An Online Intelligent Alarm-Processing System for Digital Substations

Liuhong Wei, Wenxin Guo, Fushuan Wen, Gerard Ledwich, *Senior Member, IEEE*, Zhiwei Liao, and Jianbo Xin

***Abstract*—A flood of alarm messages in an automatic digital substation makes the monitoring task a significant challenge for the operators in a remote control center, especially under fault scenarios. An online intelligent alarm-processing system is developed based on the architecture of the digital substation. First, real-time alarms are classified according to the IEC 61850 standard in order to provide synthesized and organized alarms for the alarm-processing procedure in the next step. Then, a new and systematic alarm-processing approach for digital substations is developed. Two modules (i.e., the generation of candidate hypotheses and the truth evaluation for the hypotheses) are included in the developed approach, and these two modules are operating in parallel in online implementation. This approach could not only determine the fault/disturbance cause but also the missing or false alarms as well as the causes of the false alarms. According to actual application requirements, an online intelligent alarm-processing system is developed and applied in the Xingguo substation—the first digital substation in Jiangxi Province, China. Finally, an actual alarm-processing scenario serves to demonstrate the presented alarm-processing method as well as the developed software system.**

***Index Terms*—Alarm classification, digital substation, IEC 61850, online intelligent alarm processing, power system.**

I. Introduction

A MODERNIZED digital substation usually consists of intelligent primary devices (such as optic-electric transformers and intelligent circuit breakers (CBs)) and the networked secondary devices based on the IEC 61850 protocol, which is able to implement the interoperability and information sharing between the intelligent electronic devices (IEDs). For an automatic digital substation, all of the alarm messages are collected and sent to a remote-control center. The monitoring data of the operational devices in digital substations are displayed by order of timestamps but they have not yet been processed, and this could lead to the inability of the operators to digest information from the data and, hence, identify what has occurred in a short time, especially under stressed conditions such as a fault scenario. The situation will be more challenging for cases with false or missing alarms. Therefore, it is of a great significance to develop an online intelligent alarm-processing system based on the architecture of digital substations in order to assist the operators in making a decision for maintaining the secure and reliable operation of power systems.

In the past two decades, many artificial-intelligence techniques, such as expert systems (ES), artificial neural networks (ANNs), and Petri Nets, have been employed for alarm processing in power systems.

The basic characteristic of the ES-based approach is that the operating logics of protective relays (PRs) and CBs as well as the diagnosis experience of operators can be accommodated. ES is suitable for solving the alarm-processing problem [1]–[6]. For instance, a logic-based ES developed in [6] has been successfully applied in the Italian National Control Center.

Several ANN-based alarm-processing methods are presented in [7]–[10], and they can model complex relationships between inputs (i.e., the operating information of PRs and CBs, and outputs, that is, the causes activating the alarms). Appropriate samples need to be selected to train the ANN to guarantee good generalization capability.

In recent years, analytic model-type–based approaches were developed for solving the alarm-processing problems [11]–[14]. The causes (faults/disturbances/events) for the activation of alarms are considered as optimization variables, and an objective function is defined to reflect the discrepancy between the reported and the expected alarms. The expected alarms of a cause/an event could be obtained based on the power system structure concerned as well as the PR and CB configurations. Then, alarm processing can be formulated as an unconstrained 0–1 integer programming problem. Finally, some well-developed optimization algorithms, such as the tabu search (TS) [11], [12] and genetic algorithms (GAs) [13], [14], are employed to find out the most likely hypothesis that could well explain the reported alarms.

The advantage of the Petri Net lies in that it has the characteristics of graphic discrete event representation and parallel information processing, so that it is suitable for describing the logic relationship between the operation of PRs and CBs. Some

Manuscript received June 07, 2010; revised August 15, 2010, September 05, 2010; accepted February 06, 2011. Date of publication April 05, 2011; date of current version June 24, 2011. This work was supported in part by National Natural Science Foundation of China (50477029) and in part by the National Key Technology R&D Program of China (2008BAA13B10). Paper no. TPWRD-00433-2010.

L. Wei and Z. Liao are with the School of Electrical Engineering, South China University of Technology, Guangzhou 510640, China (e-mail: weiliuhong16@gmail.com; epliao@scut.edu.cn).

W. Guo is with Guangdong Power Dispatch Center, Guangzhou 510600, China (e-mail: guowenxin2005@126.com).

F. Wen is with the School of Electrical Engineering, Zhejiang University, Hangzhou 310027, China. He is also with the School of Engineering Systems, Faculty of Built Environment and Engineering, Queensland University of Technology, Brisbane 4001, Australia (e-mail: fushuan.wen@gmail.com).

G. Ledwich is with the Faculty of Built Environment and Engineering, School of Engineering Systems, Queensland University of Technology, Brisbane 4001, Australia (e-mail: g.ledwich@qut.edu.au).

J. Xin is with the Jiangxi Electric Power Research Institute, Nanchang 330006, China (e-mail: mandyzhuhai@163.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TPWRD.2011.2117445

research work on the applications of the Petri Net for alarm processing in power systems has been conducted in recent years [15]–[18].

In addition, several other methods such as fuzzy sets [19], [20] and rough sets [21], [22] have also been employed for alarm processing in recent years.

Up to now, most research work on alarm processing is based on conventional substations [1], [4], [8], [16], [21], [22], while for digital substations, research work in this area is still very preliminary. With the support from Jiangxi Electric Power Research Institute in China, an online intelligent alarm-processing system for the 110-kV Xingguo digital substation is designed and implemented in this paper. The major contributions of this paper are as follows:

1) Based on the architecture of the digital substation, real-time alarms are classified according to the IEC 61850 standard.
2) For online implementation in digital substations, a new and systematic alarm-processing approach is presented. Two modules (i.e., the generation of candidate hypotheses and the truth evaluation for the hypotheses) are included in the developed approach. These two modules operate in parallel in online implementation as follows.
   - In the module for the generation of candidate hypotheses, the related candidate hypotheses are organized in the same hypothesis set.
   - In the module for the truth evaluation of the hypotheses, a systematic alarm-processing approach based on logic analysis is presented. Consequently, not only could the fault/disturbance cause be identified, but also the missing or false alarms. Moreover, the causes of false alarms could also be identified by analyzing the alarms associated with the secondary devices (i.e., the protection devices and communication devices).
3) According to the requirement of the actual project, a software package is developed by using the proposed online intelligent alarm-processing approach, and has been successfully applied in the Xingguo substation, the first digital substation in Jiangxi Province, China. Finally, an actual alarm-processing scenario is served for demonstrating the presented alarm-processing model as well as the developed software system.

