UDC 681.518.5

AUTOMATIC DIAGNOSIS METHOD FOR SCADA OPERABILITY

O.I. Syrotkina

State Higher Educational Institution "National Mining University", 49600, Dnipropetrovs'k,
Karl Marx Av., 19, tel.: (0562) 471555, e-mail: syrotkina@yandex.ua

Пропонується до розгляду методика автоматичної діагностики працездатності SCADA системи в режимі реального часу за зміною інформаційно-діагностичних ознак контрольованих параметрів у процесі проходження потоків даних за структурними одиницями і рівнями ієрархії SCADA. В рамках методики були сформульовані необхідні і достатні критерії виявлення відмови в системі, необхідні і достатні критерії розмежування незалежних і вторинних відмов на підставі логіки функціонування SCADA з урахуванням причинно-наслідкових зв'язків між подіями та характерних особливостей кожного рівня ієрархії системи.

Для наведеного на малюнку прикладу структурної схеми SCADA системи показана діаграма конфігураційної прив'язки структурних елементів системи з метою локалізації відмов. На базі k-значної логіки Е. Поста з використанням характеристичних функцій першого роду були виведені аналітичні залежності виявлення і локалізації відмов у системі, визначення незалежних відмов.

Використання методики автоматичного виявлення відмов у роботі SCADA дозволяє розробляти підсистеми автовідновлення працездатності системи після оборотних відмов у режимі реального часу.

Ключові слова: автоматична діагностика відмов, інформаційно-діагностичні ознаки, функція виявлення відмови в системі, k-значна логіка.

Предлагается к рассмотрению методика автоматической диагностики работоспособности SCADA системы в режиме реального времени по изменению информационно-диагностических признаков контролируемых параметров в процессе прохождения потоков данных по структурным единицам и уровням иерархии SCADA. В рамках методики были сформулированы необходимые и достаточные критерии обнаружения отказа в системе, необходимые и достаточные критерии разграничения независимых и вторичных отказов на основе логики функционирования SCADA с учетом причинно-следственных связей между событиями и характерных особенностей каждого уровня иерархии системы.

Для приведенного на рисунке примера структурной схемы SCADA системы показана диаграмма конфигурационной привязки структурных элементов системы с целью локализации отказов. На базе k-значной логики Э. Поста с использованием характеристических функций первого рода были выведены аналитические зависимости обнаружения и локализации отказов в системе, определения независимых отказов.

Использование методики автоматического обнаружения отказов в работе SCADA позволяет разрабатывать подсистемы автовосстановления работоспособности системы после обратимых отказов в режиме реального времени.

Ключевые слова: автоматическая диагностика отказов, информационно-диагностические признаки, функция обнаружения отказа в системе, k-значная логика.

Automatic diagnosis method for SCADA operability in real time by changing information and diagnostic features of controlled parameters during propagation of information flows between SCADA hierarchy levels is proposed to consider in this paper. Necessary and sufficient fault detection criteria in the system, necessary and sufficient criteria of differentiation of independent and secondary failures based on SCADA functioning logic taking into account cause-effect relations between events and features of the each system hierarchy level were formed in this method.

Configuration binding diagram of the system structure elements is shown to localize the failure for the given example. The analytical dependencies were deduced to detect and localize the failure and define independent failures based on Post's k-valued logic by using the characteristic functions of the first kind.

The use of automatic failure detection method in SCADA work allows us to develop auto recovery subsystems of system operability after reversible failures in real time.

Key words: automatic failure diagnosis, information and diagnostic features, failure detection function in the system, k-valued logic.

Introduction. At present, SCADA (Supervisory Control And Data Acquisition) systems are actively implemented to increase the efficiency of enterprises in oil and gas industry at every stage, beginning from the prospecting and mining development, well-boring and oil production to the fuel processing and transportation. This class of systems is widely used to control the technological parameters of drilling mode; to monitor the technical condition of equipment and aggregates; to control the production control systems; to ensure the alarm signals and messages in case of emergency state etc. [1,2]. Among many well-known SCADA, there are the most common systems such as SIMATIC WinCC from Siemens [3], Wonderware InTouch HMI from Invensys [4], Genesis32 from Iconics [5], TRACE MODE from AdAstrA Research Group, Ltd. [6] etc. There are increased requirements to ensure reliability and fault tolerance for mission-critical SCADA real time systems working in oil and gas industry [7,8]. Therefore, one of the ways to solve this complex task is the creation of the operability diagnosis methodology for such real time systems [9,10].

Analysis of current investigations in SCADA diagnosis area. SCADA system is a distributed multi-level and multi-tasking hardware and software complex. It works in real time mode, and it is complex, dynamic and difficult to formalize diagnosis object with changeable structure and functionality during the “life-cycle” process [1,2,7,8]. As a whole, SCADA reliability and validity of its data at each hierarchy level depend on the operability of backbone nodes, data transmission channels, peripheral equipment and software conformity.

