Duplicate Node Identification For A Network System Of Fire Alarm Control Units

CH.V. Narasimha Rao[1], S.Subba Rao[2]
[1]*M.Tech Student, E.C.E Department, V.R.Siddhartha Engineering College, A.P, India,*
[2]*Assistant Professor, E.C.E Department, V.R.Siddhartha Engineering College, A.P, India,*

Abstract

This paper explains the Duplicate Node Identification feature implemented for a network system of fire alarm control units connected using RS-485 lines. In first step identification is done at the network interface card by making necessary changes with respect to the peer-to-peer communication protocol. In the second step this information is conveyed to the main controller of the fire alarm control unit. The main controller after receiving this information first it updates the fire control unit's status by changing the LED to yellow colour, later it broadcasts this information to all the nodes present over the network about the existence of duplicate node by sending the broadcast command to network interface card which sends the received information to all the peer nodes. The above mentioned identification process is implemented by using inter-processor communication techniques and the test results are shown after loading the code along with the screen shots which are discussed.

Index Terms: *Duplicate Node Identification, inter-processor communications etc.*

1. Introduction

Duplicate addressing of the devices/nodes is one of the major problems faced both in the wired and wireless networks. It causes many problems to the network system in various ways depending on the devices that are being networked. This poses a serious problem in networks if it is being accessed by unauthorised people who join the network with same address as one of the node in the network. This is still more serious issue in wireless networks and adhoc networks as it is more prone to this problem and difficult to find who has joined the network on fly during network operations and access the confidential data.

When it comes to networking of the fire alarm control units which are life safety devices the duplicate node existence would cause many severe problems if unaddressed. Thus depending on the data that is being transferred and also the application it has severe implications on network system functionality and the people who make use of them.

Previously the responsibility to make sure that no duplicate node exists on the network system lies on the installer and sometimes due to human errors it may lead to assigning of same address to multiple nodes while allocating the node addresses. Thus the existence of duplicate nodes over the network was unidentified and hindering the efficient communication over the network among nodes. This problem is avoided by using the duplicate node identification feature.

The rest of the paper is organized as follows: Second section details the functionality of the Network Interface Card (NIC) in the networking of the fire alarm control units. The third section deals with the implementation part explained in the flow charts. The fourth section gives the test results of the implemented feature and in fifth section it is gives conclusion and future work.

2. Functionality of Network Interface Card in Fire Alarm Control Unit

2.1 Need for Networking

For large areas or campus style applications, fire alarm control units can be networked into a powerful system capable of supporting large number of smoke detector devices. The fire alarm control unit has the capability to provide true peer-to-peer networking of up to 64 control units. The network is capable of performing fire-alarm and/or suppression system operations on a network- wide basis as mentioned below.

– Event initiation
– Protected-premises local and/or remote event annunciation
– Occupant notification via audible and visible signaling appliances
– Process/equipment control to activate safety procedures
– Fire extinguishing system release
– Off-premises transmissions to central station or fire department

The network provides several convenient interconnect programming schemes wherein control panels can be configured individually or

within created groups of control panels. When utilizing the grouping configuration, the interconnection automatically provides shared alarm and trouble responses. The programmable shared responses are: acknowledge, silence, reset, event logging and logic statements. Operator events can be activated into the interconnection via the control panels or any annunciator. A location address and programmable description is used to identify the panel initiating the event.

2.2 Networking

Networking functionality is divided into layers based upon the OSI model. This is done in order to utilize appropriate pieces of the developed standards as a guide. There is however, no intention and no need to be OSI compliant.

Only four of the seven layers defined OSI layers fit this project's needs and only those four are addressed in the design. These layers, as shown in the **Error! Reference source not found.**are described below.