II. Framework of the Developed System

The developed framework for the online intelligent alarm-processing system in this paper is based on the architecture of a digital substation as shown in Fig. 1. At the system initialization stage, the alarm configuration is automatically written into the database by analyzing the substation configuration description language (SCL) file. When a fault/disturbance takes place, the received alarms will be put into the real-time database first, and then into the initial alarm queue. Based on the IEC 61850 standard, the alarms in the initial alarm queue are classified in order to provide layered and organized alarms for the alarm-processing procedure. When PRs operate or CBs trip, the module of online intelligent alarm processing will be activated. Consequently, the comprehensive alarm-processing results are

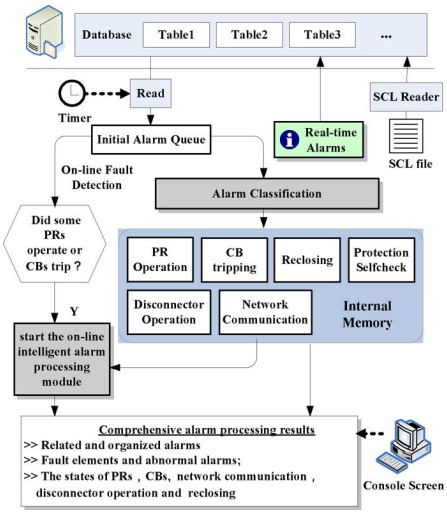

Fig. 1. Framework of the proposed system.

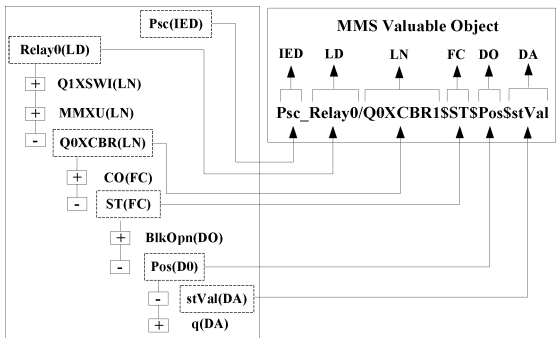

Fig. 2. Process of mapping the model information of IEDs into the MMS variable object.

displayed on the operator's console screen with the following details:

1) Related alarms are listed by groups in order to help the operators organize the real-time alarms clearly.
2) Faulted elements are identified to assist the operators rapidly restoring the network, especially under complicated fault scenarios.
3) Detailed information for IEDs, such as the network communication and protection self-check, could support the maintenance personnel to troubleshoot the malfunctioned devices, such as PR and CB malfunctions.

III. Alarm Classifications Based on the IEC 61850 Standard

In order to implement the interoperability between IEDs, the IEC 61850 standard specifies a method for mapping the model information of IEDs into the manufacturing message specification (MMS) variable object, and this leads to a unique identification for each element in the model of IEDs. The detailed process for mapping the model information of IEDs into the MMS variable object is shown in Fig. 2 [25]. The format of aN MMS variable object is as: "*IED_logic device (LD)/logic node (LN)$function constraint (FC)$data object (DO)$data attribute (DA)*".

TABLE I
RULES OF ALARM CLASSIFICATIONS

Type	Character				Value change	
	LN	DO	DA	FC	0→1	1→0
CB tripping	XCBR	Pos	stVal	ST	open	close
PR operation	P…	Op	general,phsA,phsB,phsC	ST	operate	reset
Disconnector operation	XSWI	Pos	stVal	ST	open	close
Reclosing	RREC	Op	general,phsA,phsB,phsC	ST	operate	reset
Protection self-check	chkGGIO	Ind	stVal	ST	error	restore
Network communication	Q0GGIO	Ind	stVal	ST	error	restore

All of the MMS variable objects are generated by extracting information from the SCL files. First, all of the elements in the SCL files are picked up based on the XML analytic technique. Then, the MMS variable objects are developed by assembling the elements.

Based on the IEC 61850 standard, each LN (DO or DA) is named with self-description [23]. Each MMS variable object has a unique meaning. For instance, the meanings of the components of the MMS variable object in Fig. 2 are as follows: the LN component "XCBR" represents "CB;" the DO component "Pos" represents "position;" and the DA component "stVal" represents "state." Above all, the MMS variable object in Fig. 2 can be used to mark "the state (open or close) of position of a CB."

When an alarm is received, an MMS variable object as well as its corresponding value can be obtained: the MMS variable object represents the identification of an IED model, and its corresponding value determines the state information of an IED model. For instance, if the value corresponding to the MMS variable object shown in Fig. 2 is "1," then it is known that the position (state) of the CB is "open;" if the value is "0," then the position (state) of the CB is "close." When the value of an MMS variable object changes (i.e., "0 → 1" or "1 → 0"), an alarm will be generated. The MMS variable object and the change of its corresponding value can together identify a unique alarm.

According to the characteristics of different MMS variable objects, the alarms can be classified into several types, mainly including CB tripping, PR operation, disconnector operation, reclosing, protection self-check, and network communication. For instance, the alarm with the MMS variable object shown in Fig. 2 is classified into the CB tripping type. The detailed rules for alarm classifications are shown in Table I.

IV. ONLINE INTELLIGENT ALARM PROCESSING

A. Basic Concepts

For the convenience of presentation, some basic concepts are defined first as follows.

1) a_j is defined as a specified alarm in the digital substation, and can be identified by an MMS variable object and a value. For instance, if the value of the MMS variable object in Fig. 2 is "0," this alarm represents that "the CB Q0XCBR1 is open."
2) c_i is defined as a cause (fault/disturbance/event) hypothesis, and represents an assumption for the cause of the alarms reported. For instance, suppose that CB_1 is a CB connected with the transmission line L_1; when CB_1 trips, "a fault occurs on L_1 " will be a reasonable event hypothesis.
3) Based on the configuration of a power system concerned and the actuating logic of PRs and CBs, two kinds of rules for alarm processing could be established and saved to the database as follows.
   a) (c_i, a_j) denotes that once the cause hypothesis c_i is true, the alarm a_j would occur. For example, suppose that PR_1 is a zero-sequence overcurrent PR of L_1, the event "an earth fault takes place in L_1," will cause the alarm "PR_1 operates." In Fig. 3, the rules associated with this kind include (c_1, a_1), (c_2, a_1) and (c_2, a_2).
   b) (a_j, a_k) denotes that the occurrence of a_j will trigger a_k to take place. For example, suppose that PR_2 is a distance PR of the transmission line L_1, CB_1 is a CB connected with L_1, the alarm "PR_2 operates," will trigger the alarm "CB_1 trips" to occur. In Fig. 3, the rules associated with this kind include (a_1, a_4) and (a_2, a_3).

