ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, СИСТЕМНИЙ АНАЛІЗ ТА КЕРУВАННЯ

УДК 681.516:65.011.56

Е.И. Сироткина

Государственное высшее учебное заведение „Национальный горный университет“, г.Днепропетровск, Украина, e-mail: syrotkina@yandex.ru

СТРУКТУРНО-ЛОГИЧЕСКАЯ МОДЕЛЬ ДИАГНОСТИКИ ОТКАЗОВ SCADA СИСТЕМЫ

Ye.I. Syrotkina

State Higher Educational Institution “National Mining University”, Dnipropetrovsk, Ukraine, e-mail: syrotkina@yandex.ru

STRUCTURAL AND LOGICAL MODEL OF SCADA SYSTEM FAULTS DIAGNOSTICS

Цель. Создание методики автоматической самодиагностики отказов SCADA системы, работающей в режиме реального времени в процессе сбора данных; определение достоверности полученных данных на различных уровнях иерархии системы.

Методика. Рассматриваемая в статье методика диагностики работы SCADA системы представляет детерминистический подход к распознаванию технического состояния системы по набору информационно-диагностических признаков, выбор которых основан на логике функционирования SCADA. Анализ приведенной в методике структурно-логической модели построен на базе трехзначной логики.

Результаты. Предлагаемая структурно-логическая модель диагностики учитывает причинно-следственные связи между событиями, происходящими на разных уровнях иерархии системы, и является универсальной для распределенных SCADA систем любой топологии.

Научная новизна. В данной работе выведены полиномиальные зависимости, описывающие допустимые изменения состояний контролируемых параметров, которые согласуются с логикой функционирования SCADA и являются достаточными диагностическими признаками определения недостоверности контролируемых параметров системы.

Практическая значимость. Работа оперативного и ремонтного персонала SCADA систем труднореализуема при возникновении отказов без их автоматической самодиагностики и автоматического определения достоверности данных в условиях временных ограничений для принятия решений, направленных на восстановление работоспособности системы. Использование предложенной методики диагностики отказов SCADA для формирования правил логического вывода базы знаний экспертной диагностической системы позволит в дальнейшем в режиме реального времени проводить автовосстановление работоспособности системы после обратимых отказов.

Ключевые слова: *структурно-логическая модель, SCADA система, трехзначная логика*

Постановка проблемы. В области промышленной автоматизации существует острая потребность во внедрении высоконадежных отказоустойчивых SCADA систем, к которым предъявляются повышенные требования в части безопасности их эксплуатации. Неотъемлемыми функциями SCADA системы являются автоматический сбор данных, передача информации и управляющих воздействий, осуществляемые путем интеграции информационных потоков с аппаратно-программными комплексами нижних и верхних уровней иерархии (УИ) объектов автоматизации в режиме реального времени. Разработчики наиболее известных SCADA систем, таких как WinCC фирмы Siemens [1], Genesis32 фирмы Iconics [2], iFIX фирмы General Electric [3], ТРЕЙС МОУД, компании AdAstrA Research Group, Ltd**.** [4] и другие поставляют в составе систем набор разнообразных программных средств для связи с наиболее распространенными

специализированными контроллерами и интеллектуальными периферийными устройствами. Однако это не устраняет функциональной ограниченности SCADA систем при работе со специализированным оборудованием (например, приборы КИП и автоматики, выпускаемые множеством зарубежных фирм и отечественными предприятиями). Поэтому системным интеграторам зачастую приходится применять программные продукты (в том числе драйверы, программные компоненты и пр.) как третьих компаний-разработчиков, так и собственные программные средства. Большое число применяемых форматов и протоколов передачи данных, аппаратных и программных интерфейсов, встраивание сторонних программных модулей в SCADA систему делает ее более уязвимой с точки зрения надежности, отказоустойчивости и безопасности эксплуатации.

Кроме того, важным аспектом представляемых в системе данных является определение их достоверности, которое должно выполняться автоматически в режиме реального времени.

Поэтому, актуальной задачей является разработка методики автоматической самодиагностики процесса сбора данных SCADA системы в режиме реального времени.