Today’s modern SCADA systems have built-in functions of automatic low-level diagnostics with the ability to display diagnostic messages about faults in the system. Unfortunately, modern SCADA diagnostic methods are usually oriented for manual disaster recovery of the system by using maintenance personnel. The analysis of diagnosis subsystems for such SCADA as WinCC (Siemens, Germany) [3], SPPA-T3000 (Siemens, Germany) [11] allows us to make a conclusion about their automatic operability support by using “watchdog timers” or/and “hot” backup of backbone nodes with automatic switching to backup equipment in case of failure.

Emphasis of previously unresolved parts of the general issue. However, it is possible to develop and apply an automatic real time self-recovery subsystem in case of functionality loss of the individual structural units or the entire system caused by reversible failures that do not lead to malfunction of equipment, but it can cause a full or partial software failure [10, 12].

The purpose of this paper is to consider the method of detection and localization failure type by changing information and diagnostic features of technological control object parameters during propagation of information flows between SCADA hierarchy levels.

The main research. Let’s consider a general example of SCADA structure fragment (see Fig. 1) for the failure diagnosis during propagation of information flows between SCADA structure elements and hierarchy levels.

For the timestamp t, the set of technological control object parameters (TCOP) is measured by using Smart Sensors SS_i and it is registered in specialized controllers called Data Collection Nodes DCN_j.

$$X(t) = \left\{x_1(t), x_2(t), \ldots, x_i(t), \ldots x_{n(X)}(t)\right\}.$$

The program process A_j works on the DCN_j and it provides reading $x_i(t)$ from SS_i using Data Transfer Channel Ch_m and the port P_m with DCN_j. Server S_1 joined with DCN_j as the Wide Area Network (WAN) by using Data Transfer Channels $Ch_{j,1}$ with corresponding ports $P_{S_1,j}$ and P_{j,S_1}. Processes B_j and C are responsible for the data transfer between DCN_j and server S_1 by using Data Transfer Protocol DTP_j. There are two databases (DB) on the server S_1. First of them is a real time database DB_1 and the other is an archive database DB_2. Recording the data in DB_1 and DB_2 are performed by using the program processes D and E. SCADA operating personnel work with the server S_1 through the interface of Automated Work Station places AWS_η.

SCADA structure is represented in the form of hierarchy levels that correspond to possible failure localization levels: $L = \{1, 2, \ldots n(L)\}$,

where $n(L) = |L|$ is a count of hierarchy levels.

Accepting the following:

- L_1 is a set of system hierarchy levels that corresponds to appreciate backbone nodes where it can be realized access from the system to the parameter $x_i(t)$;

- L_2 is a set of system hierarchy levels that corresponds to appreciate Data Transfer Channels.

Therefore, we have following set for SCADA structure (see Fig. 1): $L=\{1,2,3,4,5,6,\}$, where $l=1$ is a Technological Control Object (TCO); $l=2$ is Smart Sensors (SS); $l=3$ is Data Transfer Channels (DTC) from SS to the next hierarchy level; $l=4$ is Data Collection Nodes (DCN); $l=5$ is Data Transfer Channels from DCN to the next hierarchy level; $l=6$ is a SCADA server.

$$L_1 \subset L,\ L_1=\{2,4,6\},$$
$$L_2 \subset L,\ L_2=\{3,5\}.$$

According to the levels of System Failure Types (SFT) $l \in L_1$, the controlled parameter $x_i(t)$ can be found in one of the following states:

– parameter value with timestamp t on the hierarchy level l is registered and it is valid (V);

– parameter value with timestamp t on the hierarchy level l is registered and it is invalid (I);

– parameter value with timestamp t on the hierarchy level l is absent (A).