   As shown in Fig. 3, a rule network could be built up by the rules, and used to describe the relationship between the elements included in rules clearly.
4) $\mathrm{Cause}(a_j) = \{c_i | i = 1, 2, \ldots, n\}$ is defined as the set of the cause hypotheses which could trigger a_j to occur, and n is the number of elements in $\mathrm{Cause}(a_j)$. Taking the rule network in Fig. 3 as an example, two hypotheses c_1 and c_2 could trigger a_1 to occur, hence $\mathrm{Cause}(a_1) = \{c_1, c_2\}$.
5) $\mathrm{Expected}(c_i) = \{a_j | j = 1, 2, \ldots, m\}$ is defined as the set of the expected alarms corresponding to c_i. It represents the alarms to be reported if c_i is true, and m is the number of elements in $\mathrm{Expected}(c_i)$. Taking the rule network in Fig. 3 as an example, if c_2 is true, four alarms including a_1, a_2, a_3, and a_4 would be reported, hence $\mathrm{Expected}(c_2) = \{a_1, a_2, a_3, a_4\}$.
6) $G_k = \{c_1, c_2, \ldots . c_p\}$ is defined as the set of cause hypotheses, and p is the number of elements in G_k.
7) $S = \{G_1, G_2, \ldots . G_z\}$ is defined as a container for storing all of the $G_k (k = 1, 2, \ldots p)$, and z is the number of elements in S.

B. Basic Principle of the Online Intelligent Alarm Processing

As shown in Fig. 4, the basic principle of the online intelligent alarm processing is as follows.

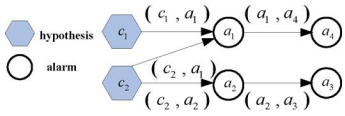

Fig. 3. Simple example of the rule network for alarm processing.

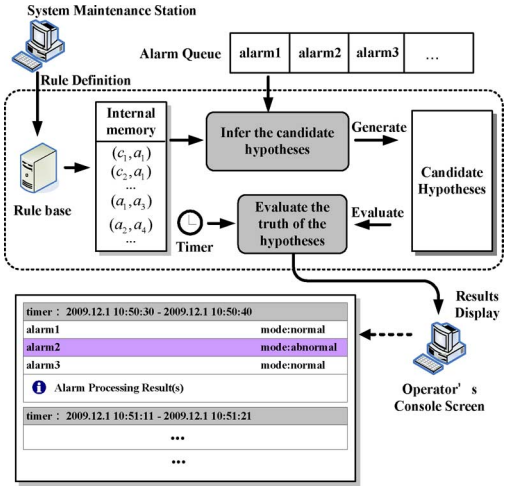

Fig. 4. Basic principle of the online intelligent alarm processing.

At the system initialization stage, all of the rules in the database are read into the internal memory. Once a fault/disturbance occurs, the candidate hypotheses are inferred according to the reported real-time alarms and the alarm-processing rules. Then, the candidate hypotheses are evaluated periodically for finding out the fault/disturbance cause and abnormal alarms. Finally, the comprehensive alarm-processing results are displayed in the operator's console screen. Two key modules are included in the proposed method (i.e., the generation of candidate hypotheses and the truth evaluation for the hypotheses). These two modules will be described in detail in the following text.

C. Generation of Candidate Hypotheses and the Truth Evaluation for the Hypotheses

When a fault occurs in a digital substation, a flood of real-time alarms will be sent to the control center in a short time. For online implementation of the intelligent alarm-processing system in digital substations, a new and systematic alarm-processing approach is proposed, which includes two modules (i.e., the generation of candidate hypotheses and the truth evaluation for the hypotheses). These two modules are operating in parallel for online implementation. The detailed flowchart is shown in Fig. 5.

1) Generation of Candidate Hypotheses: The generation of candidate hypotheses is to infer all possible causes of faults/disturbances/events for a received alarm according to the alarm-processing rules, and then the related candidate hypotheses are organized in the same hypothesis set.

Assume that a_j is received at time $t, G_k = \{c_1, c_2, \ldots . c_p\}$ and $S = \{G_1, G_2, \ldots . G_z\}$. As shown in Fig. 5, the key steps of the generation of candidate hypotheses are introduced as follows.

a) The hypotheses are determined by

$$C^* = \{c_i | a_j \in \text{Expected}(c_i) \cap c_i \in G_k \cap G_k \in S\}. \quad (1)$$

If $C^* = \emptyset$, turn to step b); otherwise, turn to step c).

b) A new hypothesis set G_{z+1} is built up and initialized as $G_{z+1} = \text{Cause}(a_j)$, and next added to S

$$S = S \cup G_{z+1}.$$

At the same time, the time window $W(G_{z+1}) = [t, t + T]$ corresponding to G_{z+1} is also established. In order to guarantee that all received real-time alarms during a fault process could be included in a same time window T, the length of $W(G_{z+1})$ is set as the maximum setting values of the operating time among all PRs. $W(G_{z+1})$ is used in the truth evaluation for the hypotheses as will be detailed.

c) If $c_i \in C^* \cap c_i \in G_k$, the hypotheses involved in $\text{Cause}(a_j)$ but not being the member of G_k (i.e., $c_b \in \text{Cause}(a_j) \cap c_b \notin G_k$ should be added to G_k

$$G_k = \{c_b | \text{ Cause}(a_j) \cap c_b \notin G_k\} \cup G_k. \quad (2)$$

2) Truth Evaluation for the Hypotheses: In this module, a systematic evaluation approach is presented based on logic analysis. Consequently, not only could the fault/disturbance cause be identified but also the missing or false alarms. Moreover, the causes of the false alarms could also be identified by analyzing the alarms associated with the secondary devices (i.e., the protection devices and communication devices).

Suppose that t_{current} is the current time. If t_{current} exceeds the time window corresponding to G_k (i.e., $t_{\text{current}} \notin W(G_k)$), then G_k is defined as "an overflowing hypothesis set." Once an overflowing hypothesis set exists, the truth of the hypotheses in it should be evaluated. The evaluation standard consists of the occurrence rate (OR) and the coverage rate (CR) of the expected alarm.

$Y(c_i) = (y_1, y_2, \ldots y_r, \ldots y_q)$ is defined as a q -dimension vector with 0–1 elements, and exactly corresponds to each element in $\text{Expected}(c_i)$. Assume that the element corresponding to y_r in $\text{Expected}(c_i)$ is a_j, if a_j occurs, $y_r = 1$; otherwise, $y_r = 0$.

The OR corresponding to c_i is defined as follows:

$$\text{Occurrence}(c_i) = \frac{1}{q} \sum_{r=1}^{q} y_r \times 100\% \quad (3)$$

where $\sum_{r=1}^{q} y_r$ represents the number of actually occurring alarms among those alarms included in $\text{Expected}(c_i)$, and q is the number of expected alarms corresponding to c_i.

