Design and Research of Distribution Network Firewall Protection Terminal

Youchan Zhu
School of Control and Computer Engineering
North China Electric Power University
Baoding, China
zyc_hd@sina.com

Jing Qiu *
School of Control and Computer Engineering
North China Electric Power University
Baoding, China
learning_qj@sina.com
* Corresponding Author

Abstract— In order to decrease the influence of failure occurred in the distribution network, and improve the reliability, this paper proposes a design of the distribution network firewall protection terminal. Statements are described in detail, including the overall architecture of the system, the communication protocol, the systematic workflow, and distribution network topology analysis, as well as fault location algorithm. The firewall is applied to "hand in hand" circular distribution network to analyze faults. The firewall which uses STM32F417 as the core has been successfully applied to somewhere, until now it has shown the advantages of stable operation and superior performance, finally demonstrated the effectiveness of the firewall terminal.

Keywords-distribution network firewall; topology analysis; fault location; "hand in hand" circular distribution network; STM32F417

I. INTRODUCTION

With the development of smart grid[1], the State Grid Corporation has made it clear that transmission, substation, distribution, consumption, scheduling and other aspects of intelligent building should be carried out [2, 3]. In this situation, this paper studies on links in the intelligent distribution network[4]. The proposed distribution network firewall is a device to isolate faults in the distribution network, decreasing the number of trips of substation outlet switches and ensuring the operational reliability of the distribution network. Protection of distribution network firewall network is based on the high-speed fiber-optic Ethernet communication, combined with precise electronic and information technology, and advanced protection technology[5,6]. By analyzing the distribution network topology, the trip node and the backup node can be positioned, and then some operations would be performed to handle the problem. The purpose of reducing the fault spreading range is achieved by this way..

II. OVERALL STRUCTURE

The overall structure of the distribution network firewall protection terminal is shown in Fig. 1. Figures indicate the data stream, specifically 0 represents the data stream of system log module, 1 represents the data stream of the FRAM, 2 represents the data stream of the FLASH, 3 represents the data stream of the USB, 4 represents the data stream of the SD card, 5 represents the data stream of the RTC, 6 represents the data stream of the temperature module, 7 represents the data stream of the GPRS module, 8 represents the data stream of the serial debugging module, 9 represents the data stream of the Bluetooth module, 10 represents the data stream of the timer module, 11 represents the data stream of the ADC module, 12 represents the data stream of the Lwip protocol stack [7] , and 13 represents the data stream of the PTPv2 protocol stack [8]. As it can be seen from Fig. 1, the terminal is designed to use the modular design concept [9], and in order to enhance the reusability of code, each module is subdivided into hardware-independent logical layer and hardware-related physical layer, so if the hardware is replaced, it is only needed to modify the code of physical layer, greatly enhancing the maintainability of the system. The embedded real-time operating system uCOS-III is used in the terminal [10,11] which also integrates embedded Ethernet communication protocol Lwip and PTPv2, so that the terminal can support high-speed Ethernet data transmission. Additionally, the terminal also joins Bluetooth and GPRS to provide a wireless data transmission capability.