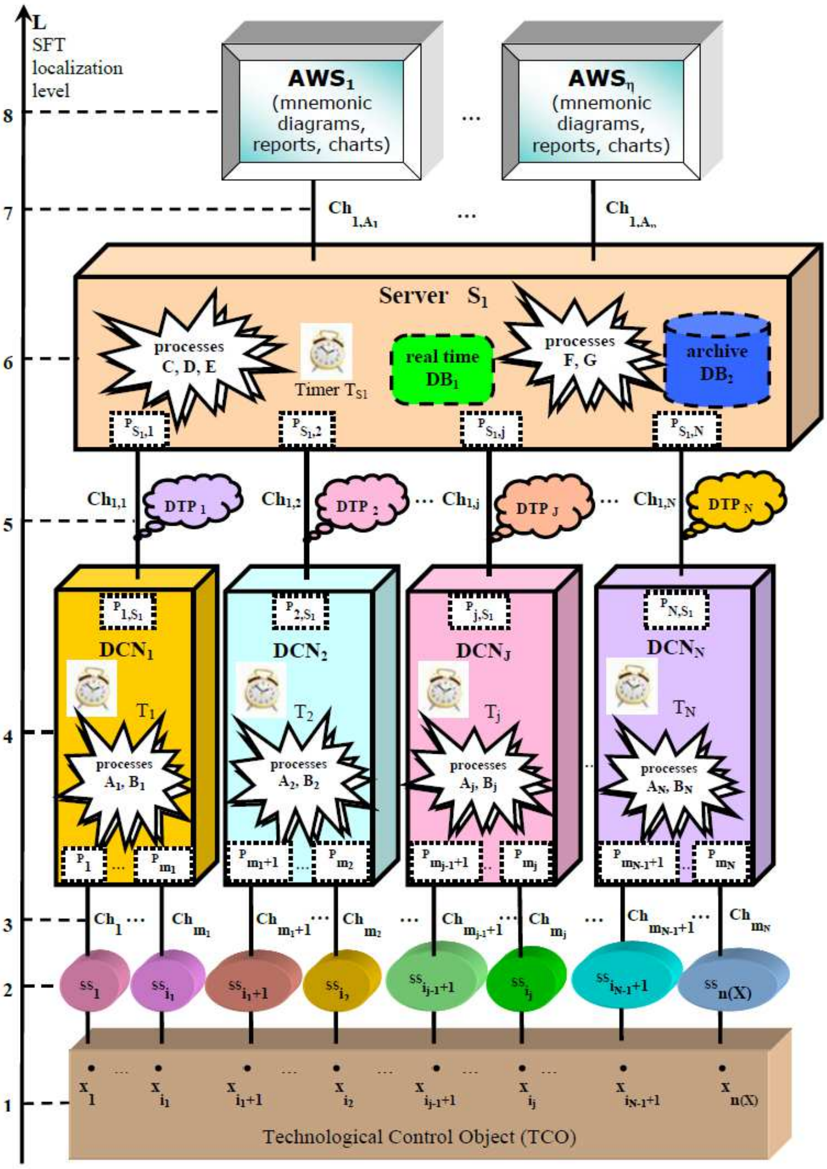

Figure 1 - Example of SCADA structure

For SCADA levels $l \in L_2$, let's define possible variants of receiving/transmitting process completion of the set $X(t)$ through Data Transfer Channels Ch_m:

– receiving/transmitting of the parameter $x_i(t)$ on the hierarchy level l is completed and it is valid (V);

– receiving/transmitting of the parameter $x_i(t)$ on the hierarchy level l is completed, but it is invalid (I);

– receiving/transmitting of the parameter $x_i(t)$ on the hierarchy level l is absent or it is not completed during configurable timeout of receiving/transmitting process completion (A).

Let's form the diagnostic matrix $D(t)$, that presents the validity of controlled parameters for $1 < l \le l(S_1)$ SCADA hierarchy levels. We define $l(S_1)$ as a server level.

We will use Post's three-valued logic P_3 [13] when forming and analyzing the matrix. Let's define the elements $d_{iL,iC}(t)$ of the matrix $D(t)$ on the three-valued set $E_3 = \{0,1,2\}$, that corresponds to the states {A,I,V} for controlled parameter $x_i(t)$, where $l \in L_1$ or we have $\{A, I, V\}$ forms of receiving/transmitting process completion, where $l \in L_2$.

$$\begin{cases} D(t) = [d_{iL,iC}(t)] \\ d_{iL,iC}(t) \in E_3 \\ iL = l(S_1) + 1 - l, \;\; 1 < l \le l(S_1) \\ 1 \le iC \le n(X). \end{cases}.$$

Let's define the distribution of controlled parameters in DCNs (see Fig. 1) on a non-decreasing sequence of positive integers I_x:

$I_x = i_1, i_2, \ldots, i_j, \ldots, i_N$, where j is an element position of the sequence member I_x. It corresponds to the DCN sequence number; N is a count of DCN; $I_N = n(X)$ is a count of controlled parameters; $(i_j - i_{j-1})$ is a count of controlled parameters connected to the DCN_j.

The other non-decreasing sequence of positive integers M_k defines the distribution of Data Transfer Channels through DCNs from SS (see Fig.1), $M_k = m_1, m_2, \ldots m_j, \ldots m_N$, where j is an element position of the sequence member M_k. It corresponds to the DCN sequence number; N is a count of DCN; m_N is a count of Data Transfer Channels from SS to DCN; $(m_j - m_{j-1})$ is a count of Data Transfer Channels from SS, connected to DCN_j.