The CR corresponding to c_i is defined as follows:

$$\text{Coverage}(c_i) = \frac{1}{h} \sum_{r=1}^{q} y_r \times 100\% \quad (4)$$

where h is the number of the reported real-time alarms whose timestamps are within the time window of the evaluated hypothesis set G_k.

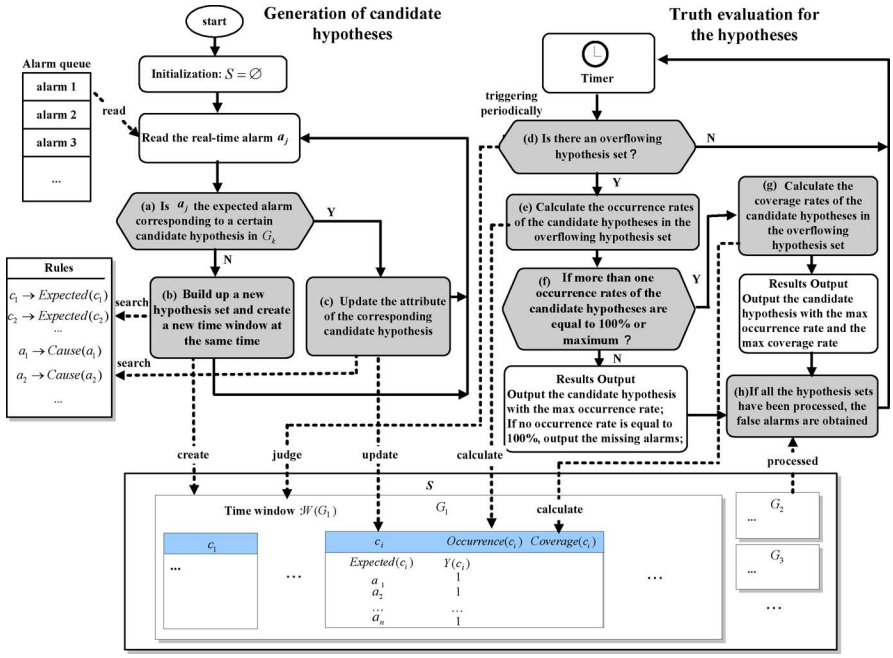

Fig. 5. Flowchart of the online intelligent alarm processing.

As shown in Fig. 5, the key steps of the truth evaluation for the hypotheses are as follows:

d) Judge whether G_k meets the condition, $t_{\text{current}} \not\subset W(G_k)$. If yes, turn to step e).

e) The ORs of all the candidate hypotheses in G_k are calculated according to (3).

f) According to the calculation results in step e), several different procedures are carried out as detailed below:

- If only one candidate hypothesis c_i in G_k satisfies the following condition:

$$\text{Occurrence}(c_i) = 100\% \cap c_i \in G_k \cap t_{\text{current}} \not\subset W(G_k) \cap G_k \in S \quad (5)$$

then it is known that c_i is true and represents that all of the expected alarms in $\text{Expected}(c_i)$ match the real-time alarms completely. Consequently, the cause of the fault/disturbance can be obtained

$$R(G_k) = \{c_i | \text{Occurrence}(c_i) = 100\% \cap c_i \in G_k \cap t_{\text{current}} \not\subset W(G_k) \cap G_k \in S\}$$

where $R(G_k)$ is the evaluation result of G_k.

- If the ORs of all candidate hypotheses in G_k do not equal 100% but only one candidate hypothesis from these hypotheses has the maximum OR value, then the candidate hypothesis with the maximum OR value should be selected as the alarm-processing result

$$\begin{aligned} \text{Occurrence}_{\max} &= \text{maximize}\{\text{Occurrence}(c_i) | \\ &\quad c_i \in G_k \cap t_{\text{current}} \not\subset W(G_k) \cap G_k \in S\} \\ R(G_k) &= \{c_i | \text{Occurrence}(c_i) = \text{Occurrence}_{\max}\} \end{aligned} \quad (6)$$

where $\text{maximize}\{\}$ is used to maximize the term included in $\{\}$.

It can be found that some alarms are missing in this situation: if $y_r = 0$, and a_j is the expected alarm corresponding to y_r in $\text{Expected}(c_i)$, it could then be inferred that a_j should have been received but, in fact, it has not been (i.e., a_j is a missing alarm).

- If more than one candidate hypotheses in G_k that was calculated in step e) satisfies (5) or (6), then turn to step g).

g) First, the example shown in Fig. 3 is employed to illustrate the CR function. Suppose that all of the expected alarms corresponding to c_1 and c_2 in the example (i.e., a_1, a_2, a_3, and a_4) have been reported, then the ORs of c_1 and c_2 could be calculated as $\text{Occurrence}(c_1) = 100\%$ and $\text{Occurrence}(c_2) = 100\%$. In this case, the cause of the fault/disturbance cannot be definitely identified by employing the ORs only. Therefore, if two or more ORs satisfy (5) or (6), the CRs will also be required in order to identify the cause of a fault/disturbance. The candidate hypothesis in G_k which not only satisfies (5) or (6) but also has the maximum CR is selected as the final alarm-processing result

$$\begin{aligned} \text{Coverage}_{\max} &= \text{maximize}\{\text{Coverage}(c_i) | \\ &\quad c_i \in G_k \cap t_{\text{current}} \not\subset W(G_k) \cap G_k \in S\} \\ R(G_k) &= \{c_i | \text{Occurrence}(c_i) = \text{Occurrence}_{\max} \\ &\quad \cap \text{Coverage}(c_i) = \text{Coverage}_{\max}\}. \end{aligned}$$

The example shown in Fig. 3 is employed to illustrate again. The CRs of c_1 and c_2 are calculated according to (4) and the results are obtained $\text{Coverage}(c_1) = 50\%$ and $\text{Coverage}(c_2) = 100\%$. Consequently, c_2 is deemed as the final result.