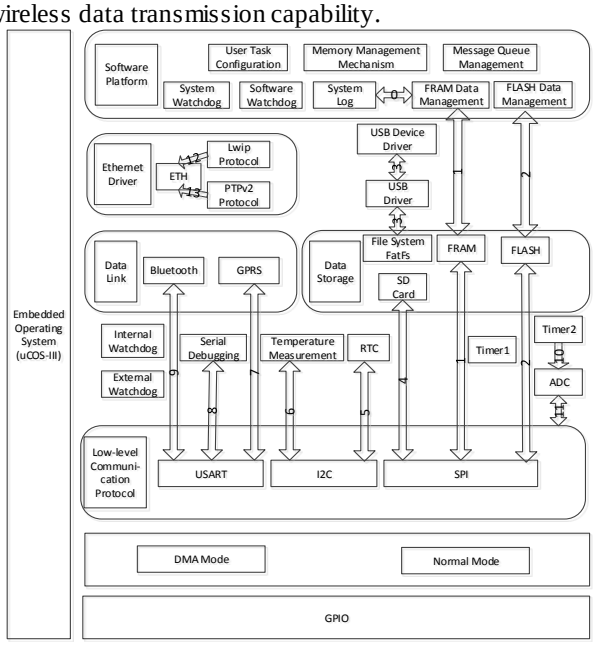

Figure 1. Structure diagram of distribution network firewall protection terminal

III. COMMUNICATION PROTOCOL

A. Packet Structure

TABLE I. COMMUNICATION PACKET

Node ID	Sequence number	Function code
1 byte	1 byte	1 byte
Length	Content	
2 bytes		

Tab. 1 is the communication packet of the distribution network firewall terminal. The following is a detailed description.

1) Node ID

- In unicast communication, the source node ID is for uplink packets, and the destination node ID is for downlink packets.
- The node ID of broadcast packets is fixed at 0xFF.
- 0 is not available.

2) Sequence number

- It is initialized to 0 after power up.
- Plus 1 after sending a new packet.
- Avoid processing retransmitted packets.

3) Function code

As is shown in Tab. 2.

TABLE II. PACKET TYPE

Values	Explanations
0x01	Heartbeat
0x81	Heartbeat Reply
0x02	Fault Report
0x82	Specifying the failed node and backup node
0x83	Switching setting group number

4) Length

The length in bytes of the content of a packet.

B. Packet format

1) Fault packet (the controlled node → the master node)

TABLE III. FAULT PACKET

No.	Contents	Data values (hexadecimal)	Remark
0	Node ID	0x??	
1	Sequence number	0x??	
2	Function code	0x02	
3	Length	0x01	
4		0x00	
5	Fault power direction	0x??	forward, negative

2) Specifying the fault node and the backup node (the master node → the controlled node)

TABLE IV. PACKET FORMAT TO SPECIFY THE FAULT NODE AND THE BACKUP NODE

No.	Contents	Data values (hexadecimal)	Remark
0	Node ID	0xFF	
1	Sequence number	0x??	
2	Function code	0x82	
3	Length	0x04	
4		0x00	
5	Failed node ID	0x??	
6	Backup node ID	0x??	

3) Switching setting group number

The packet is a broadcast message, and will be retransmitted three times by the master node.

TABLE V. SWITCHING SETTING GROUP NUMBER PACKET

No.	Contents	Data values (hexadecimal)	Remark
0	Node ID	0xFF	
1	Sequence number	0x??	
2	Function code	0x83	
3	Length	0x??	Extension number of nodes × 2
4		0x??	
5	ID of the value transformation node 1	0x??	
6	The new setting group 1		
7	ID of the value transformation node 2	0x??	
8	The new setting group 2	0x??	
9	...	0x??	
10	...	0x??	

IV. KEY PROCESSES

Fig. 2 is an overall flow of distribution network firewall protection terminal. The details are described as follows.

(1) The device registers to the master node after power up by sending heartbeat packets which contains the node ID, the current switch status, the direction of the current power, the voltage status, the switch status, and the voltage change of status. The master node replies the corresponding node type which is set up in the configuration file.

(2) After receiving a reply from the master node, the node successfully registers. After the power is on, the master node starts a registration delay timer, and the timeout signal is considered to be all the normal communication nodes which have been registered, and then the main control node sends a setting group number to each node. The way to switch the setting group number is broadcast a message which includes the node ID and a setting group number three times.

(3) After registration delay expires, the heartbeat flow is regarded as the identity of normal communication. If the communication is not normal, a stand-alone protection process should be performed. After communication is restored, the master node sends relevant messages to those which need to change the setting group number. After the

heartbeat timeout, the master node does not receive heartbeat packets, and a conclusion should be drawn that node communication is not normal, then the implementation of the relevant processes.

(4) After the protection of the failure node is started, fault packets should be sent to the master node by unicasting three ways. Especially, each packet contains faulty power direction. Communications lockout timer starts counting. All packets need to add a sequence number, however, the sequence number of retransmitted packets does not increase.