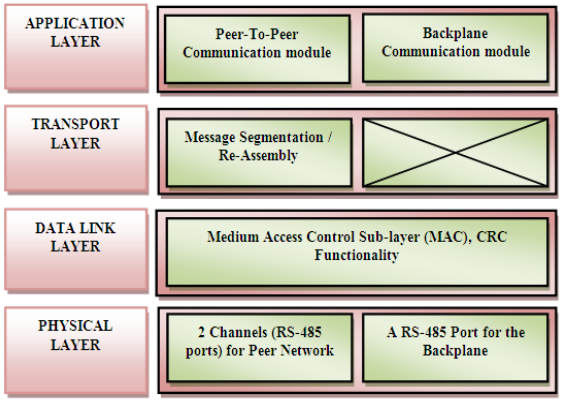

Fig: 1. Network Interface Card Stack Layers

2.2.1 Application Layer

The Application Layer is the top most layer of the network stack and it uses the lower layers in order to perform the services as specified by the peer-to-peer protocol and backplane protocol.

The Application Layer has the capability to understand the messages received from the transport layer and perform a service or execute a command. Similarly it creates a response in the format required by the transport layer. Application layer consists of two independent communication interfaces.

Backplane Communication Module implements Network-Backplane Protocol functionality and services to communicate with the Main Control Board (MCB).

Peer-to-Peer Communication Module implements the Peer-to-Peer Protocol functionality and services to communicate with the other peer nodes present on the network.

Application Layer provides the functionality to act as a router i.e. it receives messages from MCB, extracts the message data, creates a new message, inserts the message data into it and sends the new message to the intended node on the peer network and vice-versa.

2.2.2 Transport Layer

Transport Layer provides the link between application layer and data link layer. It performs message segmentation and reassembly. Application layer messages are broken into smaller segments (as necessary) to fit within the maximum frame length specified by data link layer at the transmission end. The segments will be reassembled back into the original message at the receiver end.

The transport layer is present only in the Peer-to-Peer Communication Module, where the maximum message length is 128 bytes. MCB (Main Controller Board) can send/receive maximum length packets in one command only.

2.2.3 Data Link Layer

Data Link Layer provides the access to the actual physical media. It creates the data frames for the outgoing messages as specified by the protocols and sends the data frames for transmission to the physical media. For the incoming messages, it parses and validates the messages.

In case of Peer-to-Peer Communication Module, data link layer also sends the claim tokens and acquires the tokens in order to perform the message transmission. If there is no data to be transmitted, data link layer passes the token to the next node in line. It also handles the token acknowledgements.

2.2.4 Physical Layer

- The Physical Layer provides data transmission among peer nodes and between NIC and MCB. The Physical Layer is divided into two independent communication channels, which are two Channel UARTs for Peer-to-Peer Communication Module.
- 1-Channel UART (RS-485 Port) for Backplane Communication Module

The UART module consists of the RS-485 hardware port and software driver required to control transmit and receive operations. The RS-485 UART Driver provides the link between the Physical Layer and Data Link Layer. Peer Communication layer is RS-485 lines.

2.2.5 NIC Functionality

The NIC works on the token pass protocol over a linear bus structure as shown in the figure 2. In NIC the token is passed from the higher node to lower node successively

As shown in the Figure 2, the fire alarm control unit peer network is based on a linear bus, where

each fire alarm control unit system is interconnected with one or two neighbor(s).

The peer to peer network communication is a linear bus where a transmission from any node propagates the length of the medium in both directions and can be received by all other nodes.

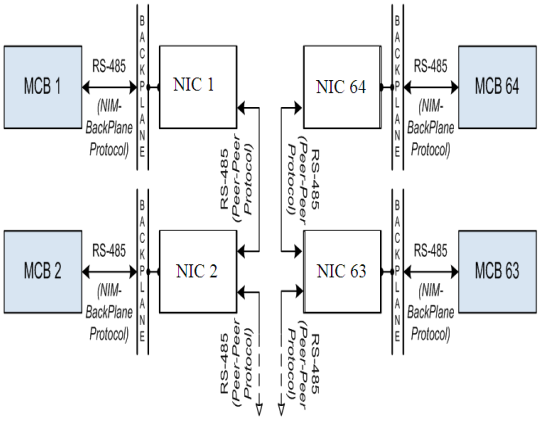

Fig: 2. NIC Architecture

3. Implementation

The duplicate node identification feature is implemented both on the Network Interface Card (NIC) and Main Controller in the below sections. The NIC module is developed by using the PIC controller PIC24FJ128GA108 whereas the MCB of the fire alarm control unit is developed by using the ARM 9 series controller AT91SAM9260. Their respective integrated development environment/ Workbenches were used for coding and compiling to generate the respective firmware to be loaded in the respective controllers