TABLE II
REPORTED ALARM MESSAGES

Timestamp (ms)	MMS Variable Object	Value Change	Content	Type
11	PCOS_ PZB2 /chkGGIO1STInd15$stVal	**0→1**	The self-check for main PR of T2 was in error	Protection self-check
29	PCOS_PZB1M/Q0GGIO4STInd31$stVal	**0→1**	The goose of the communication device of the backup PR for T1 was broken off	Network communication
32	PCOS_P10LINE5/ Q0GGIO5STInd12$stVal	**1→0**	The goose of the communication device of L918 was broken off	Network communication
50	PCOS_P35LINE3/Q0PTOC1STOp$general	**0→1**	The main PR of L313 operated	PR operation
1550	PCOS_PZB1M/Q0PTOC1STOp$general	**0→1**	The main PR of the middle backup device for T1 operated	PR operation
1580	PCOS_P35LINE6/chkGGIO21STInd4$stVal	**0→1**	The self-check for main PR of L316 was in error	Protection self-check
1599	PCOS_P35FD/Q0XCBR1STPos$stVal	**0→1**	C331 tripped	CB tripping
1652	PCOS_PZB1M/Q0PTOC3STOp$general	**0→1**	The backup PR of the middle backup device for T1 operated	PR operation
1702	PCOS_PZB1M/Q0XCBR1STPos$stVal	**0→1**	C301 tripped	CB tripping
1986	PCOS_P110LINE1/Q0GGIO2STInd1$stVal	**1→0**	The goose of the communication device of L111 was broken off	Network communication
2550	PCOS_P10LINE5/Q0PTOC11STOp$general	**0→1**	The main PR of L918 operated	PR operation
2562	PCOS_P10LINE5/Q0XCBR1STPos$stVal	**0→1**	C918 tripped	CB tripping
4505	PCOS_PZB2L/Q0PTOC1STOp$general	**0→1**	The main PR of the low backup device for T2 operated	PR operation
4566	PCOS_P10FD/Q0XCBR1STPos$stVal	**0→1**	C931 tripped	CB tripping
4610	PCOS_PZB2L/Q0PTOC3STOp$general	**0→1**	The backup PR of the low backup device for T2 operated	PR operation
4673	PCOS_PZB2L/Q0XCBR1STPos$stVal	**0→1**	C902 tripped	CB tripping
6087	PCOS_PZB1CD/Q0PDIF1STOp$general	**0→1**	The main PR of T2 operated	PR operation

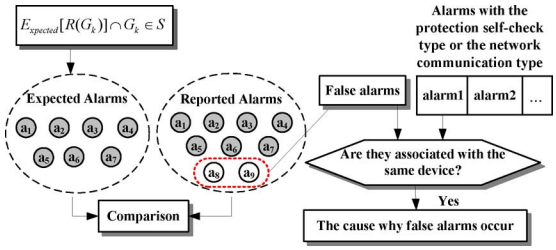

Fig. 6. Processes of identifying the false alarms and the cause of their occurrences.

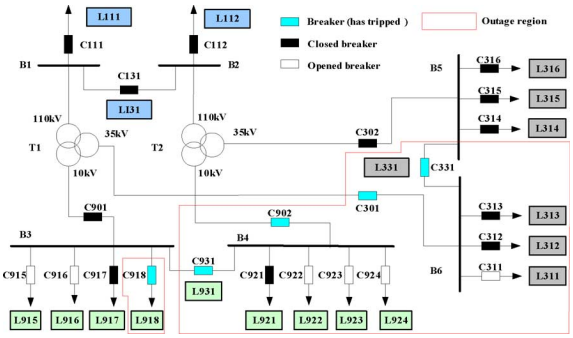

Fig. 7. Diagram of the Xingguo Substation in Ganzhou, Jiangxi Province, China.

h) If all of the hypotheses in S have been processed, the false alarms can be obtained. Suppose that $R = \{R(G_k)|G_k \in S\}$ is a collection of the evaluation results of all the hypotheses. Then, the expected alarms corresponding to all of the elements in R (i.e., Expected$(R(G_k)) \cap G_k \in S$) are compared with all of the PR operating and CB tripping alarms reported. Consequently, some reported alarms that do not match the expected alarms are considered false alarms. As shown in Fig. 6, a_8 and a_9 are considered to be false alarms.

As shown in Fig. 6, if an alarm with the protection self-check type or the network communication type is associated with the same device as the one of the false alarm, it can be inferred that the occurrence of the false alarm is caused by the malfunctioned protection devices or network communication devices. For instance, suppose that the alarm a_8 in Fig. 6 represents that "The main PR of L_1 operated." If an alarm of the protection self-check type which represents "the self-check for the main PR of L_1 was in error," and a_8 is received, then it can be inferred that the malfunction of the main PR of L_1 causes an unexpected alarm a_8.

V. APPLICATION EXAMPLES

The online intelligent alarm-processing system is implemented by using C# under the platform of Visual Studio 2005. Many test examples and actual scenarios have been used to demonstrate the correctness of the presented alarm-processing

TABLE III
ENCODING OF ALARM MESSAGES

Encoding	Content	Encoding	Content
a_1	The main PR of L313 operated	a_{16}	C921 tripped
a_2	The backup PR of L313 operated	a_{17}	The main PR of the low backup device for T2 operated
a_3	C313 tripped	a_{18}	C931 tripped
a_4	The main PR of the middle backup device for T1 operated	a_{19}	The backup PR of the low backup device for T2 operated
a_5	C331 tripped	a_{20}	C902 tripped
a_6	The backup PR of the middle backup device for T1 operated	a_{21}	The main PR of T2 operated
a_7	C301 tripped	a_{22}	C112 tripped
a_8	The main PR of L312 operated	a_{23}	C131 tripped
a_9	The backup PR of L312 operated	a_{24}	C302 tripped
a_{10}	C312 tripped	a_{25}	The self-check for main PR of T2 was in error
a_{11}	The main PR of L918 operated	a_{26}	The goose of the communication device of the backup PR for T1 was broken off
a_{12}	The backup PR of L918 operated	a_{27}	The goose of the communication device of L918 was broken off
a_{13}	C18 tripped	a_{28}	The self-check for main PR of L316 was in error
a_{14}	The main PR of L921 operated	a_{29}	The goose of the communication device of L111 was broken off
a_{15}	The backup PR of L921 operated		

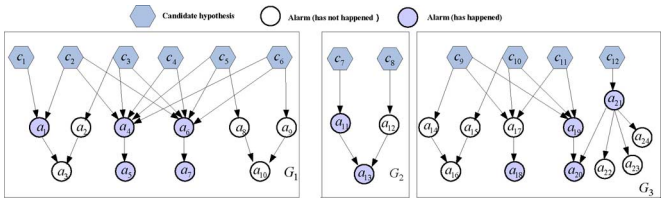

Fig. 8. Rule network corresponding to the test scenario.

approach and the computational efficiency of the developed online intelligent alarm-processing system. The software system has been applied successfully in the Xingguo digital substation in Jiangxi Province, China. A detailed alarm-processing scenario in the Xingguo digital substation is presented here for illustrating the proposed approach and the developed software system. The structure of the substation is shown in Fig. 7, and the reported real-time alarms are listed in Table II.