Анализ последних исследований. SCADA система представляет собой сложный, многоуровневый аппаратно-программный комплекс. Достоверность данных на всех его УИ зависит от работоспособности системообразующих узлов, каналов передачи данных, периферийного оборудования, согласованности работы программного обеспечения системы. Для диагностики отказов системы широкое распространение получили методы диагностики, построенные на базе теории распознавания образов [5, 6]. Суть методов заключается в том, что для диагностируемого функционального модуля системы выбирают набор диагностических параметров, изменяющих свои значения в широких пределах, в зависимости от состояния контролируемого объекта. На основе разрабатываемых диагностических моделей устанавливается зависимость между техническим состоянием функционального модуля или системы в целом и отображением данного технического состояния на пространство диагностических параметров.

Выделение нерешенных ранее частей общей проблемы. Таким образом, достоверность контролируемого параметра технологического объекта управления (КП ТОУ) в различных точках информационных потоков, функциональных модулей и УИ SCADA системы зависит от значений набора диагностических признаков (ДП) в соответствующих точках локализации.

Работа с большими массивами данных без автоматической самодиагностика отказов и автоматического определения достоверности данных КП ТОУ в процессе их сбора становится труднореализуемой в условиях временных ограничений для принятия решений оперативным и ремонтным персоналом системы.

Формулировка цели работы. Целью работы является разработка методики автоматической самодиагностики отказов, самоопределения достоверности КП ТОУ в процессе сбора данных SCADA системы с использованием критериев диагностики, основанных на логике функционирования SCADA.

Постановка задачи. Рассмотрим в общем виде пример некоторого фрагмента структуры SCADA системы (рис. 1) для диагностики отказов при автоматическом сборе данных. На момент времени t набор контролируемых параметров технологического объекта управления

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

измеряемый при помощи первичных преобразователей (***ПП),*** регистрируется в специализированных контроллерах – узлах сбора данных (***УСД).*** Считывание $x_i(t)$ с $ПП_i$, связанного по каналу передачи данных (Ch_i) через порт ($П_i$) с $УСД_j$, обеспечивает работающий на $УСД_j$ программный процесс pA_j. Сервер S_1 соединен с $УСД$ в глобальную вычислительную сеть (ГВС) при помощи каналов передачи данных Ch_{1j}. За передачу данных между $УСД_j$ и сервером (S_1) по Ch_{1j} с использованием протокола передачи данных ($ППД_j$) отвечают, соответственно, программные процессы (pB_j) и (pC_j). На сервере S_1 ведется база данных (***БД).*** Запись данных в БД осуществляется при помощи программного процесса (*pD)*.

Необходимо постоянно, в режиме реального времени, выполнять автоматическую самодиагностику функционирования SCADA системы в процессе сбора данных и определять место возникновения и вид неисправности по состоянию КП ТОУ $X(t)$ в системе.

Описание методики диагностики. Обозначим L уровни иерархии системы, соответствующие уровням возможной локализации неисправности (рис. 1); L_1 – уровни иерархии системы, соответствующие системообразующим узлам, где может быть осуществлен доступ из системы к параметру $x_i(t)$; L_2 – уровни иерархии системы, соответствующие каналам передачи данных

$$L=\{1,2,3,4,5,6\};$$
$$L_1\subset L;\quad L_1=\{2,4,6\};$$
$$L_2\subset L;\quad L_2=\{3,5\}.$$

На уровне ТОУ (l=1) на момент времени t для набора $X(t)$ параметр $x_i(t)$ может находиться в одном из следующих состояний (рис. 2):

- значение параметра находится в диапазоне технологических границ (P);
- значение параметра находится за пределами технологических границ (T);
- значение параметра находится в аварийном диапазоне (A).

На уровнях SCADA системы ($l \in L_1$) параметр $x_i(t)$ может находиться в одном из состояний:

- значение параметра достоверно (Д), т.е. корректно передано / зарегистрировано в системе. Все состояния параметра уровня ТОУ относятся к достоверному состоянию параметра в системе (рис. 2);

- значение параметра недостоверно (Н), например: зарегистрированное в системе значение параметра невозможно по физическому смыслу (находится вне диапазона допустимых значений); в протоколе передачи данных были зафиксированы ошибки передачи; на разных УИ системы зарегистрированы разные значения одного и того же параметра и т.д.;

- параметр отсутствует в системе (О), значение параметра не определено.