3.1 Duplicate Node Identification on NIC

When duplicate nodes exist on the network it was observed that one of the duplicate nodes was sending the claim token messages continuously to all the nodes (including other duplicate nodes) present on the network. Upon receiving this claim token message a comparison is made with source node address from where the claim tokens are being transmitted with node address on the node which this message is received. If the source address (duplicate node's address) matches with any of the network nodes address in the above comparison then it indicates that particular network node is a duplicate node. Then that particular node status is changed to the "Trouble" state for the duplicate node fault by calling the appropriate function with valid parameters. This is the process that is happening at NIC level for a given node initially in indentifying the duplicate node.

In the above function call, variables indicating the NIC status and MCB status (i.e., status bits to be sent to MCB) are set with the corresponding hexadecimal values that indicate the duplicate node fault which are defined earlier. These variables that are set for NIC and MCB status bits are used later while clearing of the fault.

To implement the above defined functionality, firmware changes were first made to define the corresponding duplicate node event as one of the many events that NIC supervises or monitors for to update its status on occurrence of any one of these events. This defined event is passed as parameter to update the NIC status to the corresponding function and to set that fault in ON state. In figure 3 the above process is shown in flow chart.

All the above mentioned firmware changes were done with respect to the peer-to-peer communications module of the NIC using C language on the PIC microcontroller.

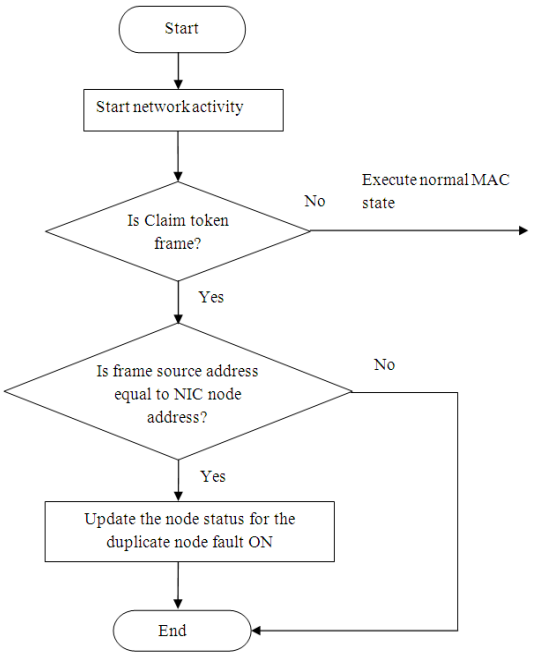

*Fig: 3.*Process to identify duplicate node on NIC

3.2 Duplicate Node Identification on MCB

The change in the NIC status information is sent to the MCB, as a response to the periodic polling messages sent by the MCB to NIC in order to know the status of the network nodes. To achieve this, firmware changes were made on the NIC's Backplane Communication module by defining an event in the list of events that were monitored by NIC to be send to the MCB. An available code value (a hexadecimal value) is assigned to the defined event variable so that it could be identified by the MCB code to report that particular event on the screen of the panel's user interface.

To report the duplicate node fault trouble message the MCB has to recognize the message sent by the NIC. For this the same hexadecimal value that was used to define the event variable in NIC is used to define the event on the MCB side as well to identify that a particular event has occurred.

Then the duplicate node fault event's corresponding display string is defined in MCB event list string array for display on the screen. This is added in network events range as one of the supervising events in appropriate index location. Thus this event value when passed to the string array while the code is getting executed it fetches the corresponding text message from the string array and displays it on the screen. The MCB changes the trouble status LED to ON state on reception of the duplicate node fault event which is defined as a trouble event.

In order to fetch the display message string the event code of the duplicate node fault is passed at runtime if this fault has occurred. This firmware changes were done on the MCB side for the ARM 9 controller. The above defined process is shown in the below figure 4 flow chart.

