Honeywell

Network Gateway Implementation and Operation

NG09-510

Total Plant

Honeywell

Implementation
Network Gateway

Network Gateway Implementation and Operation

NG09-510
Release 500
12/96

Total Plant

Copyright, Trademarks, and Notices

Revision 02 - December 20, 1996

About This Publication

This publication supports **TotalPlant** Solution (TPS) System network Release 500 through 520. TPS is the evolution of TDC 3000^{X}.

This publication is intended for the following types of users:

- Engineers—for planning and configuring Plant Information Networks
- Operators—for network startup and restart
- Service technicians—for network analysis and troubleshooting

The sections in this publication are organized as follows:

Section 1—Introduces the Network Gateway, its characteristics and its functions.

Section 2—Provides the framework for the planning of a Plant Information Network that is used to connect two or more TPS Local Control Networks.

Section 3—Discusses each of the steps required to configure Network Gateways on a local LCN to prepare for communication with other LCNs over the Plant Information Network.

Section 4—Discusses the displays that are available for network operation and problem analysis.

Appendix A—Explains how to change modem definition parameters when required.

Appendix B—Is a glossary of terms and acronyms specific to the Network Gateway.

Change bars are used to indicate paragraphs, tables, or illustrations containing changes that have been made to this manual. Pages revised only to correct minor typographical errors contain no change bars.

Table of Contents

Table of Contents

INTRODUCTION
Section 1

This section introduces you to characteristics of the Network Gateway and how it is used in connecting a number of LCNs to a Plant Information Network. It also includes references to other publications needed or useful for preparation of a Plant Information Network.

1.1 NETWORK GATEWAY DESCRIPTION

The Network Gateway (NG) is a standard LCN node that connects the LCN to a Plant Information Network or PIN. This connection enables the exchange of data between the local LCN and remote systems on the same PIN. Currently, the remote systems must also be LCNs. Data exchange with other types of systems that may exist on the PIN is a future possibility, but is not presently supported.

The NG acts as a transparent conduit for data exchange requests between the local LCN and remote systems (currently limited to other LCNs) connected to the same PIN. The NG contains no database except the NCF data required for communication routing; therefore, the NG does not "checkpoint," thus eliminating the need for node level redundancy of the NG. Network Gateways provide communication robustness through the ability to route messages through an alternate NG. This is in addition to the NG's ability to route messages through an optional alternate PIN cable.

Each system on the PIN can establish access restrictions limiting the types and directions of data transfers between itself and requesting remote systems.

The LCN database is not duplicated across the PIN. There remains only one database. Values from it can be copied to a remote system, but are not synchronized with the actual database.

Because it is connected both to the PIN and to the LCN, each NG has two unique addresses controlled by physical pinning, its PIN address and its LCN address.

Each NG requires a modem to connect it to the PIN. If the NG is to be connected to a redundant (two cable) PIN, separate modems are used.

Functions that can be carried on between LCNs via NGs are:

- Parameter access—reading or writing parameters of a point, either singly or in lists.
- File transfer—reading or writing entire files (and auxiliary information).
- Advanced control—Application Modules and Computing Modules can execute advanced control schemes on remote LCNs.

NOTE

With R400 through R430, certain unit configurations of LCNs would allow a local LCN to access history data directly on a remote LCN HM. Because this was not supported and did not always work satisfactorily, the LCN's data access mechanism has been changed to block such requests. Effective with releases later than R430, access of remote network history will no longer be allowed.

1.1.1 NG Performance and Throughput

1.1.1.1 Total Throughput

The total simultaneous throughput of an NG, assuming the serving nodes can supply the data, consists of:

- 1200 parameters per second by means of parameter access requests from up to 6 networks. 200 parameters are allowed per parameter access request.
- A file transfer rate of 1 block per second (maximum of 12,000 words)
- All normal node administration messages for the LCN
- Normal PIN and LCN status accessing.