We define the distribution of controlled parameters through the Data Transfer Channels from SS to DCN on a non-decreasing sequence of positive integers K_X, $K_X = k_1, k_2, \ldots, k_\mu, \ldots, k_{m_N}$, where μ is an element position of the sequence member K_X. It corresponds to the sequence number of the Data Transfer Channels from SS to DCN Ch_μ; N is a count of DCNs; m_N is a count of Data Transfer Channels from SS to DCNs; $(k_\mu - k_{\mu-1})$ is a count of controlled parameters. They are configured to transfer data through the DTC Ch_μ.

The configuration diagram of the TCO controlled parameters X through the Data Transfer Channels Ch and the Data Collection Nodes is shown in Fig. 2.

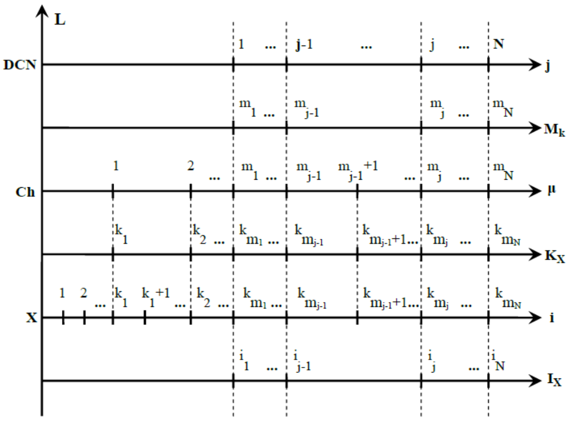
L
DCN
1 … j-1 … j … N
j
m1 … mj-1 mj … mN
Mk
Ch
1 2 … m1 … mj-1 mj-1+1 … mj … mN
μ
k1 k2 … km1 … kmj-1 kmj-1+1… kmj … kmN
KX
X
1 2 … k1 k1+1 … k2 … km1 … kmj-1 kmj-1+1… kmj … kmN
i
i1 … ij-1 ij … iN
IX

Figure 2. The configuration diagram of the TCO controlled parameters through the Data Transfer Channels and the Data Collection Nodes of SCADA

According to this diagram (see Fig. 2), there is the structure of the diagnostic matrix D(t), taking into account the distribution of controlled parameters through the DCNs, as follows:

$$D = \begin{array}{c} \left[\begin{array}{ccccccc} d_{1,1} \cdots d_{1,i_1} & d_{1,i_1+1} \cdots d_{1,i_2} & \cdots & d_{1,i_{j-1}+1} \cdots d_{1,i_j} & \cdots & d_{1,i_{N-1}+1} \cdots d_{1,i_N} \\ d_{2,1} \cdots d_{2,i_1} & d_{2,i_1+1} \cdots d_{2,i_2} & \cdots & d_{2,i_{j-1}+1} \cdots d_{2,i_j} & \cdots & d_{2,i_{N-1}+1} \cdots d_{2,i_N} \\ d_{3,1} \cdots d_{3,i_1} & d_{3,i_1+1} \cdots d_{3,i_2} & \cdots & d_{3,i_{j-1}+1} \cdots d_{3,i_j} & \cdots & d_{3,i_{N-1}+1} \cdots d_{3,i_N} \\ d_{4,1} \cdots d_{4,i_1} & d_{4,i_1+1} \cdots d_{4,i_2} & \cdots & d_{4,i_{j-1}+1} \cdots d_{4,i_j} & \cdots & d_{4,i_{N-1}+1} \cdots d_{4,i_N} \\ \underbrace{d_{5,1} \cdots d_{5,i_1}}_{УСД_1} & \underbrace{d_{5,i_1+1} \cdots d_{5,i_2}}_{УСД_2} & \cdots & \underbrace{d_{5,i_{j-1}+1} \cdots d_{5,i_j}}_{УСД_j} & \cdots & \underbrace{d_{5,i_{N-1}+1} \cdots d_{5,i_N}}_{УСД_N} \end{array}\right] \end{array} \begin{array}{l} l = l(S_1) = 6 \\ l = 5 \\ l = 4 \\ l = 3 \\ l = 2 \\ \\ \end{array}$$

Similarly, there is the structure of the diagnostic matrix D(t), taking into account the distribution of controlled parameters through the Data Transfer Channels, as follows:

$$D=\left[\begin{array}{ccccccc} d_{11}\cdots d_{1k_1} & d_{1,k_1+1}\cdots d_{1k_2} & \cdots & d_{1,k_{m_1-1}+1}\cdots d_{1,k_{m_1}} & \cdots & d_{1,k_{m_N-1}+1}\cdots d_{1,k_{m_N}} \\ d_{21}\cdots d_{2k_1} & d_{2,k_1+1}\cdots d_{2k_2} & \cdots & d_{2,k_{m_1-1}+1}\cdots d_{2,k_{m_1}} & \cdots & d_{2,k_{m_N-1}+1}\cdots d_{2,k_{m_N}} \\ d_{31}\cdots d_{3k_1} & d_{3,k_1+1}\cdots d_{3k_2} & \cdots & d_{3,k_{m_1-1}+1}\cdots d_{3,k_{m_1}} & \cdots & d_{3,k_{m_N-1}+1}\cdots d_{3,k_{m_N}} \\ d_{41}\cdots d_{4k_1} & d_{4,k_1+1}\cdots d_{4k_2} & \cdots & d_{4,k_{m_1-1}+1}\cdots d_{4,k_{m_1}} & \cdots & d_{4,k_{m_N-1}+1}\cdots d_{4,k_{m_N}} \\ d_{51}\cdots d_{5k_1} & d_{5,k_1+1}\cdots d_{5k_2} & \cdots & d_{5,k_{m_1-1}+1}\cdots d_{5,k_{m_1}} & \cdots & d_{5,k_{m_N-1}+1}\cdots d_{5,k_{m_N}} \end{array}\right]\begin{array}{l} l=6 \\ l=5 \\ l=4 \\ l=3 \\ l=2 \end{array}$$

$$\underbrace{\underbrace{\qquad\quad}_{Ch_1}\;\underbrace{\qquad\quad}_{Ch_2}\cdots\underbrace{\qquad\quad}_{Ch_{m_1}}}_{УСД_1}\cdots\underbrace{\qquad\quad}_{Ch_{m_N}}$$

Thus, the coordinates (iL,iC) of element $(d_{iL,iC})$ of diagnostic matrix D(t) are strictly tied to SCADA structural elements.

We apply the elementary function φ_e of k-valued logic to analyze the diagnostic matrix D(t). It is a characteristic function of the first kind of value e [13, 14]. We have:

$$\phi_e(x)=\begin{cases}1, & x=e,\ \ e\in E_k\\ 0, & x\neq e,\ \ e\in E_k\ .\\ E_k=\{0,1,k-1\}\end{cases} \tag{1}$$

Let's define the diagnostic features for failure detection:

– the sufficient diagnostic feature of failure absence for a SCADA structural element with the coordinates (iL,iC) and for timestamp t is $\varphi_2(d_{iL,iC}(t))=1$, where φ_2 is the characteristic function of the first kind (1);

– the necessary, but not sufficient feature of failure detection for a SCADA structural element with the coordinates (iL,iC) and for timestamp t is $\neg\varphi_2(d_{iL,iC}(t))$;

– the necessary, but not sufficient feature of failure detection due to absence the TCO controlled parameter on the system hierarchy level, that corresponds to the backbone nodes or due to absence the transmitting/receiving process on the system hierarchy level, that corresponds to the Data Transmission Channels for SCADA structural element with the coordinates (iL,iC) and for timestamp t is $\varphi_0(d_{iL,iC}(t))=1$, where ϕ_0 is the characteristic function of the first kind (1);

– the necessary, but not sufficient feature of failure detection due to invalidity the TCO controlled parameter on the system hierarchy level, that corresponds to the backbone nodes, or due to invalidity the transmitting/receiving process on the system hierarchy level, that corresponds to the Data Transmission Channels for SCADA structural element with the coordinates (iL,iC) and for timestamp t is $\varphi_1(d_{iL,iC}(t))=1$, where ϕ_1 is the characteristic function of the first kind (1).

The count of the diagnostic features $\varphi_0(d_{iL,iC}(t))$ and $\varphi_1(d_{iL,iC}(t))$ for the row iL of the diagnostic matrix D(t) is determined by using follows formulas:

$$n_{\varphi_0}(iL,1,i_N,t)=\sum_{iC=1}^{i_N}\varphi_0(d_{iL,iC}(t)),$$

$$n_{\phi_1}(iL,1,i_N,t)=\sum_{iC=1}^{i_N}\phi_1(d_{iL,iC}(t))\,.$$

The total count of diagnostic features for failure detection $\neg\varphi_2(d_{iL,iC}(t))$ for the row il of the diagnostic matrix D(t) is determined as follows:

$$n_{\overline{\phi_2}}(iL,1,i_N,t)=n_{\phi_0}(iL,1,i_N,t)+n_{\phi_1}(iL,1,i_N,t)\,.$$

To analyze the diagnostic matrix D(t), we might argue, that the all of the SCADA functional elements, that are involved in propagation of TCO controlled parameters from SS to the server are worked without failures on the timestamp t. So, for the first row (iL=1) of the matrix D(t), that corresponds to the server hierarchy level $l(S_1)$, we have:

$$\mathop{\&}_{iC=1}^{i_N}\phi_2(d_{1,iC}(t))=1\,.$$

In general, there is the failure detection function in the system, based on diagnostic matrix D(t) analysis as follows:

$$g_2(iL,\alpha,\beta,t)=\neg(\mathop{\&}_{iC=\alpha}^{\beta}\varphi_2(d_{iL,iC}(t))),$$

where α and β take values on the scales of the configuration diagram TCO controlled parameters (see Fig. 2) depending on SCADA hierarchy levels il.