На уровнях SCADA системы ($l \in L_2$) определим возможные статусы завершения процесса приема-передачи набора $\boldsymbol{X(t)}$ по каналам передачи данных $\boldsymbol{Ch_i}$:

- прием-передача параметра $\boldsymbol{x_i(t)}$ завершена корректно и считается достоверной (Д);

- прием-передача параметра $\boldsymbol{x_i(t)}$ завершена, но обнаружены ошибки **ППД** или некорректные настройки среды передачи данных и т.д. Передача параметра считается недостоверной (Н);

- прием-передача параметра $\boldsymbol{x_i(t)}$ отсутствовала (О).

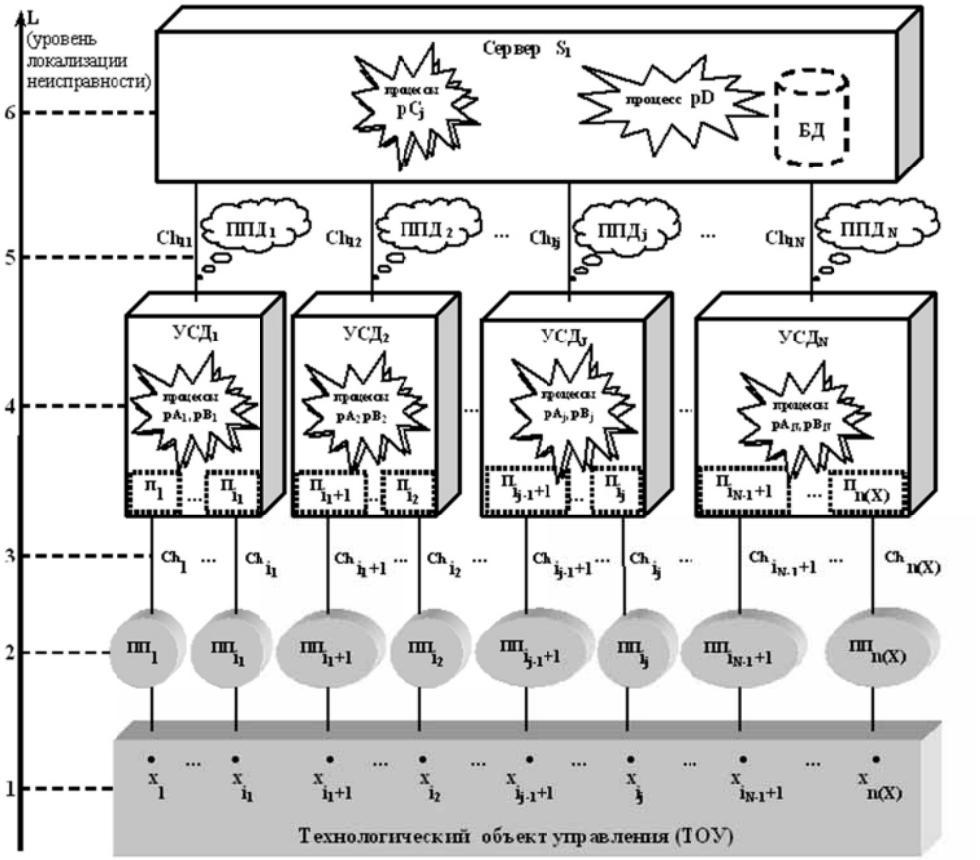

Рис. 1. Пример структуры SCADA системы для диагностики отказов при автоматическом сборе данных

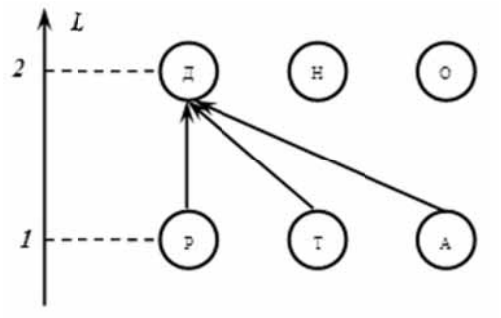

Рис. 2. Изменение состояния контролируемого параметра при переходе с уровня иерархии технологического объекта управления на уровень иерархии системы