Note that every transaction across the PIN requires two NGs, one at the sending system and one at the receiving system, and the throughput described above applies to each NG individually. Therefore, two NGs cannot operate at maximum throughput if all their requests are being made to a third NG, since the third NG would have to operate at twice the maximum rate to service the requests.

1.1.1.2 Response Time

Under the maximum load conditions, stated above, the time for a request initiation to reply completion is increased no more than 5 seconds over the time required if it were a local request. For example, a group display referencing 8 points from another LCN will take up to 5 seconds longer than a group display that references 8 local points.

1.1.1.3 Overload Characteristics

On overload conditions, the NG rejects new requests in each functional queue as it becomes full, except for parameter access requests where it will replace already queued requests with new requests of higher priority. When a request is rejected or removed from the queue, the request initiator is notified through the request return status.

Data Access requests—The return status will be something other than $D_OK.

File Transfer requests—The return status will be something other than $FMS_Successful.

The application that initiated the rejected/removed request must provide recovery actions.

1.1.1.4 Priority

The relative priority of functions processed by the NG is:

- Parameter access
- File transfer

The priority within parameter access requests is:

- Operator changes
- AM prefetch/poststore
- CM fetch/stores
- Display update following change
- Display initiations
- Display periodic updates

1.1.2 Other NG Characteristics

- Reasonably current data (i.e., seconds old) is provided over the PIN.
- Failure of the PIN will not prevent the LCNs from operating independently.
- Allows AM-type control to be performed between LCNs.
- The LCN does not care about the internal structure of nodes with which it is communicating.
- Communications priority and bad values propagation are not affected by the fact that data is being moved between LCNs.
- The order of replies may not be the same as the order of requests.

1.2 PLANT INFORMATION NETWORK DESCRIPTION

1.2.1 PIN Characteristics

A Plant Information Network (PIN) consists of a token passing network compatible with IEEE specification 802.4. It has the following characteristics:

- 10 Mb/s broadband, 5 Mb/s carrierband, or 10 Mb/s fiber optic network (Honeywell no longer sells new broadband configurations, but they will support them with a previously installed PIN).
- The PIN can be either single (A or B cable) or dual (A and B cables).
- The two cables are independent with a separate token for each cable.
- Each NG can be connected to either or to both cables.
- When connected to both cables, each NG transmits on a "preferred" cable and receives on both.
- High performance proprietary token passing protocol
- PIN network is expected to be provided by another vendor (Honeywell may, in some cases, handle the subcontracting for the installation and maintenance of this network).
- The vendor is expected to supply and maintain the required repeater units.
- The maximum number of node connections to the PIN is 64.
- Both local (hard pinned) and global (software) addressing are supported by the PIN (global addressing is not implemented as of LCN release R500).

When two cables are present, the NG transmits on the "preferred" cable and waits for an acknowledgement. If there is no acknowledgement, the NG retries once on the same cable before switching to the other cable. The condition of both cables is continuously reassessed as a background function. A record of unacknowledged messages by cable and destination is kept for use in selecting the preferred cable for each NG message destination.

1.2.2 PIN Layouts

The following three illustrations show how the PIN can be used to tie together geographically separated LCNs for such inter-network operations such as parameter access and file transfers.