It should be noted that, nether diagnostic feature for failure detection $\neg\varphi_2(d_{iL,iC}(t))$ nor function for failure detection in SCADA $g_2(iL,\alpha,\beta,t)$ discerns independent and secondary failure.

It is needed the additional diagnostic criteria to discern the independent and secondary failures on the hierarchy levels $l>l_{\min}$. They will be examined below.

Thus, for the current stage of matrix analysis D(t), it is possible to argue the following:

– the absence of failure detection on the certain SCADA hierarchy level is sufficient condition for the failure absence on this hierarchy level;

– the availability of failure detection on the hierarchy level $l_{\min}$ is sufficient condition for the appearance of independent failures. Thus, all of the diagnostic features for failure detection refer to the independent failures, because of the information flow direction during the automatic data collection from upper to lower hierarchy levels;

– the count of independent failures through the level of Smart Sensors $(l_{\min} = 2)$ is equal to the count of diagnostic features for failure detection;

– it is needed the additional analysis of diagnostic matrix D(t) to define the count of failures on the some upper hierarchy level $l_{\min} > 2$, because of the different diagnostic features can be referred to the same failure;

– the availability of the diagnostic feature for failure detection on the hierarchy level $l > l_{\min}$ for $l \in L_1$ is necessary but not sufficient condition to detect the independent failure on the upper hierarchy level. Thus, it is needed the additional criteria to determine the diagnostic feature as a secondary or independent failure;

– the absence of the detection of the independent failures on the hierarchy level $l > l_{\min}$ is the sufficient condition of absence oa independent failures on the current hierarchy level;

– it is needed the additional analysis of the diagnostic matrix D(t) to define the count of independent failures on the certain hierarchy level $l > l_{\min}$, because of the different diagnostic features can be referred to the same failure.

Let's define the upper SCADA hierarchy level $l_{\min}$ for diagnostic matrix D(t) using the following formula:

$$\begin{aligned} iL_{\min} := (g_2(1,1,i_N,t))?\\ ((g_2(2,1,i_N,t))?\\ ((g_2(3,1,i_N,t))?\\ ((g_2(4,1,i_N,t))?\\ ((g_2(5,1,i_N,t))?5:4):3):2):1):0. \end{aligned}$$

If $iL_{\min} = 0$, then there are no failures detected in the system for the timestamp t , else we can determine the upper level of failure detection using the following formula:

$$l_{\min} = l(S_1) + 1 - iL_{\min}.$$

If $l_{\min} < l(S_1)$, then we should define remaining SCADA hierarchy levels $l_{\min} < l \le l(S_1)$. It is possible to determine the failure detection for these hierarchy levels (they are not depended of previous hierarchy levels) by analyzing the current matrix D(t).

Let's consider the algorithm of localization of independent failures. The upper level of failure detection in SCADA refers to the backbone nodes $l_{\min} \in L_1$.

According to SCADA functioning logic, the increasing count of diagnostic features for failure detection, compared to a lower level of system $l_{\min} \le l_h \in L_1$, is the necessary but not sufficient criteria η of existence of independent failures. As we know, low hierarchy levels $l_{\min} < l_{h+1} \in L_1$ also refer to the backbone nodes.

$$\begin{cases} l_h = l_{\min} + 2 \times h \le l(S_1), \quad h = 1, 2, \ldots \\ iL_h = l(S_1) + 1 - l_h \\ n_{\overline{\varphi_2}}(iL_h, 1, i_N, t) = n_{\varphi_0}(iL_h, 1, i_N, t) + n_{\varphi_1}(iL_h, 1, i_N, t). \end{cases} \qquad (2)$$

If the count of diagnostic features of the lower hierarchy level $l_{h+1} \in L_1$ (2) is increased, compared to a lower level of system $l_h \in L_1$, then we made a conclusion about the performance of needed condition of the existence of independent failures on the SCADA hierarchy level l_{h+1}.

$$\begin{aligned} \eta(iL_{h+1}) = (n_0(iL_{h+1},1,i_N,t) - n_0(iL_h,1,i_N,t) > 0) \vee \\ \vee (n_1(iL_{h+1},1,i_N,t) - n_1(iL_h,1,i_N,t) > 0). \end{aligned}$$

If $\eta(iL_{h+1}) = 1$, then we compute the count of diagnostic features to detect the independent failures on the SCADA hierarchy level $l_{h+1} \in L_1$.

