On-Line Checking of Faults in Cyber-Physical Systems

Volodymyr G. Skobelev and Volodymyr V. Skobelev

June 9, 2019

On-Line Checking of Faults in Cyber-Physical Systems

V.G. Skobelev$^{[0000-0002-7018-2319]}$ and V.V. Skobelev$^{[0000-0003-1581-3859]}$

Glushlov Institute of Cybernetics of NAS of Ukraine,
Glushkov Ave., 40, Kyiv, 03187, Ukraine
skobelevvg@gmail.com

Abstract. Numerous applications of cyber-physical systems in safety-critical spheres of human activity are the main reason for the fact that the development of methods intended for on-line faults diagnoses in these systems is one of the actual problems. One of the essential sub-problems for this problem is elaboration of models and methods intended for on-line checking of faults in cyber-physical systems. In the given paper this sub-problem is investigated under the supposition that these systems can be modeled by the 1-dimensional hybrid automata defined in the given paper. On the base of this model-based approach, some completely distributed system intended for on-line monitoring and fault components isolation in cyber-physical systems is proposed. This system consists of controllers of two types. Controllers of the first type are intended for checking the dynamics of physical processes, while controllers of the second type are intended for checking switching between dynamics. The structure of both types of proposed controllers is considered in detail. Necessary and sufficient conditions that guarantee for both types of proposed controllers that they carry out correct on-line checking are established and proved.

Keywords: Hybrid automata · Faults · On-line checking.

1 Introduction

Modern information technologies have stimulated penetration of cyber-physical systems (CPS) into different spheres of mankind activity. Informally, any CPS (see [1], for example) consists of some computer networks and/or built-in controllers that are used for control of considered physical processes via the feedback, i.e. the considered physical processes conduct the computations, while the computations, in its turn, conduct the choice and the mode of these physical processes. The state of the art in the development of CPS is presented in [2,3].

At present, CPS are widely used at the research of the Space, in power, military, transport, healthcare, and production spheres, for the design of modern infrastructure, etc. By this reason, in the overwhelming majority of cases, these domains are critical ones. Therefore, in the vast majority of cases, CPS are safety-critical systems. For this reason, the development of methods intended for faults diagnoses in CPS is one of the actual problems. Different approaches for investigation of this problem have been presented in [4–6].

The essential sub-problem for the problem of on-line faults diagnoses in CPS is the problem of on-line monitoring and fault components isolation in these systems. The given paper is devoted to the investigation of this problem.

We propose some model-based completely distributed system intended for on-line monitoring and fault components isolation in the analyzed CPS. This system consists controllers of two types. Controllers of the first type are intended for checking the dynamics of physical processes in the analyzed CPS, while controllers of the second type are intended for checking switching between dynamics in the analyzed CPS.

2 Mathematical Backgrounds

It is well-known that hybrid automata (HA) are one of the most often used mathematical models for the design of formal specification and the analysis of CPS. Therefore, it is natural to develop any model-based algorithms or systems intended for analysis of CPS in terms of HA.

One of the first definitions for HA has been proposed in [7]. Although this definition of HA provides to us a convenient conceptual model, it is very difficult to apply this model for the development of algorithms for CPS. Indeed, at the solution of specific problems for CPS by means of these or those software tools, the researcher, as the rule, must predetermine, detail and reformulate analyzed objects and concepts in such way that the received model can be very problematically squeezed in this definition of HA.

For the development of algorithms for analysis of CPS, much more convenient and much more widely used is the model of HA defined in [8] in the following way.

An HA is a system

$$\mathcal{H} = (Q, X, I, D, f, E, G, R),$$

where:

Q is a finite set of discrete states;

$X \subseteq \mathrm{R}^n$ is a set of continuous states;

$f : Q \times X \to \mathrm{R}^n$ is vector field;

$I \subseteq Q \times X$ is a set of initial states;

$D : Q \to \mathrm{B}(X)$ is a domain;

$E \subseteq Q \times Q$ is a set of edges;

$G : E \to \mathrm{B}(X)$ is a guard condition;

$R : E \times X \to \mathrm{B}(X)$ is a reset map.

It is well-known that there is a considerable number of difficulties connected with computations and algorithmic solvability for such general model of HA. By this reason, at the resolving of specific problems for CPS, the researchers take this circumstance into consideration and usually limit themselves to the analysis of sufficiently narrow sets of HA.