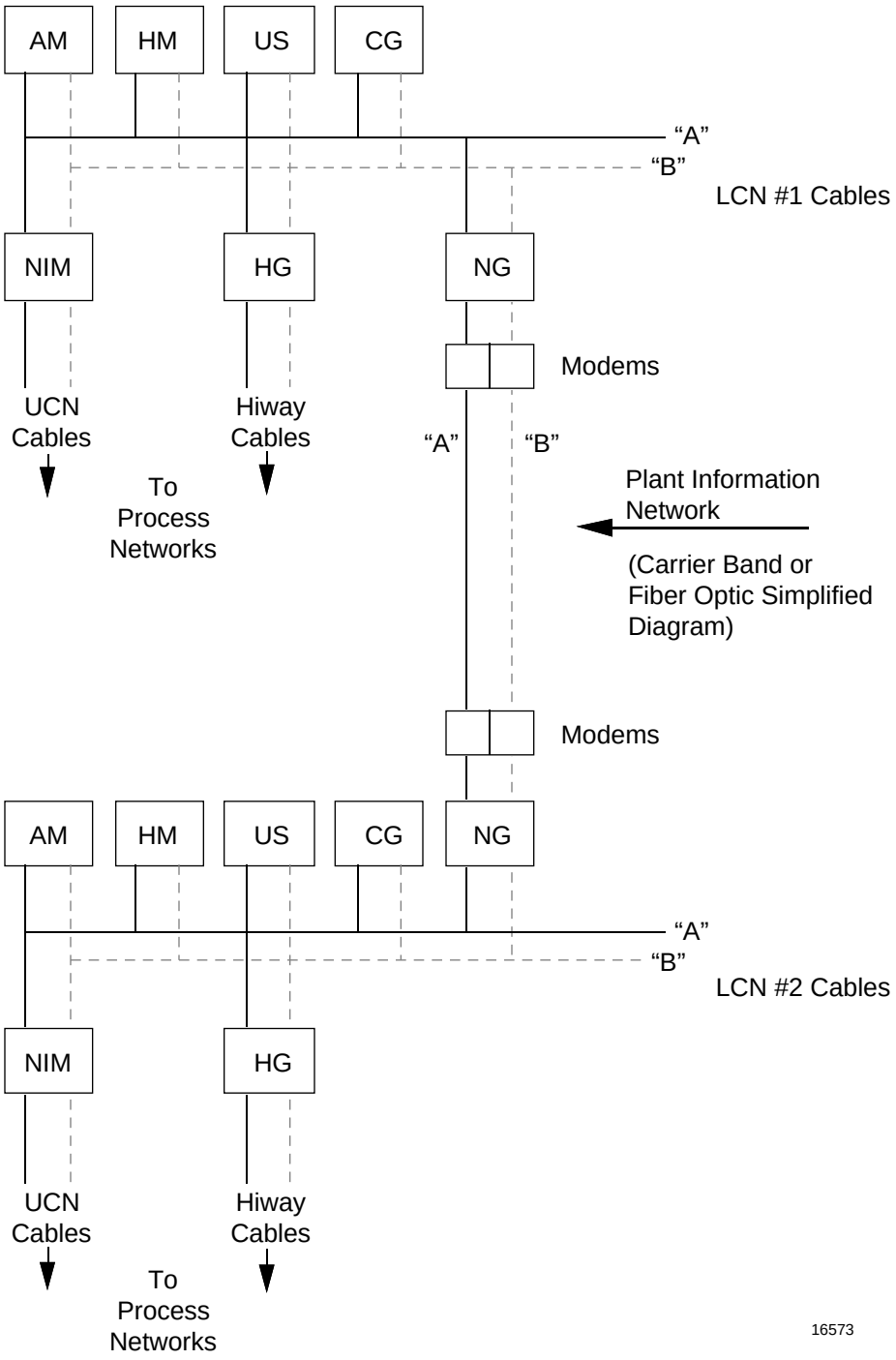

Figure 1-1 — Block Diagram of a Simple LCN to LCN Interconnection

Figure 1-1 shows a simple interconnection between two LCN systems that uses both an "A" cable and a "B" cable for the PIN. The "B" cable is an option that improves system availability requirements in the event of "A" cable failure. Because this example uses a single NG at each LCN, the failure of either NG would cause the LCNs to loose communication.

