu J. and S. Tan. 2010. A novel approach to qualitative prediction. *The 2nd In. Conf. on Computer and Automation Engineering*, ICCAE'2010 Singapore 816-821

WEBREFERENCES

CPNTools 2.2.0 http://wiki.daimi.au.dk/ cpntools/},
University of Aarhus, Denmark, CPN Group