При переходе с уровня $\boldsymbol{l_k}$ на уровень $\boldsymbol{l_{k+1}}$ (для $\boldsymbol{l \in L_1}$) состояние параметра может измениться в результате возникновения неисправности, как показано на рис. 3. Недопустимые изменения состояния параметра при переходе с уровня $\boldsymbol{l_k}$ на уровень $\boldsymbol{l_{k+1}}$ (для $\boldsymbol{l \in L_1}$) приведены на рис. 4.

Критерием обнаружения неисправности является:

- для уровня ТОУ - выход значения параметра за технологические границы / нахождение в аварийном диапазоне;

- на уровне системы (для $\boldsymbol{l \in L_1}$) – недостоверное значение / отсутствие параметра;

- изменение достоверного состояния параметра (рис. 3) при переходе на более высокий уровень иерархии ($\boldsymbol{l \in L_1}$);

- недостоверность / отсутствие приема-передачи параметра ($l \in L_2$).

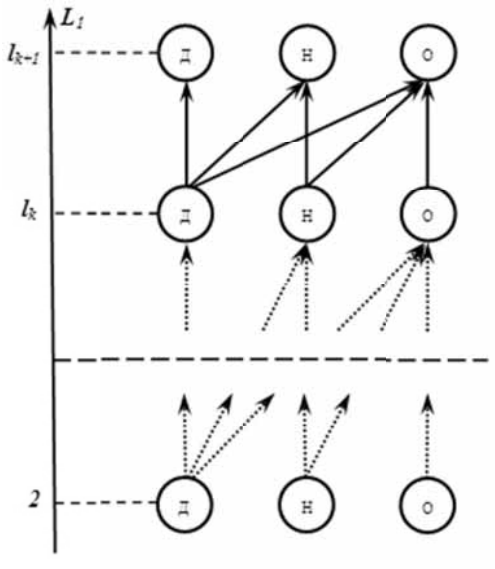

Рис. 3. Допустимые (возможные) изменения состояния параметра по уровням иерархии системы

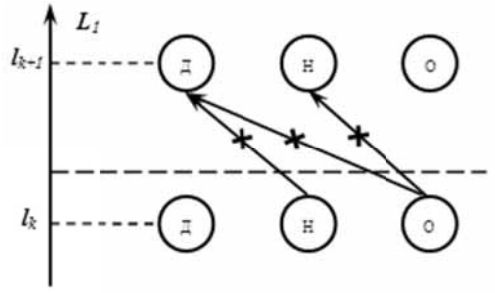

Рис. 4. Недопустимые (невозможные) изменения состояния параметра по уровням иерархии системы

Определим множество состояний для набора ***X(t)*** по УИ в виде матрицы ***M(t)***

$$M(t) = (m_{iL,iC});$$
$$iL = n(L) + 1 - l; \quad l = \overline{1, n(L)}; \quad iC = \overline{1, n(X)};$$
$$m_{iL,iC} \in \begin{cases} \{Д, H, O\}, l > 1 \\ \{P, T, A\}, l = 1 \end{cases},$$

где iL – индекс строки матрицы, соответствующий уровням иерархии системы, расположенным в порядке убывания; iC – индекс столбца матрицы, соответствующий индексу контролируемого параметра; $n(L)$ – количество уровней иерархии системы; $n(X)$ – количество КП ТОУ.