To do this, let's show the function of independent failure diagnostic feature detection $f_1(x, y)$ in a tabular format (see Tab. 1). This failure can be detected using controllable parameter state during its transmission on the next SCADA hierarchy level. Where: x is a controllable parameter state on the previous hierarchy level $l_h \in L_1$; y is a controllable parameter state on the next hierarchy level $l_{h+1} \in L_1$; $f_1(x, y) = 1$ is necessary, but not sufficient condition of diagnostic feature existence to detect the independent failure; $f_1(x, y) = 0$ is necessary, but not sufficient condition of diagnostic feature absence to detect the independent failure.

There is the following polynomial for this function $f_1(x, y)$:

$$f_1(x,y)=(2xy-2x^2-2x^2y+2xy^2)\pmod 3. \quad (3)$$

Table 1 - The function of independent failure diagnostic feature detection in tabular format

x	0	0	0	1	1	1	2	2	2
y	0	1	2	0	1	2	0	1	2
$f_1(x,y)$	0	0	0	1	0	0	1	1	0

Let's determine the count of diagnostic features for detection of independent failures on the hierarchy level $l_{h+1}\in L_1$, $l_{\min}<l_{h+1}\le l(S_1)$ based on polynomial function $f_1(x,y)$ (3).

$$n_{f_1}(iL,1,i_N,t)=\sum_{iC=1}^{i_N} f_1(d_{iL+2,iC}(t),d_{iL,iC}(t)).$$

If $n_{f_1}(iL,1,i_N,t)=0$, then this criterion is a sufficient condition, that no independent failures have been detected on the hierarchy level iL.

If $n_{f_1}(iL,1,i_N,t)>0$, then this criterion is a necessary, but not sufficient condition of detection of independent failures. We need to determine the dependence of these diagnostic features from previous hierarchy level to make a final diagnosis. Furthermore, these diagnostic features should correspond to the Data Transmission Channels taking into account a state of receiving/transmitting process completion.

We present the function $f_2(x,y,z)$ in a tabular format (see Tab. 2) to determine the failure diagnostic feature during transmission of TCO controlled parameter through the system hierarchy levels taking into account a state of receiving/transmitting process completion between neighboring levels. Where: x is a controlled parameter state on the transmitting hierarchy level $l_h\in L_1$; y is a state of the receiving/transmitting process completion on the hierarchy level $l\in L_2$; z is a controlled parameter state on the receiving hierarchy level $l_{h+1}\in L_1$; $f_2(x,y,z)=1$ is necessary, but not sufficient condition of diagnostic feature existence to detect the independent failure; $f_2(x,y,z)=0$ is a sufficient condition of diagnostic feature absence to detect the independent failure.

There is the following polynomial for this function $f_2(x,y,z)$:

$$\begin{aligned}f_2(x,y,z)=(&2xyz-2x^2yz-2xy^2z-xyz^2+x^2y^2+\\+&2x^2y^2z+x^2yz^2+xy^2z^2-2x^2y^2z^2)\pmod 3.\end{aligned} \quad (4)$$

We determine the count of diagnostic features for detection of independent failures on the hierarchy level $l_{h+1}\in L_1$, $l_{\min}<l_{h+1}\le l(S_1)$ taking into account a state of receiving/transmitting process completion based on polynomial function $f_2(x,y,z)$ (4).

$$n_{f_2}(iL,1,i_N,t)=\sum_{iC=1}^{i_N} f_2(d_{iL+2,iC}(t),d_{iL+1,iC}(t),d_{iL,iC}(t)).$$

If $n_{f2}(iL,1,i_N,t)=0$, then this criterion is a sufficient condition, that no independent failures have been detected on the hierarchy level iL.

If $n_{f_2}(iL,1,i_N,t)>0$, then this criterion is a sufficient condition of detection of independent failures.

Table 2 - The function of independent failure diagnostic feature detection levels taking into account a state of receiving/transmitting process completion in tabular format

№ п/п	x	y	z	$f_2(x,y,z)$	№ п/п	x	y	z	$f_2(x,y,z)$
1	0	0	0	0	15	1	1	2	0
2	0	0	1	0	16	1	2	0	1
3	0	0	2	0	17	1	2	1	0
4	0	1	0	0	18	1	2	2	0
5	0	1	1	0	19	2	0	0	0
6	0	1	2	0	20	2	0	1	0
7	0	2	0	0	21	2	0	2	0
8	0	2	1	0	22	2	1	0	1
9	0	2	2	0	23	2	1	1	0
10	1	0	0	0	24	2	1	2	0
11	1	0	1	0	25	2	2	0	1
12	1	0	2	0	26	2	2	1	1
13	1	1	0	1	27	2	2	2	0
14	1	1	1	0					

Let's form the matrix row of markers of independent failures $\Lambda(t)$ for the hierarchy level iL:

$$\begin{cases}\Lambda(t)=[\lambda_{iL,iC}(t)]\\ \lambda_{iL,iC}(t)=f_2(d_{iL+2,iC}(t),d_{iL+1,iC}(t),d_{iL,iC}(t)).\end{cases}$$