Due to this approach, we investigate the problem of checking of faults in CPS under the assumption that the associated model of HA is an element of the set H_0 of 1-dimensional HA that has been defined and investigated in [9].

This set H_0 of 1-dimensional HA has been defined proceeding from the model of HA offered in [8], as follows.

It is assumed that for each discrete state $q \in Q$ the following six conditions hold:

1. The set $D(q) = X_q \subseteq X$ is some finite interval.

2. The set of initial values of the continuous state is the set of pair-wise disjoint closed intervals $[\alpha_{q,h}, \mathrm{A}_{q,h}]$ $(\alpha_{q,h} \leq \mathrm{A}_{q,h})$, where $h = 1, \ldots, r_q$.

3. The guard condition associated with the set of initial values $[\alpha_{q,h}, \mathrm{A}_{q,h}]$ $(h = 1, \ldots, r_q)$ is some closed interval $[\beta_{q,h}, \mathrm{B}_{q,h}]$ $(\beta_{q,h} \leq \mathrm{B}_{q,h})$, and the sets $[\beta_{q,h}, \mathrm{B}_{q,h}]$ $(h = 1, \ldots, r_q)$ are pair-wise disjoint.

4. For each set $[\alpha_{q,h}, \mathrm{A}_{q,h}]$ $(h = 1, \ldots, r_q)$ of initial values the dynamics is presented by the differential equation $\dot{x} = f_{q,h}(x)$, where $Dom(f_{q,h}) \supseteq X_q$ and $f_{q,h}$ is some Lipschitz continuous function.

5. For each set $[\alpha_{q,h}, \mathrm{A}_{q,h}]$ $(h = 1, \ldots, r_q)$ of initial values the duration of the dynamics is some number $t_{q,h} \in [\theta_{q,h}, \varTheta_{q,h}]$ (where either $\theta_{q,h} = \varTheta_{q,h} = 0$, or $0 < \theta_{q,h} < \varTheta_{q,h}$), such that $x(t_{q,h}) \in [\beta_{q,h}, \mathrm{B}_{q,h}]$.

6. For each guard condition $[\beta_{q,h}, \mathrm{B}_{q,h}]$ $(h = 1, \ldots, r_q)$ there exists the single arc $(q, q') \in E$ and the single set $[\alpha_{q',m}, \mathrm{A}_{q',m}]$ $(m \in \{1, \ldots, r_{q'}\})$ of initial values, such that the inclusion $R_{(q,q')}([\beta_{q,h}, \mathrm{B}_{q,h}]) \subseteq [\alpha_{q',m}, \mathrm{A}_{q',m}]$ holds, where $R_{(q,q')}(\cdot) = R((q, q'), \cdot)$.

It should be noted that when the condition $\theta_{q,h} = \varTheta_{q,h} = 0$ holds, de facto we deal not with the continuous dynamics, but with usual switching. Besides, it is more correct to use denotation $((q, h), (q', m))$ for the elements of the set E. This denotation will be used in what follows.

The set H_0 has been called the set of 1-dimensional HA, since each dynamics is presented by a differential equation from the same variable, though the number the different dynamics in discrete states can be different. The main aim to define this set of HA has been to aggregate the discrete states of HA, and thus to simplify structure of the transition graph due to reduction the number of vertices.

Let $S^{in}_{q,h}$ and $S^{fin}_{q,h}$ be the maximal relatively to the inclusion relation sets that are defined by the following three axioms:

(i) $S^{in}_{q,h} \subseteq [\alpha_{q,h}, \mathrm{A}_{q,h}] \& S^{fin}_{q,h} \subseteq [\beta_{q,h}, \mathrm{B}_{q,h}]$;

(ii) $\theta_{q,h} = \varTheta_{q,h} = 0 \Rightarrow S^{in}_{q,h} = S^{fin}_{q,h}$;

(iii) $0 < \theta_{q,h} < \varTheta_{q,h} \Rightarrow (\forall x(t))(x(0) \in S^{in}_{q,h} \Rightarrow$

$$\Rightarrow (\exists t_0 \in [\theta_{q,h}, \varTheta_{q,h}])(x(t_0) \in S^{fin}_{q,h}) \& (\forall t \in [0, \varTheta_{q,h}])(x(t) \in X_q)) \&$$

$$\& (\forall b \in S^{fin}_{q,h})(\exists x(t))(x(0) \in S^{in}_{q,h} \& (\exists t_0 \in [\theta_{q,h}, \varTheta_{q,h}])(x(t_0) = b)).$$

It has been proved in [9] that each HA $\mathcal{H} \in \mathrm{H}_0$ can be reduced to equivalent model, such that the following two conditions hold:

Condition 1. The equalities

$$S_{q,h}^{in} = [\alpha_{q,h}, \mathrm{A}_{q,h}]$$

and

$$S_{q,h}^{fin} = [\beta_{q,h}, \mathrm{B}_{q,h}]$$

are true for all $q \in Q$ and $h = 1, \ldots, r_q$.