For the convenience of presentation, the corresponding alarms and the candidate hypotheses are encoded as shown in Tables III and IV, respectively. Due to space limitations, only some important rules are listed in Table V. Then, a rule network is established and shown in Fig. 8. As shown in Table II, the reported alarms in the time interval [11 ms, 6087 ms] are $\{a_1, a_4, a_5, a_6, a_7, a_{11}, a_{13}, a_{18}, a_{19}, a_{20}, a_{21}, a_{25}, a_{26}, a_{27}, a_{28}, a_{29}\}$. Then, the detailed alarm-processing process is illustrated as follows:

1) Alarm classifications. Based on the IEC 61850 standard, the reported real-time alarms are classified into four types according to Table II:
   a) a_{25} and a_{28} belong to the protection self-check type;
   b) a_{26}, a_{27} and a_{29} belong to the network communication type;
   c) $a_1, a_4, a_6, a_{11}, a_{19}$, and a_{21} belong to the PR operation type;
   d) a_5, a_7, a_{13}, a_{18}, and a_{20} belong to the breaker tripping type.

   Since the alarms associated with PR operation and CB tripping are involved in the real-time alarm queue, the module of online intelligent alarm processing is then activated.
2) The generation of the candidate hypotheses. First, all of the candidate hypotheses are inferred according to (1) and the results are listed in Table VI. Then, the related candidate hypotheses are classified into the same hypothesis set according to (2). As shown in Fig. 8, three hypothesis sets $G_1 = \{c_1, c_2, c_3, c_4, c_5, c_6\}, G_2 = \{c_7, c_8\}$ and $G_3 = \{c_9, c_{10}, c_{11}, c_{12}\}$ are built up according to the relationships of the candidate hypotheses and then stored into $S = \{G_1, G_2, G_3\}$. Suppose that T is set as 10 s, the corresponding time windows of G_1, G_2, and G_3 can be determined as $W(G_1) = [11\text{ ms}, 10011\text{ ms}], W(G_2) = [2550\text{ ms}, 12550\text{ ms}]$ and $W(G_3) = [4505\text{ ms}, 14505\text{ ms}]$.
3) The truth evaluation for the hypotheses of G_1, G_2 and G_3:
   a) According to step d) in Section IV, once $t_{\text{current}} \notin W(G_1)$ (i.e., $t_{\text{current}} > 10011$ ms), the ORs of all candidate hypotheses in G_1 are calculated according to (3) and the results are listed in Table VII. For instance, $E_{\text{xpected}}(c_1) = \{a_1, a_3\}$. Since a_1 has occurred ($y_1 = 1$) and a_3 has not yet occurred ($y_2 = 0$), then the OR of c_1 is determined as

TABLE IV
ENCODING OF CANDIDATE HYPOTHESIS

Encoding	Alarms	Encoding	Alarms
c_1	A fault occurred on L313 and the main PR of L313 operated	c_7	A fault occurred on L918 and the main PR of L918 operated
c_2	A fault occurred on L313 and the main PR of L313 operated, but C313 failed to trip	c_8	A fault occurred on L918 but the main PR of L918 failed to operate, so that the backup PR of L918 operated
c_3	A fault occurred on L313 but the main PR of L313 failed to operate, so that the backup PR of L313 operated but C313 failed to trip	c_9	A fault occurred on L921 and the main PR of L921 operated, but C921 failed to trip
c_4	A fault occurred on B6	c_{10}	A fault occurred on L921 but the main PR of L921 failed to operate, so that the backup PR of L921 operated but C921 failed to trip
c_5	A fault occurred on L312 and the main PR of L313 operated, but C312 failed to trip	c_{11}	A fault occurred on B4
c_6	A fault occurred on L312 but the main PR of L312 failed to operate, so that the backup PR of L312 operated but C312 failed to trip	c_{12}	A fault occurred on T2

TABLE V
RULE BASE

Rules									
(c_1, a_1)	(c_2, a_1)	(c_2, a_4)	(c_2, a_6)	(c_3, a_2)	(c_3, a_4)	(c_3, a_6)	(c_4, a_4)	(c_4, a_6)	(c_5, a_4)
(c_5, a_6)	(c_5, a_8)	(c_6, a_4)	(c_6, a_6)	(c_6, a_9)	(c_7, a_{11})	(c_8, a_{12})	(c_9, a_{14})	(c_9, a_{17})	(c_9, a_{19})
(c_{10}, a_{15})	(c_{10}, a_{17})	(c_{10}, a_{19})	(c_{11}, a_{17})	(c_{11}, a_{19})	(c_{12}, a_{21})	(a_1, a_3)	(a_2, a_3)	(a_4, a_5)	(a_6, a_7)
(a_8, a_{10})	(a_9, a_{10})	(a_{11}, a_{13})	(a_{12}, a_{13})	(a_{14}, a_{16})	(a_{15}, a_{16})	(a_{17}, a_{18})	(a_{19}, a_{20})	(a_{21}, a_{20})	(a_{21}, a_{22})
(a_{21}, a_{23})	(a_{21}, a_{24})								

TABLE VI
CORRESPONDING $C_{\text{ause}}(a_j)$ OF a_j

a_j	$C_{ause}(a_j)$	a_j	$C_{ause}(a_j)$	a_j	$C_{ause}(a_j)$	a_j	$C_{ause}(a_j)$
a_1	c_1, c_2	a_4	c_2, c_3, c_4, c_5, c_6	a_5	c_2, c_3, c_4, c_5, c_6	a_6	c_2, c_3, c_4, c_5, c_6
a_7	c_2, c_3, c_4, c_5, c_6	a_{11}	c_7	a_{13}	c_7, c_8	a_{17}	c_9, c_{10}, c_{11}
a_{18}	c_9, c_{10}, c_{11}	a_{19}	c_9, c_{10}, c_{11}	a_{20}	$c_9, c_{10}, c_{11}, c_{12}$	a_{21}	c_{12}

$O_{\text{ccurrence}}(c_1) = (y_1 + y_2)/(2) \times 100\% = 50\%$. As shown in Table VII, since two ORs of these candidate hypotheses are equal to 100% (i.e., Occurrence$(c_2) = 100\%$ and Occurrence$(c_4) = 100\%$, the final result cannot be determined definitely. As the result, the CRs of c_2 and c_4 also need to be calculated according to (4), and the calculation results are shown in Table VIII. For instance, $E_{\text{xpected}}(c_2) = \{a_1, a_4, a_5, a_6, a_7\}$. Since all five expected alarms have occurred $(y_1 = y_2 = y_3 = y_4 = y_5 = 1)$, then $C_{\text{overage}}(c_2) = (y_1 + y_2 + y_3 + y_4 + y_5)/(5) \times 100\% = 100\%$. As shown in Table VIII, because $C_{\text{overage}}(c_4) = 80\% < C_{\text{overage}}(c_2)$, then c_2 is the solution hypothesis of G_1.

b) Once $t_{\text{current}} \not\subset W(G_2)$ holds (i.e., $t_{\text{current}} > 12550$ ms, the ORs of all candidate hypotheses in G_2 are calculated according to (3). The evaluation results are also listed in Table VII. It is obvious that Occurrence$(c_7) = 100\%$ is the solution of G_2.

c) Once $t_{\text{current}} \not\subset W(G_3)$ holds (i.e., $t_{\text{current}} > 14505$ ms), the ORs of all candidate hypotheses in G_3 are calculated according to (3), and the results are listed in Table VII. It is obvious that Occurrence$(c_{11}) = 75\%$ is the solution of G_3.