(5) The master node collects fault information of all nodes, after the maximum communication delay, the distribution network topology would be analyzed to identify the action node and the backup node. After the failure analysis is complete, the master node broadcast the command message to all the nodes three times, and the message contains the action node ID and the backup node ID.

(6) After communicating lockout time expires, nodes which received tripping instructions trip, and which received backup node instructions play protection blocking delay, and within the protection lockout time, protection is not exported. After the protection lockout expires, if the fault is not removed, the backup node performs protective actions. Other nodes that don't receive packets trip locking

(7) The information of the change of the switch, the power direction or the voltage status in non-master nodes is reported by the heartbeat message.

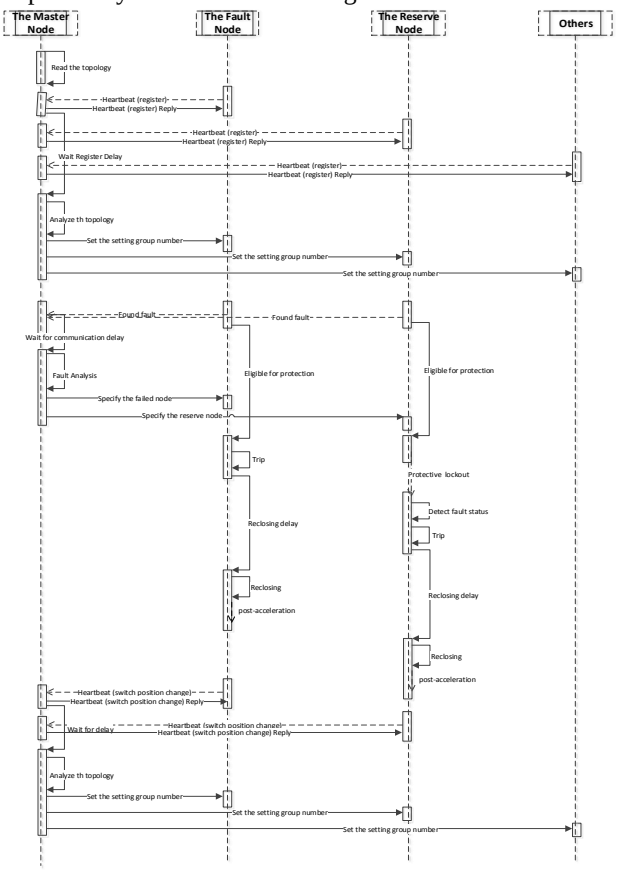

Figure 2. An overall flow of distribution network firewall protection terminal.

V. ALGORITHMS

A. Key data structure

```
struct
{
uint 8 _t u8Parent ID;      /* Parent node ID */
uint 8 _t u8Sibling ID;     /* Sibling node ID */
uint 8 _t u8ChildID;        /* Child node ID */
} TopoNode;
struct
{
 NodeTypeType eNodeType;    /* Node type */
 CommStateType eCommState;  /* Communication status */
uint8_t u8TimeToLive;       /* node lifetime, and 0 is the sign of a communication error. This value reduces 1 after each heartbeat cycle. The initial value of node lifetime should be greater than 1. */
 BreakerStateType eBreakerSwitchState; /* Node switching state. When the switch operation is not determined, the state does not upload. When the switch fails, the node does not continue to carry the heartbeat.*/
PowerDirType ePowerDir;     /* Node power direction. */
VoltageStateType eVoltageState;  /* Charged state. */
uint8_t au8MacAddr[6];      /* MAC address of the node. */
FaultStateType eFaultState; /* Node failure state. */
uint8_t u16TopoTreeID;      /* The topology tree ID or setting group ID. If the branch node is changed, to switch setting group number. */
 uint8_t u8FaultPacketIndex; /* Sequence number of the last fault packet. */
uint8_t u8StatusPacketIndex; /* Sequence number of the last heartbeat packet. */
} TopoNodeDesc;.
```

B. Topology analysis

1) Definition

To be confirmed area: The list of trunk nodes in the current traversal process, which can not be determined the subordinate relationship, is called to be confirmed area. The area includes two kinds of trunk nodes. One is the abnormal communication node, another is normal communication node which the switch state is off and the power is zero.