Condition 2. The equality

$$R_{((q,h),(q',m))}(S_{q,h}^{fin}) = S_{q',m}^{in}$$

is true for all $((q, h), (q', m)) \in E$.

In what follows it is supposed that the Conditions 1 and 2 hold for any considered HA.

3 Main Results

It is evident that different architectures for the system of on-line checking of faults in CPS can be offered. The main criteria of the efficiency for this system are the reliability, the scalability, and the minimal time for decision-making.

Due to these criteria, the best solution is the completely distributed system for on-line checking of faults in CPS. Thus, for each dynamical process, as well as for each switching its own controller can be associated.

It should be emphasized that we consider the controller as some discrete electronic device implemented on the base of the microprocessor and RAM.

Let us characterize these controllers for CPS presented by HA $\mathcal{H} \in \mathrm{H}_0$.

3.1 On-Line Checking of Continuous Dynamics

It is assumed that if any of physical processes in the analyzed CPS is not activated after obtaining the relevant input data, then the special physical device instantly blocks this process. Thus, we will deal with the situation when each physical process in the analyzed CPS is activated after obtaining the relevant input data.

It is also assumed that the controllers which are carrying out on-line checking of different dynamical processes in the analyzed CPS are different, and do not interact with each other in any way. Therefore, considering the HA $\mathcal{H} \in \mathrm{H}_0$ associated with the analyzed CPS, we conclude that the total number of controllers intended for on-line checking of different dynamical processes in the analyzed CPS does not exceed the integer $\sum\limits_{q \in Q} r_q$.

Now we define the controller

$$\mathcal{C}_{q,h} \;\; (q \in Q;\; h \in \{1, \ldots, r_q\}),$$

which for the fixed discrete state $q \in Q$ of HA $\mathcal{H} \in \mathrm{H}_0$ carries out on-line checking of the continuous dynamics for the analyzed CPS, under assumption that this dynamics is presented in the HA $\mathcal{H}$ by the differential equation

$$\dot{x} = f_{q,h}(x) \ , \tag{1}$$

where $f_{q,h}$ is, at least, some Lipschitz continuous function on the closed interval $[0, \Theta_{q,h}]$.

It should be noted that this assumption about the function $f_{q,h}$ holds for sufficiently wide class of CPS.

Applying the Euler method, we can transform the equation (1) into the finite-difference equation

$$x_{j+1} = x_j + f_{q,h}(x_j) \cdot \Delta t \ \ (j = 0, 1, \ldots), \tag{2}$$

where $\Delta t = L_{q,h}^{-1} \cdot \Theta_{q,h}$, and $L_{q,h}$ is some suitably chosen sufficiently large positive integer. It is also assumed that there exists positive integer $l_{q,h}$ $(l_{q,h} < L_{q,h})$, such that the identity $\theta_{q,h} = l_{q,h} \cdot \Delta t$ holds. This assumption does not restrict the reasoning, but simplifies the presentation.

Therefore, with each solution $x(t)$ of the differential equation (1) can be associated the sequence

$$x_0, x_1, \ldots \ \ (x_0 = x(0)), \tag{3}$$

calculated in accordance with the formula (2).

The controller $\mathcal{C}_{q,h}$ $(q \in Q; \ h \in \{1, \ldots, r_q\})$ consists of the two blocks, namely B_1 and B_2.

The block B_1 consists of two input channels, namely $i_{1,1}$ and $i_{1,2}$, and one output channel, namely o_1.

The input channel $i_{1,1}$ obtains from some sensor the information that the initial value for the analyzed physical process in CPS is x_0.

The input channel $i_{1,2}$ is a binary channel. It obtains through some sensor the information whether the analyzed physical process in CPS presented by the differential equation (1) in the HA is activated or is not activated.