Матрице состояний КП ТОУ поставим в соответствие диагностическую матрицу ***D*** достоверности контролируемых параметров для $l > 1$ уровней иерархии системы.

$$D = \begin{bmatrix} d_{11} & \dots & d_{1i_1} & \dots & d_{1i_{j-1}+1} & \dots & d_{1i_j} & \dots & d_{1i_{N-1}+1} & \dots & d_{1i_N} \\ d_{21} & \dots & d_{2i_1} & \dots & d_{2i_{j-1}+1} & \dots & d_{2i_j} & \dots & d_{2i_{N-1}+1} & \dots & d_{2i_N} \\ d_{31} & \dots & d_{3i_1} & \dots & d_{3i_{j-1}+1} & \dots & d_{3i_j} & \dots & d_{3i_{N-1}+1} & \dots & d_{3i_N} \\ d_{41} & \dots & d_{4i_1} & \dots & d_{4i_{j-1}+1} & \dots & d_{4i_j} & \dots & d_{4i_{N-1}+1} & \dots & d_{4i_N} \\ d_{51} & \dots & d_{5i_1} & \dots & d_{5i_{j-1}+1} & \dots & d_{5i_j} & \dots & d_{5i_{N-1}+1} & \dots & d_{5i_N} \end{bmatrix} \begin{matrix} l=6 \\ l=5 \\ l=4. \\ l=3 \\ l=2 \end{matrix}$$

$$\underbrace{\quad}_{\text{УСД}_1} \dots \underbrace{\quad}_{\text{УСД}_j} \dots \underbrace{\quad}_{\text{УСД}_N}$$

Для анализа матрицы будем использовать трехзначную логику Э. Поста P_3 [7, 8, 9]. Определим элементы матрицы $d_{iL,iC}$ на трехзначном множестве $E_3 = \{0, 1, 2\}$, соответствующем {О, Н, Д} состояниям параметра при $l \in L_1$ или {О, Н, Д} статусам завершения процесса приема-передачи параметра при $l \in L_2$.

$$iL = n(L) + 1 - l; \quad l = \overline{2, n(L)}; \quad iC = \overline{1, n(X)}.$$

Представим в табличном виде (табл. 1) функцию $f_1(x, y)$ изменения состояния параметра по УИ системы (рис. 3 и 4), где x – состояние параметра на предыдущем УИ $l_k \in L_1$; y – состояние параметра на следующем УИ $l_{k+1} \in L_1$; $f_1(x, y) = 1$ – допустимое изменение состояния параметра по УИ L_1 системы; $f_1(x, y) = 0$ – недопустимое изменение состояния параметра по УИ L_1 системы.

Таблица 1

Табличное задание функции изменения состояния контролируемого параметра по УИ системы

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

Данному табличному заданию функции $f_1(x, y)$ соответствует полином

$$f_1(x, y) = (1 + xy - y^2 - xy^2 - 2x^2 y) \pmod 3.$$

Таким образом, корректность формирования матрицы ***D,*** в соответствии с допустимыми изменениями состояния контролируемого параметра $x_{iC}(t)$ по УИ $l \in L_1$, проверяется следующим образом

$$f_1(d_{iL+2,iC}, d_{iL,iC}) = 1; \quad iL = n(L) + 1 - l; \quad l \in L_1.$$

Представим в табличном виде (табл. 2) функцию $f_2(x, y, z)$ допустимых изменений состояния параметра по УИ системы с учетом статуса завершения процесса приема-передачи между соседними УИ системы, где x – состояние параметра на передающем УИ $l_k \in L_1$; y – статус завершения процесса приема-передачи параметра $l \in L_2$; z – состояние параметра на принимающем УИ $l_{k+1} \in L_1$; $f_1(x,y,z) = 2$ – необходимое

изменение состояния параметра на принимающем УИ, т.е. $(x \vee y)||\rightarrow \Box z$ (события x или y являются причиной необходимости события z); $f_2(x,y,z) = 1$ – допустимое (возможное) изменение состояния параметра на принимающем УИ, т.е. $\neg(x\&y)||\rightarrow \Diamond z$ (события x и y не являются причиной события z, но событие z в системе возможно); $f_2(x,y,z) = 0$ – недопустимое (невозможное) изменение состояния параметра на принимающем УИ, т.е. $(x \vee y)||\rightarrow \neg\Diamond z$ (события x или y являются причиной невозможности события z).