The node before to be confirmed area: The parent node of the starting node in to be confirmed area.

2) Algorithm description

In this algorithm, topology analysis[12] and setting group number analysis performed at the same time, and while the analysis process of setting group number, if found abnormal communication node, then immediately switching state inference.

Setting group number of the branch node only can be affected by the switching state of the trunk node, therefore just analyze the decisive factor. According to communication state of the trunk node, the following two cases are concluded.

All trunk nodes with normal communication

In this case, starting from the root node of two topology trees, and using BFS algorithm to iterate them, until meeting the node which the switching state is open. The setting group number of the branch node which has been iterated is consistent with owned tree ID, otherwise the setting group number is uncertain.

There is a trunk node with abnormal communication

In this case, two trees are at the root of the tree topology, according to the breadth-first traversal of the tree topology, setting group number traverse to the branch node belongs tree ID consistent, if you encounter communication error node, divided to be confirmed district, then to be confirmed in accordance with the following rules inference abnormal node communication area switching state:

- If the state of the node after to be confirmed area is on, start from the node to analyze level by level, and if the node or any node of its sibling subtrees has power, a conclusion can be drawn, that the state of nodes that between the node and the starting node of to be confirmed area is off. There is no need to operate the node before to be confirmed area.
- If the state of the node after to be confirmed area is off, and the power direction of the node before to be confirmed area is nonzero, additionally, the node after to be confirmed area hold the same power direction with the node before to be confirmed area, then a conclusion can be drawn, that the state of nodes of to be confirmed area is off.

C. Fault location analysis

1) Definition

The end node of the topology tree: Use BFS[13] algorithm to traverse the topology tree to the last trunk node. The node has a feature that its switch status is on or its communication status is abnormal.

2) Algorithm description

The algorithm traverses the two topology trees, and then if the switch status of their end nodes is not fully on, then traversing the branch sub-trees between end nodes of the two topology trees. When using BFS to traverse trees, the first step is to find a faulty node, and then locate the failed node in the child node of the node, and so on, until the fault status of all child nodes are not failed, or no child nodes. The last failed node is a tripping node, and other failed nodes found earlier are backup nodes.

VI. CASE STUDY

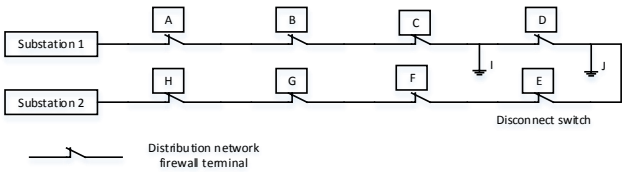

Figure 3. Distribution network line

All firewalls are equipped with a breaker. As is shown in Fig. 3, where A, H, E are firewall terminals, and A, H are at the substation export, but E is located at a section switch. When I and J have a transient fault or permanent fault, the following analyzes the actions of a network firewall protection terminal.

A. Point I have a transient fault

(1) During normal operation, disconnect switches are off. A-E are powered by substation 1. E-H are supplied by substation 2.

(2) After I fails, A-C monitor fault currents, and if they are greater than the setting values, C trips for protection, however, A and B maintain their status. After C recloses firstly, transient fault disappears, then C keeps closing state. Normal power supplies.

(3) D and E protection do not act, and just keep closing state.

B. Point I have a permanent fault

(1) During normal operation, disconnect switches are off. A-E are powered by substation 1. E-H are supplied by substation 2.

(2) After I fails, A-C monitor fault currents, and if they are greater than the setting values, C trips for protection, however, A and B maintain their status. After the C recloses firstly, the fault still maintains, so C starts running post-acceleration tripping without reclosing.

(3) During the process of C recloses and runs post-acceleration tripping, D and E detect residual voltage whose duration is less than the limit time of Y.

(4) D is a non-disconnect switch, and once residual voltage is detected, it closes.

(5) E is a disconnect switch, if one side loses power for a certain time, E closes the auto-control switch.