It is assumed that the symbol 1 is associated with the situation that analyzed physical process in the analyzed CPS is activated, the symbol 0 is associated with the situation that this physical process is not activated, the impulse $0 \to 1$ activates the block B_1 and the impulse $1 \to 0$ deactivates this block.

As soon as the block B_1 is activated, it carries out calculation of the sequence (3) sequentially, symbol by symbol.

It is assumed that the symbol x_0 and each calculated symbol x_j $(j = 1, 2, \ldots)$ at once appears on the output channel o_1 of the block B_1.

The block B_2 consists of three input channels, namely $i_{2,1}$, $i_{2,2}$ and $i_{2,2}$, and one output channel, namely o_2.

The input channel $i_{2,1}$ is identical with the input channel $i_{1,2}$. Thus, the input channels $i_{2,1}$ and $i_{1,2}$ can be treated as the branching of the same line connected with the same sensor.

Similarly, to destination of the input channel $i_{1,2}$, the input channel $i_{2,1}$ activates the block B_2 by the impulse $0 \to 1$.

The input channel $i_{2,2}$ of the block B_2 is connected with the output channel o_1 of the block B_1.

The input channel $i_{2,3}$ of the block B_2 obtains from some sensor, symbol by symbol, the information that the analyzed physical process generates the sequence

$$y_0, y_1, \dots \ \ (y_0 = x_0)$$

of its output values.

The output channel o_2 of the block B_2 is a binary channel connected with the physical device $\mathcal{D}_{q,h}$ that can immediately deactivate and isolate the analyzed physical process in CPS.

It is assumed that the symbol 1 is associated with the situation when the device $\mathcal{D}_{q,h}$ must be activated and the symbol 0 is associated with the situation when this device is deactivated.

As soon as the block B_2 is activated, the value of the signal on its output channel o_2 is equal to 0.

When the block B_2 obtains the symbols x_j and y_j, respectively, on its input channels $i_{2,2}$ and $i_{2,3}$, where $j = 1, 2, \dots$, it carries out the following calculations.

The block B_2 computes the value

$$t_j = t_{j-1} + \varDelta t \ \ (t_0 = 0),$$

and checks whether the inequality

$$t_j \leq \varTheta_{q,h}$$

holds.

Let

$$t_j > \varTheta_{q,h}$$

and the value of the signal on the input channel $i_{2,1}$ is equal to 1. Then the signal 1 is generated on the output channel o_2 of the block B_2, and the block B_2 deactivates itself.

Let

$$t_j \leq \varTheta_{q,h}$$

and the value of the signal on the input channel $i_{2,1}$ is equal to 1. Then the block B_2 checks, whether the condition

$$y_j \in X_q$$

holds.

Suppose, that this condition is violated. Then the signal 1 is generated on the output channel o_2 of the block B_2, and the block B_2 deactivates itself.

Otherwise (i.e. when the condition $y_j \in X_q$ holds), the condition

$$|x_j - y_j| \leq \varepsilon$$

is checked, where ε is some sufficiently small properly chosen positive number.

If this condition is violated, then the signal 1 is generated on the output channel o_2 of the block B_2, and the block B_2 deactivates itself.

Let

$$t_j \leq \varTheta_{q,h}$$

and the impulse 1 → 0 is applied to the input channel $i_{2,1}$ of the block B_2. Then this block checks whether the inequality

$$t_j \geq \theta_{q,h}$$

holds.

If $t_j < \theta_{q,h}$ then the signal 1 is generated on the output channel o_2 of the block B_2, and the block B_2 deactivates itself.

Otherwise (i.e. when $t_j \geq \theta_{q,h}$), the block B_2 deactivates itself.

It is evident that the time spent by the block B_2 on the considered above calculations is insignificant in the comparison with the time spent by the block B_1 on its calculations. By this reason, the time spent by the block B_2 on the considered above calculations can be neglected at all.

Therefore, it can be assumed that the calculations of the block B_2 are carried out instantly.

The controller $\mathcal{C}_{q,h}$ $(q \in Q; h \in \{1, \ldots, r_q\})$ offered above can be characterized as follows.

Theorem 1. *It can be guaranteed that the controller*

$$\mathcal{C}_{q,h} \ \ (q \in Q;\ h \in \{1, \ldots, r_q\})$$

carries out correct on-line checking of the analyzed physical process in the analyzed CPS if and only if the equality

$$T_{B_1} = T_{B_2} \tag{4}$$

holds, where T_{B_1} is the time necessary for the block B_1 to calculate any value x_j $(j \in \{0, 1, \ldots, L_{q,h}\})$ and T_{B_2} is the time necessary for the block B_2 to obtain from some sensor any value y_j $(j \in \{0, 1, \ldots, L_{q,h}\})$.