Таблица 2

Табличное задание функции изменения состояния параметра по уровням иерархии системы с учетом статуса завершения приема-передачи

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

Данному табличному заданию функции $f_2(x,y,z)$ соответствует полином

$$f_2(x,y,z) = (2 - 2z^2 - xyz^2 + 2x^2y^2 + x^2y^2z + x^2yz^2 + xy^2z^2 - 2x^2y^2z^2) \pmod 3.$$

Таким образом, корректность формирования матрицы $\boldsymbol{D}$ для контролируемого параметра $x_{iC}(t)$ с учетом статуса завершения процесса приема-передачи проверяется следующим образом

$$f_2(d_{iL+2,iC}, d_{iL+1,iC}, d_{iL,iC}) \neq 0.$$

Проведем анализ корректно сформированной матрицы $\boldsymbol{D}$ для структуры SCADA системы, представленной на рис. 1.

Рассмотрим матрицу $\boldsymbol{D}$ на некоторой неубывающей последовательности положительных целых чисел $\boldsymbol{I_X}$, определяющей распределение контролируемых параметров по УСД

$$I_X = i_1, i_2, \ldots i_j, \ldots, i_N,$$

где j – порядковый номер члена последовательности, соответствующий порядковому номеру УСД; N – количество УСД; $i_N = n(X)$ – количество контролируемых параметров; $i_j - i_{j-1}$ – количество контролируемых параметров, подключенных к УСД$_j$.

Можно утверждать, что автоматический сбор данных SCADA системы на момент времени $\boldsymbol{t}$ проходит безотказно, если для 1-ой строки матрицы $\boldsymbol{D}$ ($\boldsymbol{iL=1}$), соответствующей (рис. 1) уровню сервера $\boldsymbol{l=6}$, имеем

$$\mathop{\&}_{iC=1}^{i_N} \varphi_2(d_{1,iC}(t)) = 1,$$

где φ_2 – характеристическая функция первого рода, определяемая следующим образом

$$\varphi_e(d_{iL,iC}) = \begin{cases} 1, & d_{iL.iC} = e, \quad e \in E_3 \\ 0, & d_{iL,iC} \neq e, \quad e \in E_3 \end{cases}.$$

Выводы и перспективы дальнейшего развития. Предлагаемая в статье методика диагностики процесса сбора данных SCADA системы, рассмотренная на базе структурно-логической модели с использованием трехзначной логики P_3, позволяет автоматически определять достоверность КП ТОУ по информационно-диагностическим признакам, основанным на логике функционирования SCADA системы с учетом причинно-следственных связей между событиями. Использование данной методики при формировании правил логического вывода базы знаний экспертной диагностической системы для обнаружения отказов в работе SCADA, позволит в дальнейшем в режиме реального времени проводить автовосстановление работоспособности системы после обратимых отказов.

Список литературы / References

1. Официальный сайт SCADA системы SIMATIC WinCC [Электронный ресурс] – Режим доступа: http://automation.siemens.com

The official site of SIMATIC WinCC SCADA System, (2013), available at: http://automation.siemens.com (accessed September 5, 2013).

2. Официальный сайт SCADA системы GENESIS32 [Электронный ресурс] – Режим доступа: http://iconics.com

The official site of GENESIS32 SCADA System, (2013), available at: http://iconics.com (accessed September 5, 2013).

3. Официальный сайт SCADA системы iFIX [Электронный ресурс] – Режим доступа: http://ge-ip.com

The official site of iFIX SCADA System, (2013), available at: http://ge-ip.com (accessed September 5, 2013).

4. Официальный сайт SCADA системы ТРЕЙС МОУД [Электронный ресурс] – Режим доступа: http://adastra.ru

The official site of Trace Mode SCADA system, (2013), available at: http://www.adastra.ru (accessed September 5, 2013).

5. Воронин В.В. Диагностические модели технических объектов / В. В. Воронин // Складні системи і процеси. – 2002. – №1. – С. 20–30.

Voronin, V.V. (2002), "Diagnostic models of technical objects", *Skladni systemy i protsesy,* no. 1, pp. 20–30.

6. Оводенко А.В. Системный мониторинг методов диагностики сложных систем / А.В. Оводенко, А.П. Самойленко // Інформаційно-керуючі системи на залізничному транспорті. – 2010. – №2. – С. 36–41.