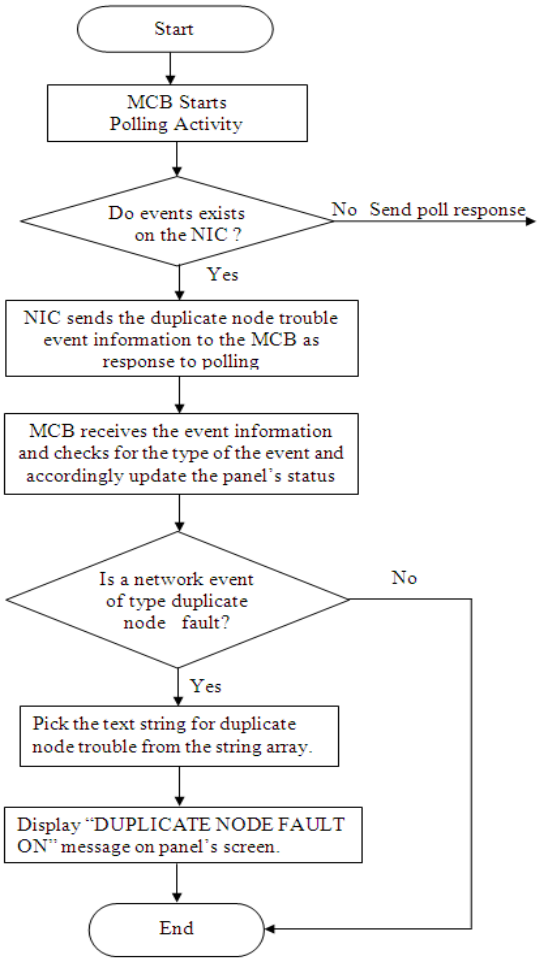

Fig: 4. Process to identify duplicate node on MCB

3.3 Implementation to Transmit Fault to Non-duplicate Node

This section deals with the transmission of the duplicate node fault event information from a duplicate node to all the non-duplicate nodes present over the network.

The MCB issues a command to NIC to transmit the event information over the network. Then NIC extracts the message from MCB and frames it appropriately as per the peer-to-peer communications protocol and sends over the network to all the remote nodes present on it.

In firmware implementation this is done by calling a function to generate the command from MCB by passing the parameters like event type, status of event whether it is ON/OFF and module type to specify to which module this command has to be reached. The time and date are picked from the panel's real time clock. This function is called on checking whether it can be transmitted or not by passing the event number to a function which checks for the valid events and then returns true on successful check otherwise returns false.

NIC on reception of this command prepares the network message by extracting the data from MCB command and transmits over the network.

The implementation part for the above defined process is shown in the figure 5.

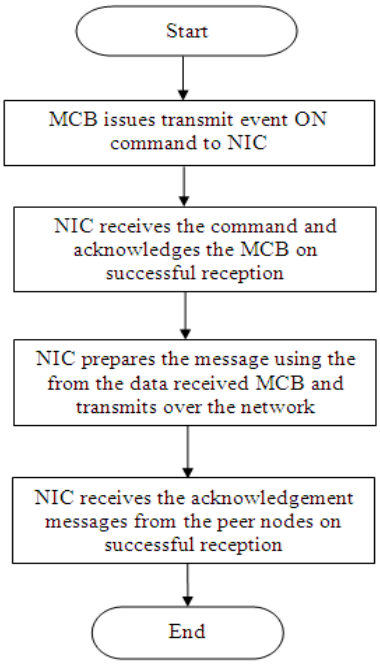

Fig: 5. Process to transmit duplicate node fault to non-duplicate nodes

3.4 Implementation for the Clearing of Duplicate Node Fault

This section deals with the NIC firmware changes to give the intelligence to clear the duplicate node fault on taking the appropriate actions like change of the node address.

3.4.1 Approach to Clear the Duplicate Node Fault

On the absence of duplicate nodes over the network there are no claim token messages observed with source address as node's self address on which the claim token messages are received. Thus if claim tokens are not received which

satisfies above condition where source and destination addresses are same for a certain period of time then it implies that there are no duplicate nodes over the network. Hence by monitoring for a certain period of time the NIC status is updated to clear the duplicate node fault and this is further transmitted to the MCB to clear on the local node first. This clearing command is then transmitted from the MCB to NIC which then transfer the duplicate node fault OFF event to all peer nodes present on the network and thus clear the trouble from all nodes present on the network.