Proof. Let us suppose that the equality (4) holds.

From the definition of the controller $\mathcal{C}_{q,h}$ $(q \in Q; h \in \{1, \ldots, r_q\})$ we get that if this controller is activated then on the input channels $i_{2,2}$ and $i_{2,3}$ of the block B_2 the signals x_j and y_j, associated to each other, are obtained in each instant of time.

Besides, from the definition of the block B_2 it follows that the signal 1 can be produced on its output channel o_2 if and only if this block is activated, and some fault in the analyzed physical process in the analyzed CPS reveals itself at the current instant of time. In this case the device $\mathcal{D}_{q,h}$ is activated, and the analyzed physical process in the analyzed CPS is deactivated and isolated.

Thus, it can be guaranteed that the controller $\mathcal{C}_{q,h}$ $(q \in Q; h \in \{1, \ldots, r_q\})$ carries out correct on-line checking of the analyzed physical process in the analyzed CPS.

Let us suppose that the equality (4) isn't met, i.e. the inequality

$$|T_{B_1} - T_{B_2}| > 0$$

holds.

From the definition of the controller $\mathcal{C}_{q,h}$ $(q \in Q; h \in \{1, \ldots, r_q\})$ it follows that if this controller is activated then there can exist some instant of time such that on the input channels $i_{2,2}$ and $i_{2,3}$ of the block B_2 are obtained the signals x_{j_1} and y_{j_2}, where $j_1 \neq j_2$. Starting from this instant of time the functioning of the controller $\mathcal{C}_{q,h}$ $(q \in Q; h \in \{1, \ldots, r_q\})$ can be incorrect.

Thus, there is no guarantee that the controller $\mathcal{C}_{q,h}$ $(q \in Q; h \in \{1, \ldots, r_q\})$ carries out correct on-line checking of the analyzed physical process in the analyzed CPS.

Q.E.D.

3.2 On-Line Checking of Switching

It is assumed that with each switching between dynamics in the analyzed CPS its own controller is associated, and different non-interacting with each other controllers are associated with different switching. Therefore, there is a one-to-one correspondence between non-interacting controllers intended for on-line checking of switching between dynamics in the analyzed CPS and the elements of the set E in the associated HA $\mathcal{H} \in \mathrm{H}_0$, i.e. the total number of these controllers is equal to $|E|$.

It is also assumed that for the analyzed CPS the time needed to carry out any switching between dynamics is some sufficiently small positive number τ. This assumption reflects the fact that in real systems switching are made not instantly, but with some delay.

Now we define the controller

$$\mathcal{C}_{((q,h),(q',m))} \ \ (q, q' \in Q;\ h \in \{1, \ldots, r_q\};\ m \in \{1, \ldots, r_{q'}\}),$$

intended for on-line checking of switching in the analyzed CPS, defined by the arc $((q,h),(q',h')) \in E$ in the associated HA $\mathcal{H} \in \mathrm{H}_0$.

The controller $\mathcal{C}_{((q,h),(q',m))}$ consists of three input channels i_1, i_2, i_3 and one output channel o.

The input channel i_1 of the controller $\mathcal{C}_{((q,h),(q',m))}$ is a binary channel, and through some sensor obtains the information whether the physical process in the analyzed CPS, associated with the dynamics $\dot{x} = f_{q,h}(x)$ in the HA $\mathcal{H}$, is activated or is not activated.

It is assumed that the symbol 1 is associated with the situation when the physical process in the analyzed CPS, associated with the dynamics $\dot{x} = f_{q,h}(x)$ in the HA $\mathcal{H}$, is activated, the symbol 0 is associated with the situation when this process is deactivated, and the impulse $1 \to 0$ activates the controller $\mathcal{C}_{((q,h),(q',m))}$.

The input channel i_2 of the controller $\mathcal{C}_{((q,h),(q',m))}$ is connected with the output channel of the block B_1 of the controller $\mathcal{C}_{q,h}$, which is intended for on-line checking of the dynamics $\dot{x} = f_{q,h}(x)$, and obtains, symbol by symbol, the sequence

$$x_0, x_1, \ldots, x_{t_{q,h}}$$

computed by this block.