Ovodenko, A.V. and Samoylenko, A.P. (2010), "System monitoring methods for complex systems diagnostics", *Informatsiino-keruiuchi systemy na zaliznychomu transporti,* no. 2, pp. 36–41.

7. Карпенко А.С. Развитие многозначной логики / Карпенко А.С. – М.: ЛКИ, 2010. – 448 с.

Karpenko, A.S. (2010), *Razvitie mnogoznachnoy logiki* [The Development of Many-Values Logics], LKI, Moscow, Russia.

8. Ивин А.А. Модальные теории Яна Лукасевича / Ивин А.А. – М.: ИФ РАН, 2001. – 176 с.

Ivin, A.A. (2001), *Modalnye teorii Yana Lukasevicha* [Modal Theory of Jan Lukasiewicz], IF RAN, Moscow, Russia.

9. Скобелев В.Г. Анализ дискретных систем / Скобелев В.Г. – Донецк: ИПММ НАН Украины, 2002. – 172 с.

Skobelev, V.G. (2002), *Analiz diskretnykh system* [Discrete Systems' Analysis], IPMM NAN Ukrainy, Donetsk, Ukraine.

Мета. Створення методики автоматичної самодіагностики відмов SCADA системи, що працює в режимі реального часу у процесі збору даних; визначення достовірності отриманих даних на різних рівнях ієрархії системи.

Методика. Розглянута у статті методика діагностики роботи SCADA системи представляє детерміністичний підхід до розпізнавання технічного стану системи за набором інформаційно-діагностичних ознак, вибір яких заснований на логіці функціонування SCADA. Аналіз наведеної в методиці структурно-логічної моделі побудований на базі тризначної логіки.

Результати. Запропонована структурно-логічна модель діагностики враховує причинно-наслідкові зв'язки між подіями, що відбуваються на різних рівнях ієрархії системи, та є універсальною для розподілених SCADA систем будь-якої топології.

Наукова новизна. У даній роботі виведені поліноміальні залежності, що описують допустимі зміни станів контролюючих параметрів, які узгоджуються з логікою функціонування SCADA та мають достатні діагностичні ознаки для визначення недостовірності контролюючих параметрів системи.

Практична значимість. Робота оперативного та ремонтного персоналу SCADA систем важко реалізовується при виникненні відмов без їх автоматичної самодіагностики та автоматичного визначення достовірності даних в умовах часових обмежень для прийняття рішень, спрямованих на відновлення працездатності системи. Використання запропонованої методики діагностики відмов SCADA для формування правил логічного висновку бази знань експертної діагностичної системи дозволить надалі в режимі реального часу проводити автозбереження працездатності системи після оборотних відмов.

Ключові слова: *структурно-логічна модель, SCADA система, тризначна логіка*

Purpose. Developing an automatic real-time SCADA failures self-test methodology during collecting data; determining the data reliability at different levels within the system hierarchy.

Methodology. The methodology of SCADA systems diagnostics is examined in this paper. It is a deterministic approach to the technical system condition recognition by a set of information-diagnostic features. The selection of these features is based on SCADA functioning logic. The structural and logical model analysis is described in this methodology and founded on three-valued logic.

Findings. The diagnostic structural and logical model that takes into account the cause-effect relations between events that occur at different levels within the system hierarchy is proposed. It is the universal model for distributed SCADA systems of any topology.

Originality. The polynomial dependencies, describing the permissible changes within the state-monitored parameters that are consistent with SCADA functioning logic are derived in this paper. They are sufficient diagnostic features determining the system controlled parameters unreliability.

Practical value. The work of operating and maintenance SCADA system personnel is poor-selling in case the failure appearing without an automatic self-diagnostics and automatic determination of the data reliability in time limits terms for decisions to restore the system health. Using the proposed SCADA failures testing method for forming logical conclusion rules of the diagnostic systems expert knowledge will allow performing disaster recovery of the system health in real time after reversible failures in the future.

Keywords: *structural and logical model, SCADA system, three-valued logic*

Рекомендовано до публікації докт. техн. наук В.В. Слєсарєвим. Дата надходження рукопису 07.10.13.