3.4.2 Usage of Timer

To implement the above defined functionality, a timer is used to monitor the reception of claim token messages which are having their source address matching with node address of the node on which this claim token is received continuously. This timer is started every time the above condition is satisfied. The time of the timer is dependent on the number of nodes present on the network. By considering the full network the timer value is set to 10 seconds.

If the claim tokens (i.e. no duplicate node exists on the network) are not received then the timer gets expired as the control does not go to that part of the code where the source address of the node which sends the claim token matches with node address of the node receiving this message. By checking the status of the timer we update NIC status accordingly. If the timer expires then the NIC status is cleared for the duplicate node fault. Thus in this way the duplicate node fault clearance is implemented using the timer concept.

The PIC controller used has four 16 bit timers. Two timers are used in conjunction to achieve the 32 bit timer functionality. A separate timer ID is defined for the duplicate node fault clearing purpose. The time duration is also defined for timer. The timer ID and time value are passed as parameters to initiate/start a timer. The timer's time value alone is passed as parameter while checking for the timer expiration/elapse condition. The implementation part for the above defined process is shown in the below figures 6 and 7.

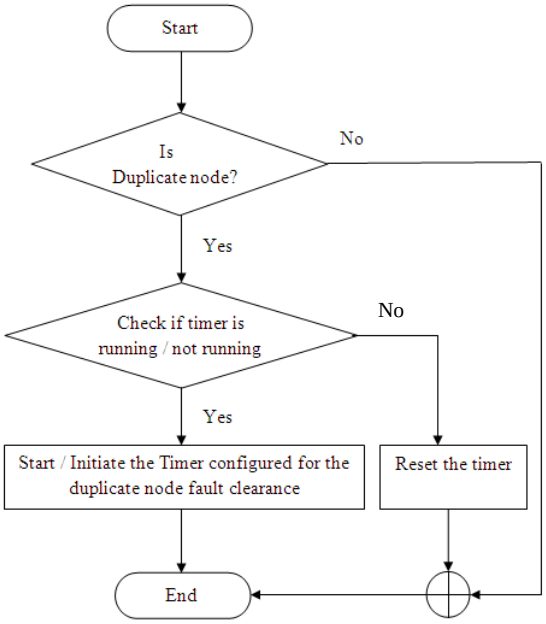

Fig: 6. Process to initiate a timer on the duplicate node fault detection

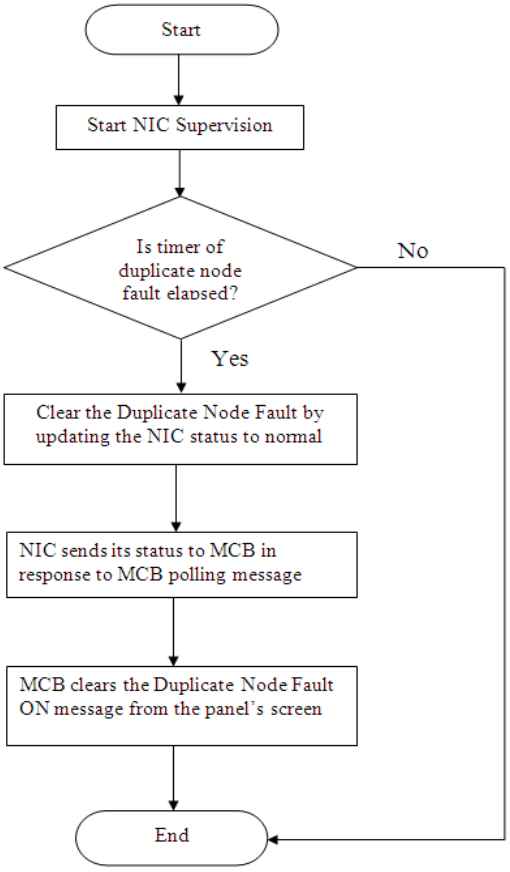

Fig: 7. Process to clear duplicate node fault on timer expiration

3.4.3 Clearing Fault When the Network has Duplicate Nodes Alone

The duplicate node fault reported over the network system having all the nodes with same address has to be treated separately due to the following issue faced while testing and the corresponding code has been written to fix the issue as explained below.