The input channel i_3 of the controller $\mathcal{C}_{((q,h),(q',m))}$ through some sensor obtains, symbol by symbol, the values

$$y_0, y_1, \ldots, y_{t_{q,h}}$$

produced by the physical process in the analyzed CPS, associated with the dynamics $\dot{x} = f_{q,h}(x)$ in the HA $\mathcal{H}$.

The output channel o of the controller $\mathcal{C}_{((q,h),(q',m))}$ is a binary channel connected with the physical device $\mathcal{S}_{((q,h),(q',m))}$. This device carries out in the analyzed CPS the switching between the physical process associated with the dynamics $\dot{x} = f_{q,h}(x)$ in the HA $\mathcal{H}$ and the physical process associated with the dynamics $\dot{x} = f_{q',m}(x)$ in the HA $\mathcal{H}$.

It is assumed that the symbol 1 on the output channel o of the controller $\mathcal{C}_{((q,h),(q',m))}$ is associated with the situation when the device $\mathcal{S}_{((q,h),(q',m))}$ is activated, and the symbol 0 is associated with the situation when this physical device is deactivated.

It is also assumed that initially the value of the signal on the output channel o of the controller $\mathcal{C}_{((q,h),(q',m))}$ is equal to 1.

In the instance of time when the impulse $1 \to 0$ is applied to the input channel i_1, the values of the symbols on the input channels i_2 and i_3 are equal to $x_{t_{q,h}}$ and $y_{t_{q,h}}$ respectively, where $t_{q,h} \in [\theta_{q,h}, \Theta_{q,h}]$.

The controller $\mathcal{C}_{((q,h),(q',m))}$ is activated, and carries out checking of the truth value of the following condition

$$|x_{t_{q,h}} - y_{t_{q,h}}| \leq \varepsilon \& y_{t_{q,h}} \in [\beta_{q,h}, \mathrm{B}_{q,h}] \&$$

$$\& R(((q,h),(q',m)), y_{t_{q,h}}) \in [\alpha_{q',m}, \mathrm{A}_{q',m}], \tag{5}$$

where ε is some sufficiently small positive number designating the size of admissible absolute difference between the associated with each other the model and the real values of the analyzed physical process in the CPS.

If the condition (5) holds then the value of the signal on the output channel o of the controller $\mathcal{C}_{((q,h),(q',m))}$ remains be equal to 1, and a violation of this condition changes this value on 0.

The controller $\mathcal{C}_{((q,h),(q',m))}$ offered above can be characterized as follows.

Theorem 2. *It can be guaranteed that the controller*

$$\mathcal{C}_{((q,h),(q',m))} \ \ (q, q' \in Q; \ h \in \{1, \ldots, r_q\}; \ m \in \{1, \ldots, r_{q'}\})$$

carries out correct on-line checking of the switching in the analyzed CPS, defined by the arc $((q,h),(q',h')) \in E$ *in the HA* $\mathcal{H} \in \mathrm{H}_0$, *if and only if the inequality*

$$T_{|x-y|\leq\varepsilon} + T_{y\in[\beta_{q,h},B_{q,h}]} + T_R < \tau \qquad (6)$$

is true, where $T_{|x-y|\leq\varepsilon}$ *is the time necessary for checking the condition* $|x-y| \leq \varepsilon$, $T_{y\in[\beta_{q,h},B_{q,h}]}$ *is the time necessary for checking the condition* $y \in [\beta_{q,h}, B_{q,h}]$, T_R *is the total time necessary for calculating the value* $z = R(((q,h),(q',m)),y)$ *and checking the condition* $z \in [\alpha_{q',m}, A_{q',m}]$, *and* τ *is the time necessary for the physical device* $\mathcal{S}_{((q,h),(q',m))}$ *to carry out switching between dynamics in the analyzed CPS.*

Proof. Let us suppose that the inequality (6) holds.

From the definition of the controller $\mathcal{C}_{((q,h),(q',m))}$ we get that at the instance when this controller is activated, the symbols on its input channels i_2 and i_3 are equal to $x_{t_{q,h}}$ and $y_{t_{q,h}}$ respectively, where $t_{q,h} \in [\theta_{q,h}, \Theta_{q,h}]$, and the value of the signal on the output channel o of the controller $\mathcal{C}_{((q,h),(q',m))}$ is equal to 1.