The count of detection of independent failures is computed by using the following formulas:

$$n^*_{\phi_0}(iL,1,i_N,t)=\sum_{iC=1}^{i_N}(\lambda_{iL,iC}(t)\,\&\,\phi_0(d_{iL,iC}(t))),$$

$$n^*_{\phi_1}(iL,1,i_N,t)=\sum_{iC=1}^{i_N}(\lambda_{iL,iC}(t)\,\&\,\phi_1(d_{iL,iC}(t))),$$

$$n^*_{\neg\phi_2}(iL,1,i_N,t)=n_{f_4}(iL,1,i_N,t)=\sum_{iC=1}^{i_N}\lambda_{iL,iC}(t).$$

CONCLUSIONS

The method of automatic diagnosis of SCADA failures by changing the information and diagnostic features of TCO controlled parameters during propagation of information flows between SCADA hierarchy levels has been considered in this paper.

This method has been developed by using Post’s three-valued logic P_3. It allows to perform an automatic detection and localization of independent failures by using information and diagnostic features based on SCADA functionality logic taking into account cause-effect relations between events. The method allows to perform detection and localization of independent and secondary failures in SCADA using appropriate necessary and sufficient criteria. These criteria can be defined taking into account the characteristic features for each system hierarchy level.

So, in this method:

– the configuration binding of SCADA structural elements has been designed to localize the failure in the system;

– the diagnostic features for failure detection have been formed and failure detection function has been deduced for the SCADA structural element;

– the criteria of independent failure detection have been determined. Furthermore, the analytical dependencies have been derived to detect the independent failure for the SCADA structural element.

Further development of this method is forming of criteria of diagnostic feature correspondence to independence failures taking into account characteristic features for each SCADA hierarchy level.

In future, the usage of this method for automatic failure detection during SCADA work allows you to realize auto-recovery for system operability in real time after reversible failures.

1. Ozhygin M.V. The purpose, structure and main functions of SCADA systems [Electronic resource]/ M.V. Ozhygin// VOTUM Ltd. – 2010. – Access mode to journal: http: //www.votum.if.ua/uk/publications/scada.htm 2. Technical Manual. Supervisory Control and Data Acquisition (SCADA) Systems for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities [Electronic resource]. – Washington: Department of the Army, TM 5-601. – 2006. – Access mode to journal: http://armypubs.army.mil/eng/DR_pubs/dr_a/pdf/tm5_601.pdf 3. The official site of SIMATIC WinCC SCADA System [Electronic resource]. – 2014. – Access mode to URL: http://www.automation.siemens.com 4. The official site of Wonderware HMI/SCADA [Electronic resource]. – 2014. – Access mode to URL: http://www.wonderware.com 5. The official site of GENESIS32 HMI/SCADA Visualization Energy [Electronic resource]. – 2014. – Access mode to URL: http://www.iconics.com 6. The official site of Trace Mode SCADA system [Electronic resource]. – 2014. – Access mode to URL: http://www.adastra.ru. 7. IEEE Standard for SCADA and Automation Systems (EN IEEE Std C37.1™-1994): IEEE Std C37.1™-2007. – [Valid since 2008-05-01]. – New York.: IEEE-SA Standards Board, 2008, 143 p. 8. Stouffer K. Guide to supervisory control and data acquisition (SCADA) and industrial control systems security. Recommendations of the National Institute of Standards and Technology. / Stouffer K., Falco J., Kent K. – Gaithersburg: National Institute of Standards and Technology, 2006. – 164 p. 9. Ovodenko A.V. System monitoring methods for complex systems diagnostics / A. V. Ovodenko, A. P. Samoylenko // Information and control systems on rail transport. – 2010. – No 2. – P. 36–41. 10. Gerasimov B.M. Decision support system for real time process control / B. M. Gerasimov, V. I. Glutskiy, A. A. Rabchun // Artificial intelligence. – 2000. – No 3. – P. 39–47. 11. User guide SPPA-T3000. Diagnostic system. – Munich: Siemens AG, 2009. – 251 p. 12. Bernard J. An Expert System for Fault Diagnosis Integrated in Existing SCADA Systems / J. Bernard, D. Durocher // IEEE Transactions on Power Systems. – 1994. – No 1. – P. 548–554. 13. Karpenko A.S. The Development of Many-Values Logics / Karpenko A.S. – M.: LKI Publishers, 2010. – 448 p. 14. Gorbatov V.A. Fundamentals of Discrete mathematics. Information mathematics / Gorbatov V.A. – M.: Nauka. Fizmatlit, 2000. – 544 p.

Поступила в редакцію25.03.2015р.

Рекомендували до друку: докт. техн. наук, проф. Горбійчук М. І., докт. техн. наук, с. н. с. Троїцький В. О.