Issue

When the nodes having the same addresses alone are added in the network, they are reporting the duplicate node fault and this fault is getting cleared immediate after 10 seconds. This is because whenever a node is added in the network it first sends a claim token and as the receiving nodes are all with same address they report the duplicate node fault and later there is no network activity among self addressed nodes. Thus duplicate node fault is getting cleared even though the network had all nodes with same address.

Solution

In the implementation of the clearing the duplicate node fault a separate logic is used to deal with this special scenario of network with all nodes having the same address. The node map in this case consists of a single node address value even though the actual number of nodes is greater than one. Thus before clearing the duplicate node fault the node count checked whether the number of nodes is greater than one. If node map is having just one node address then the fault is not cleared otherwise it is cleared. The implementation part for the above defined process is shown in the figure 8.

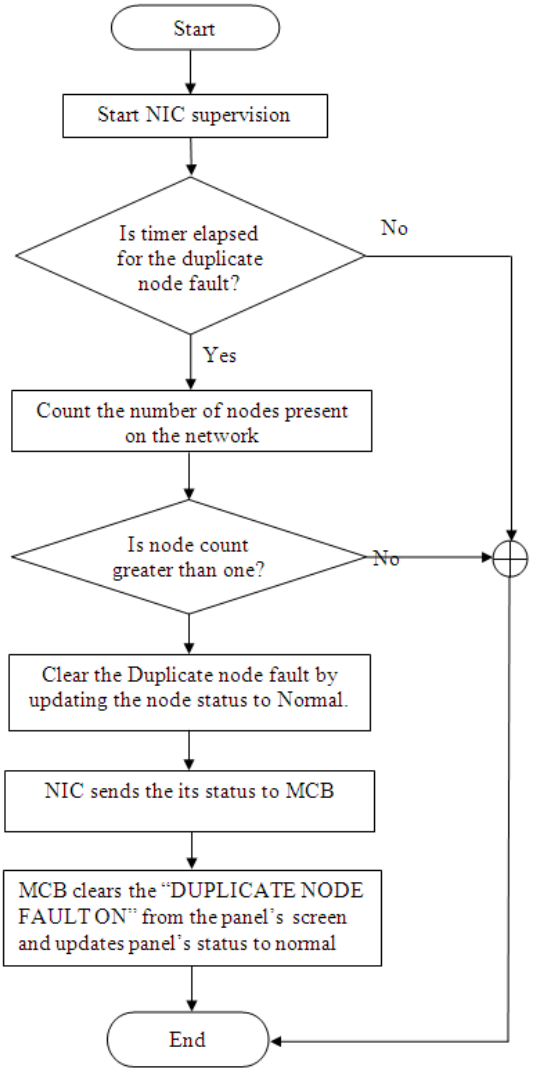

Fig: 8. Process to clear duplicate node fault for network having all nodes as duplicates

4. Test Results

Test Purpose

The purpose of the test is to test for the reporting of duplicate node fault on a network consisting of nodes with same addresses (any value from 1 to 64) and also to test for clearing of the fault on appropriate actions.

Test Setup

Three panels with NIC connected to their respective back planes. These panels are connected via RS-485 lines to form as network system. This test setup is used for testing.

Following are the displays of the three panels assigned with addresses 1, 2 and 3 respectively which are connected using the RS-485 interface lines with each other but not included in the network. Thus the panel's display shows normal with off net status as shown in figures 9.a to 9.c.

Fig: 9.a. Node 1 panel's display with off net status when not in network

Fig: 9.b Node 2 panel's display with off net status when not in network

Fig: 9.c Node 3 panel's display with off net status when not in network.

4.1 Panel Displays after adding into Network with no duplicate nodes

When the panels are included in the network their network status is displayed on the LCD display which gives details like node number/address of the panel and whether channel 1 or channel 2 connections are active for providing the network communications with other network panels.