Besides, from the definition of the controller $\mathcal{C}_{((q,h),(q',m))}$ it follows that the signal 0 can be produced on its output channel o if and only if this controller is activated, and some fault in the analyzed physical process in CPS reveals itself. In this case the physical device $\mathcal{S}_{((q,h),(q',m))}$ is deactivated.

Due to the inequality (6), the deactivation of the physical device $\mathcal{S}_{((q,h),(q',m))}$ is occurred in time, smaller than τ, and the analyzed switching in the analyzed CPS is blocked.

Thus, it can be guaranteed that the controller $\mathcal{C}_{((q,h),(q',m))}$ carries out correct on-line checking of the analyzed switching in the analyzed CPS.

Let us suppose that the inequality (6) is false, i.e. the inequality

$$T_{|x-y|\leq\varepsilon} + T_{y\in[\beta_{q,h},\mathrm{B}_{q,h}]} + T_R \geq \tau$$

holds.

From the definition of the controller $\mathcal{C}_{((q,h),(q',m))}$ it follows that it is possible such situation that some fault reveals itself on the controller $\mathcal{C}_{((q,h),(q',m))}$ on the expiration of time τ. In this case the physical device $\mathcal{S}_{((q,h),(q',m))}$ is deactivated later than in the analyzed CPS has occurred, perhaps incorrect, switching between the considered physical processes.

Thus, there is no guarantee that the controller $\mathcal{C}_{((q,h),(q',m))}$ carries out correct on-line checking of the analyzed switching in the analyzed CPS.

Q.E.D.

4 Conclusions

The given paper is a theoretic one. Its main aim consisted in the developing some structure of a completely distributed system intended for on-line monitoring and fault components isolation in CPS. The proposed system is developed on the model-based approach under the supposition that 1-dimensional HA of special type is used as the mathematical model for the analyzed CPS. The use for the analyzed CPS of different controllers for checking the dynamics of physical processes and for checking switching between dynamics, gave the possibility to establish the necessary and sufficient conditions guaranteeing correct on-line checking of faults in the analyzed CPS.

The detailed analysis of the structure of these controllers shows that the offered completely distributed system intended for on-line monitoring and fault components isolation in CPS can be easily generalized on the more general case of CPS, when multi-dimensional HA are used. To achieve this aim, it is sufficient to demand that the restrictions on the time spent by the controllers on their calculations that are similar to the restrictions that have been established in theorems 1 and 2 were carried out.

The main direction of further researches is the specification of the proposed general completely distributed system for on-line monitoring and fault components isolation in specific CPS.

References

1. Lee, E.A.: Cyber physical systems: design challenges. In: Proceedings of the 11$^{\text{th}}$ IEEE International Symposium on Object Oriented Real-Time Distributed Computing, pp. 363–369. Orlando, FL, USA (2008)
2. Gunes, V., Peter, S., Givargis, T., and Vahid, F.: A survey on concepts, applications, and challenges in cyber-physical systems. KSII Transactions on Internet and Information Systems, **8**(12), 4242–4268 (2014)
3. Liu, Y., Peng, Y., Wang, B., Yao, S., and Liu, Z.: Review on cyber-physical systems. IEEE/CAA Journal of Automatica Sinica, **4**(1), 27–40 (2017)
4. Asadollah, S.A., Inam, H., and Hansson, H.: A survey on testing for cyber physical system. In: Proceedings of IFIP International Conference ”Testing Software and Systems”, pp. 194–207. Sharjah and Dubai, United Arab Emirates (2015)
5. Gao, Z., Ding, S.X., and Cecati C.: Real-time fault diagnosis and fault-tolerant control. IEEE Transactions on Industrial Electronics, **62**(6), 3752–3756 (2015)
6. Severson, K., Chaiwatanodom P., and Braatz, R.D.: Perspectives on process monitoring of industrial systems. Annual Reviews in Control, **42**, 190–200 (2016)
7. Henzinger, T.A.: The theory of hybrid automata. In: Proceedings of the 11$^{\text{th}}$ Annual IEEE Symposium on Logic in Computer Science, pp. 278–292. New Brunswick, NJ, USA (1996)
8. Lygeros, J.: Lecture notes on hybrid systems. University of Cambridge, Cambridge (2004). https://fenix.tecnico.ulisboa.pt/downloadFile/3779579688470/lygeros.pdf.
9. Skobelev, V.V., and Skobelev, V.G.: Some problems of analysis of hybrid automata. Cybernetics and Systems Analysis, **54**(4), 517–526 (2018)