4) Analysis of alarm-processing results.

a) Three faults have occurred in the system. The hypotheses c_2, c_7, and c_{11} are selected as the final alarm-processing results (i.e., "A fault occurred on L313 and the main PR of L313 operated, but C313 failed to open," "A fault occurred on L918 and the main PR of L918 operated," and "A fault occurred on B4").

b) Since Occurrence$(c_2) = 100\%$ and Occurrence$(c_7) = 100\%$, there is not any missing alarm in G_1 and G_2. However,

TABLE VII
CORRESPONDING $O_{\text{ccurrence}}(c_i)$ OF c_i

G_z	c_i	$E_{xpected}(c_i)$	y_r **corresponding to** $E_{xpected}(c_i)$	$O_{ccurrence}(c_i)$
G_1	c_1	$\underline{a_1}, a_3$	$y_1=1, y_2=0$	50%
	c_2	$\underline{a_1}, \underline{a_4}, \underline{a_5}, \underline{a_6}, \underline{a_7}$	$y_1=1, y_2=1, y_3=1, y_4=1, y_5=1$	100%
	c_3	$a_2, \underline{a_4}, \underline{a_5}, \underline{a_6}, \underline{a_7}$	$y_1=0, y_2=1, y_3=1, y_4=1, y_5=1$	80%
	c_4	$\underline{a_4}, \underline{a_5}, \underline{a_6}, \underline{a_7}$	$y_1=1, y_2=1, y_3=1, y_4=1$	100%
	c_5	$\underline{a_4}, \underline{a_5}, \underline{a_6}, \underline{a_7}, a_8$	$y_1=1, y_2=1, y_3=1, y_4=1, y_5=0$	80%
	c_6	$\underline{a_4}, \underline{a_5}, \underline{a_6}, \underline{a_7}, a_9$	$y_1=1, y_2=1, y_3=1, y_4=1, y_5=0$	80%
G_2	c_7	$\underline{a_{11}}, \underline{a_{13}}$	$y_1=1, y_2=1$	100%
	c_8	$a_{12}, \underline{a_{13}}$	$y_1=0, y_2=1$	50%
G_3	c_9	$a_{14}, a_{17}, \underline{a_{18}}, \underline{a_{19}}, \underline{a_{20}}$	$y_1=0, y_2=0, y_3=1, y_4=1, y_5=1$	60%
	c_{10}	$a_{15}, a_{17}, \underline{a_{18}}, \underline{a_{19}}, \underline{a_{20}}$	$y_1=0, y_2=0, y_3=1, y_4=1, y_5=1$	60%
	c_{11}	$a_{17}, \underline{a_{18}}, \underline{a_{19}}, \underline{a_{20}}$	$y_1=0, y_2=1, y_3=1, y_4=1$	75%
	c_{12}	$\underline{a_{20}}, \underline{a_{21}}, a_{22}, a_{23}$	$y_1=1, y_2=0, y_3=0, y_4=0$	50%

Note: $\underline{a_j}$ represents the alarm that has happened; a_j represents the alarm that has not happened.

TABLE VIII
CORRESPONDING $C_{\text{overage}}(c_i)$ OF c_2 AND c_4

c_i	$E_{xpected}(c_i)$	$C_{overage}(c_i)$	c_i	$E_{xpected}(c_i)$	$C_{overage}(c_i)$
c_2	a_1, a_4, a_5, a_6, a_7	100%	c_4	a_4, a_5, a_6, a_7	80%

TABLE IX
DETERMINATION OF FALSE ALARMS

Results	$E_{xpected}(c_i)$ **responding to** c_2, c_7 and c_{11}	**The reported alarms of PR operation and CB tripping type**	**False alarms**
c_2, c_7, c_{11}	$a_1, a_4, a_5, a_6, a_7, a_{11}, a_{13}, a_{17}, a_{18}, a_{19}, a_{20}$	$a_1, a_4, a_5, a_6, a_7, a_{11}, a_{13}, a_{18}, a_{19}, a_{20}, a_{21}$	a_{21}

Occurrence$(c_{11}) = 75\%$, so a_{17} is identified to be the missing alarm in G_3.

c) According to step h) in Section IV, by comparing the expected alarms corresponding to c_2, c_7, and c_{11}. with all of the reported alarms as shown in Table IX, the reported alarm a_{21} (i.e., "the main PR of T2 operated)" is identified as a false alarm that should not have occurred but actually had been received. Moreover, since the alarm a_{25} (i.e., "the self-check for main PR of T2 was in error)" has also been received, the reason for the false alarm occurrence can be identified as the malfunction of the main PR of T2.

It is demonstrated that the alarm-processing results are consistent with the actual scenarios.

VI. CONCLUSION

Based on the architecture of digital substations, a systematic alarm-processing approach and a further online intelligent alarm-processing system are developed in this paper. Not only can the developed software system classify the real-time alarms according to the IEC 61850 standard, but it can also find out the cause of a fault/disturbance, missing or false alarms, as well as the causes of the false alarms' occurrences. It has been demonstrated by many test examples and actual scenarios that the proposed approach is correct, and the developed software system can meet the requirements of online alarm processing in actual power systems.

REFERENCES

[1] H. J. Lee, B. S. Ahn, and Y. M. Park, "A fault diagnosis expert system for distribution substations," *IEEE Trans. Power Del.*, vol. 15, no. 1, pp. 92–97, Jan. 2000.

[2] J. W. Jung, C. C. Liu, M. G. Hong, M. Gallanti, and G. Tornielli, "Multiple hypotheses and their credibility in on-line fault diagnosis," *IEEE Trans. Power Del.*, vol. 16, no. 2, pp. 225–230, Apr. 2001.

[3] Y. C. Huang, "Fault section estimation in power systems using a novel decision support system," *IEEE Trans. Power Syst.*, vol. 17, no. 2, pp. 439–444, May 2002.

[4] W. H. Chen, C. W. Liu, and M. S. Tsai, "On-line fault diagnosis of distribution substations using hybrid cause-effect network and fuzzy rule-based method," *IEEE Trans. Power Del.*, vol. 15, no. 2, pp. 710–717, Apr. 2000.

[5] G. Cardoso, J. G. Rolim, and H. H. Zurn, "Identifying the primary fault section after contingencies in bulk power systems," *IEEE Trans. Power Del.*, vol. 23, no. 3, pp. 1335–1342, Jul. 2008.