Following figures 10.a to 10.c gives the displays of three panels assigned with addresses 1, 2 and 3 which are connected via RS-485 lines and added into the network to form a network system of three fire panels.

Fig: 10.a. Node 1 panel's display with on net status when in network

Fig: 10.b Node 2 panel's display with on net status when in network

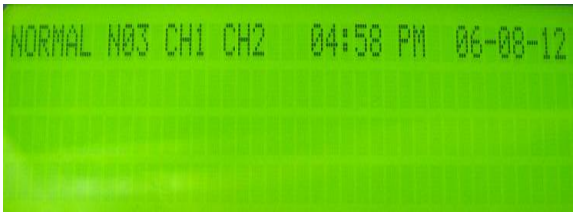

Fig: 10.c Node 3 panel's display with on net status when in network

4.2 Results for Reporting of the Duplicate Node Fault

Consider three panels assigned with addresses 3, 3 (duplicate nodes) and 50 connected via RS-485 interface lines but not included in the network. The displays of those panels are shown in the figures 11.a to 11.c.

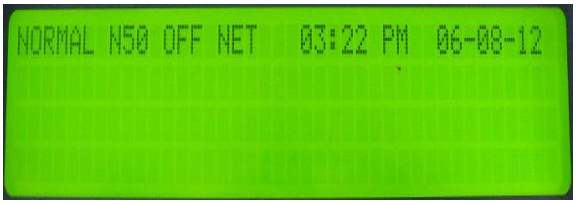

Fig: 11.a. Node 50 panel's display with off net status when not in network

Fig: 11.b. Node 3 panel's display with off net status when not in network

Fig: 11.c. Node 3 panel's display with off net status when not in network

4.2.1 Panel Displays after Adding into Network

Include the panels into the network by adding them through one of the panel's user interface as mentioned in the test cases. As soon as the nodes are added into the network the duplicate node fault is reported on both non-duplicate node and duplicate nodes respectively and the corresponding displays on the panel's LCD screen are shown in the below figures 12 and 13.

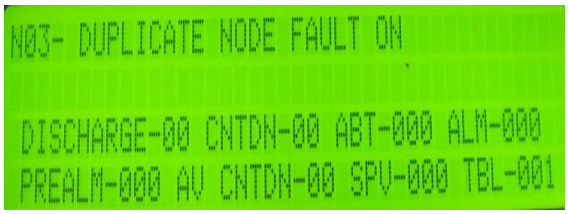

Fig: 12. Display on node 50 reporting duplicate node fault received from node 03

Fig: 13. Display on node 03 which is duplicate node

5. Conclusion and Future Work

The duplicate node identification feature will enable the network system of Fire Alarm Control units to identify the existence of a panel with duplicate address and the information about duplicate node is reported over the network to all the nodes. This helps to avoid the installation flaws and also the problems associated with duplicate node like token not received faults, un-synchronized event reporting, unable or delay in remote node accessing of the duplicate node and unable to use the configuration utility for configuring the duplicate nodes. Thus it avoids all those issues and by conveying the information to user/installer through panel's display and help him to take appropriate actions that were defined to clear the duplicate node fault and restore the normal network operations.

The present duplicate node identification feature will identify the presence of the duplicate nodes on the network and the appropriate action is taken by the installer to overcome the issues. This feature can be further extended such that network system itself takes care of this issue by changing the address of the duplicate node. This can be done by choosing address from the available addresses and if no addresses are available continue to display the duplicate node trouble on.

References

[1] "Fire Alarm Control panel", http://en.wikipedia.org/wiki/Fire_alarm_control_panel.
[2] "OSI Reference Model" http://en.wikipedia.org/wiki/OSI_model.
[3] "RS-485 Interface", http://en.wikipedia.org/wiki/RS-485.
[4] "RS-485 Circuit Implementation Guide" an Application Note by Hein Marais, Analog Devices.
[5] "UART Types ", http://www.pccompci.com/uarts.html
[6] "UART Functionality", http://en.wikipedia.org/wiki/Universal_asynchronous_receiver/transmitter.