(6) If D detects voltage, D closes on the fault line. D runs post-acceleration tripping without reclosing.

(7) The fault is isolated, and the system power is restored.

C. Point J have a transient fault

(1) During normal operation, disconnect switches are off. A-E are powered by substation 1. E-H are supplied by substation 2.

(2) After J fails, A-D detects fault currents, and if they are greater than the setting values, D trips for protection, however, A and C maintain their status. After D recloses, transient fault disappears, then D keeps closing state. Normal power supplies.

(3) E protection does not act, and just keeps closing state.

D. Point J have a permanent fault

(1) During normal operation, disconnect switches are off. A-E are powered by substation 1. E-H are supplied by substation 2.

(2) After J fails, A-D detect fault currents, and if they are greater than the setting values, D trips for protection, however, A and C maintain their status. After the D recloses firstly, the fault still maintains, so D starts running post-acceleration tripping without reclosing.

(3) E is a disconnect switch, if one side loses power for a certain time, E closes auto-control switch on the fault line, and runs post-acceleration tripping, as well as lockout reclosing.

(4) The fault is isolated, and the system power is restored.

VII. CONCLUSIONS

Using a modular idea, distribution network firewall protection terminal is designed in this paper. For a specific processor chip, only hardware-level code needs to be changed, which greatly simplifies the software maintenance process, and enhances the reusability of code. The distribution network fault simulation shows the working process of the firewall terminal and the terminal has been successfully used in somewhere for distribution network protection. Until now, it shows stable operation and superior performance, demonstrating the effectiveness of the firewall terminal and meeting the design objectives.

REFERENCES

[1] Ghosh D, Ghose T, Mohanta D K. Communication feasibility analysis for smart grid with phasor measurement units[J]. Industrial Informatics, IEEE Transactions on, 2013, 9(3): 1486-1496.

[2] Zhabelova G, Vyatkin V. Multiagent smart grid automation architecture based on IEC 61850/61499 intelligent logical nodes[J]. Industrial Electronics, IEEE Transactions on, 2012, 59(5): 2351-2362.

[3] Kriger C, Behardien S, Retonda-Modiya J C. A detailed analysis of the GOOSE message structure in an IEC 61850 standard-based substation automation system[J]. 2013.

[4] Higgins N, Vyatkin V, Nair N K C, et al. Distributed power system automation with IEC 61850, IEC 61499, and intelligent control[J]. Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on, 2011, 41(1): 81-92.

[5] Mohagheghi S, Tournier J C, Stoupis J, et al. Applications of IEC 61850 in distribution automation[C]//Power Systems Conference and Exposition (PSCE), 2011 IEEE/PES. IEEE, 2011: 1-9.

[6] Blair S M, Coffele F, Booth C D, et al. An open platform for rapid-prototyping protection and control schemes with IEC 61850[J]. Power Delivery, IEEE Transactions on, 2013, 28(2): 1103-1110.

[7] Yonghui S. Implementation of LwIP TCP/IP stack with ARM-based MCU[J]. Foreign Electronic Measurement Technology, 2009, 10: 021.

[8] Jones, M. T. Embedded system TCP/IP application-layer protocol [M]. Electronic Industry Press. 2003, 4.

[9] Cooling J E. Software design for real-time systems[M]. Springer, 2013.

[10] Labrosse J J. uC/OS-III: The Real-Time Kernel and the Texas Instruments Stellaris MCUs[M]. Micrium Press, 2010.

[11] Fan Z, Kulkarni P, Gormus S, et al. Smart grid communications: overview of research challenges, solutions, and standardization activities[J]. Communications Surveys & Tutorials, IEEE, 2013, 15(1): 21-38.

[12] Güngör V C, Sahin D, Kocak T, et al. Smart grid technologies: communication technologies and standards[J]. Industrial informatics, IEEE transactions on, 2011, 7(4): 529-539.

[13] Qattawi A, Mayyas A, Omar M A. An investigation of graph traversal algorithms in folded sheet metal parts design[J]. The International Journal of Advanced Manufacturing Technology, 2013, 69(9-12): 2237-2246..