[6] H. J. Miao, M. Sforna, and C. C. Liu, "A new logic-based alarm analyzer for on-line operational environment," *IEEE Trans. Power Syst.*, vol. 11, no. 3, pp. 1600–1606, Aug. 1996.
[7] G. J. Cardoso, J. G. Rolim, and H. H. Zurn, "Application of neural-network modules to electric power system fault section estimation," *IEEE Trans. Power Del.*, vol. 19, no. 3, pp. 1034–1041, Jul. 2004.
[8] A. P. Alves da Silva, A. H. F. Insfran, P. M. da Silveira, and G. Lambert-Torres, "Neural networks for fault location in substations," *IEEE Trans. Power Del.*, vol. 11, no. 1, pp. 234–239, Jan. 1996.
[9] G. Rigatos, P. Siano, and A. Piccolo, "Neural network-based approach for early detection of cascading events in electric power systems," *Inst. Eng. Technol. Gen., Transm. Distrib.*, vol. 3, no. 7, pp. 650–665, Jul. 2009.
[10] Y. C. Huang, H. T. Yang, and K. Y. Huang, "Abductive network model-based diagnosis system for power transformer incipient fault detection," in *Proc. Inst. Elect. Eng., Gen., Transm. Distrib.*, May 2002, vol. 149, no. 3, pp. 326–330.
[11] F. S. Wen and C. S. Chang, "Tabu search approach to alarm processing in power systems," *Proc. Inst. Elect. Eng., Gen., Transm. Distrib.*, vol. 144, no. 1, pp. 31–38, 1997.
[12] W. X. Guo, F. S. Wen, Z. W. Liao, L. H. Wei, and J. B. Xin, "An analytic model-based approach for power system alarm processing employing temporal constraint network," *IEEE Trans. Power Del.*, vol. 25, no. 4, pp. 2435–2447, Oct. 2010.
[13] F. S. Wen, C. S. Chang, and W. H. Fu, "New approach to alarm processing in power systems based upon the set covering theory and a refined genetic algorithm," *J. Elect. Mach. Power Syst.*, vol. 26, no. 1, pp. 53–67, 1998.
[14] D. Srinivasan, R. L. Cheub, Y. P. Poh, and A. K. C. Ng, "Automated fault detection in power distribution networks using a hybrid fuzzy-genetic algorithm approach," *Eng. Appl. Artif. Intell.*, vol. 13, no. 4, pp. 407–418, Aug. 2000.
[15] K. L. Lo, H. S. Ng, and J. Trecat, "Power systems fault diagnosis using Petri nets," *Proc. Inst. Elect. Eng., Gen., Transm. Distrib.*, vol. 144, no. 3, pp. 231–236, May 1997.
[16] K. L. Lo, H. S. Ng, and J. Trecat, "Extended Petri-net models for fault diagnosis for substation automation," in *Proc. Inst. Elect. Eng., Gen. Transm. Distrib.*, May 1999, vol. 146, no. 3, pp. 229–234.
[17] X. Luo and M. Kezunovic, "Implementing fuzzy reasoning Petri-nets for fault section estimation," *IEEE Trans. Power Del.*, vol. 23, no. 2, pp. 676–685, Apr. 2008.
[18] J. Sun, S. Y. Qin, and Y. H. Song, "Fault diagnosis of electric power systems based on fuzzy Petri nets," *IEEE Trans. Power Syst.*, vol. 19, no. 4, pp. 2053–2059, Nov. 2004.
[19] P. Jarventausta, P. Verho, and J. Partanen, "Using fuzzy sets to model the uncertainty in the fault location process of distribution networks," *IEEE Trans. Power Del.*, vol. 9, no. 2, pp. 954–960, Apr. 1994.
[20] S. W. Min, J. M. Sohn, J. K. Park, and K. H. Kim, "Adaptive fault section estimation using matrix representation with fuzzy relations," *IEEE Trans. Power Syst.*, vol. 19, no. 2, pp. 842–848, May 1994.
[21] C. L. Hor and P. A. Crossley, "Unsupervised event extraction within substations using rough classification," *IEEE Trans. Power Del.*, vol. 21, no. 4, pp. 1809–1816, Oct. 2006.
[22] C. L. Hor and P. A. Crossley, "Building knowledge for substation-based decision support using rough sets," *IEEE Trans. Power Del.*, vol. 22, no. 3, pp. 1372–1379, Jul. 2007.
[23] *IEC. Communication Networks and Systems in Substations*, IEC Std. 61850, 2003.
[24] T. S. Sidhu and P. K. Gangadharan, "Control and automation of power system substation using IEC 61850 communication," in *Proc. IEEE Conf. Control Applications*, Toronto, ON, Canada, Aug. 28–31, 2005, pp. 1331–1336.
[25] R. E. Mackiewicz, "Overview of IEC 61850 and benefits," presented at the IEEE Power Eng. Soc. Gen. Meeting, Montreal, QC, Canada, 2006.

Liuhong Wei is a postgraduate student in South China University of Technology, China. Her main research interests are power system alarm processing, fault diagnosis, and system restoration.

Wenxin Guo is an Engineer with the Guangdong Power Dispatching Center, Guangzhou, China. His main research interests are power system alarm processing and fault diagnosis.

Fushuan Wen received the B.E. and M.E. degrees in electrical engineering from Tianjin University, China, in 1985 and 1988, respectively, and the Ph.D. degree in electrical engineering from Zhejiang University, China, in 1991.

He joined the faculty of Zhejiang University in 1991, and has been a Full Professor and the Director of the Institute of Power Economics and Information since 1997. He was a University Distinguished Professor, the Deputy Dean of the School of Electrical Engineering, and the Director of the Institute of Power Economics and Electricity Markets at the South China University of Technology (SCUT), China, from 2005 to 2009. His research interests are power industry restructuring, power system alarm processing, fault diagnosis and restoration strategies, as well as artificial-intelligence applications in power systems.

Gerard Ledwich (SM'89) received the Ph.D. degree in electrical engineering from the University of Newcastle, Newcastle, Australia, in 1976.

He has been Chair Professor in Electrical Asset Management with the Queensland University of Technology (QUT), Brisbane, Australia, since 1998. His interests are in the areas of power systems, power electronics, and controls.

Prof. Ledwich is a Fellow of I.E. Australia.

Zhiwei Liao received the Ph.D. degree in electrical engineering from Tianjin University, China, in 2002.

Currently, he is an Associate Professor with South China University of Technology, China. His research interests are power system alarm processing, fault diagnosis, and intelligent control.

Jianbo Xin received the Ph.D. degree in electrical engineering from Huazhong University of Science and Technology, China.

Currently, he is a Senior Engineer with Jiangxi Electric Power Research Institute, China. His research interests are power system alarm processing and fault diagnosis.