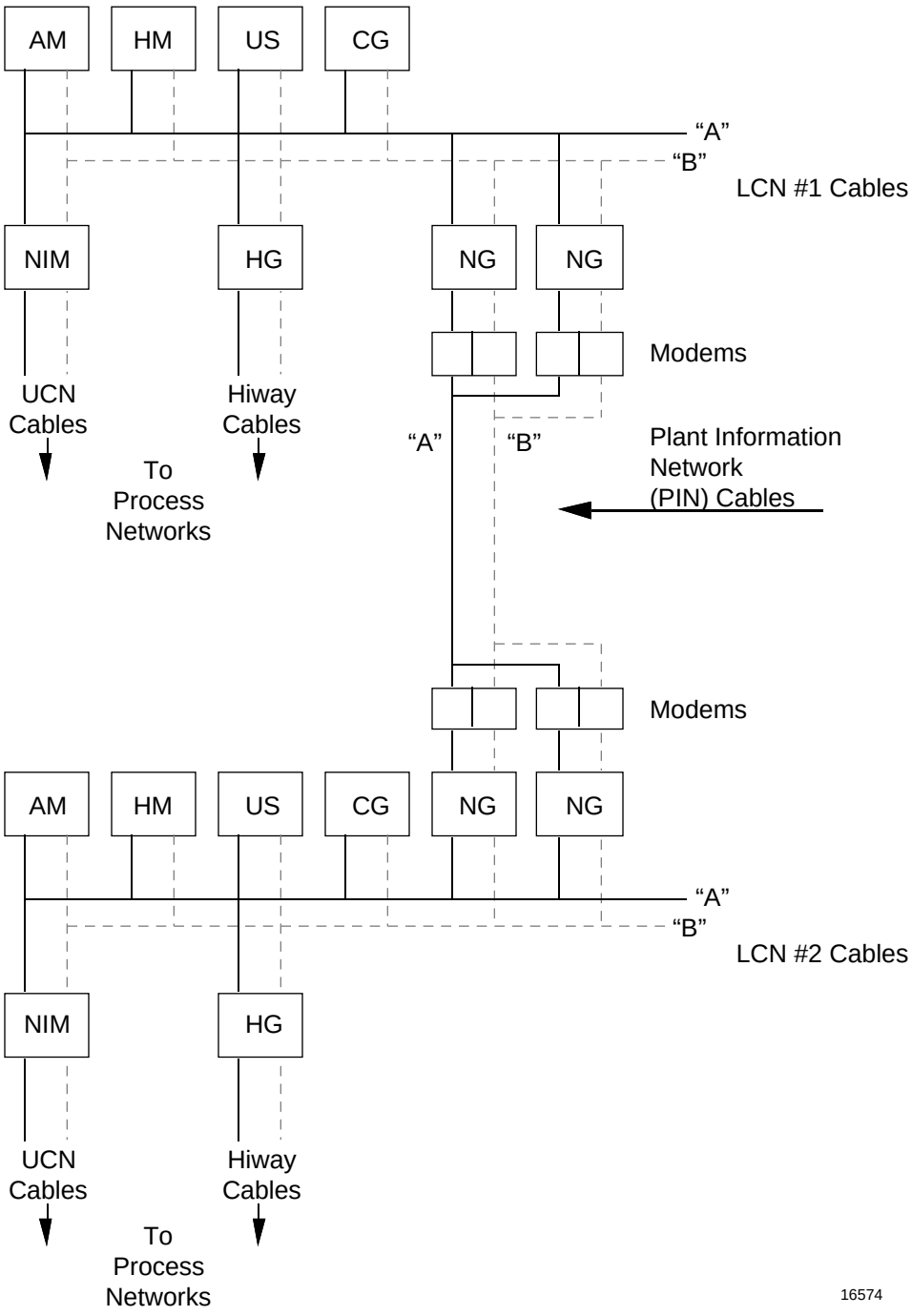

Figure 1-2 — Block Diagram of an Improved LCN to LCN Interconnection

Figure 1-2 shows an improved interconnection that provides alternate routing capability by placing two NGs on each LCN. Note that the NGs are not redundant. Each NG is a separate node (on both the LCN and PIN networks) and software configuration determines what communication traffic runs on each and selects alternate paths for communication. This allows for continued system operation even if one NG should fail.

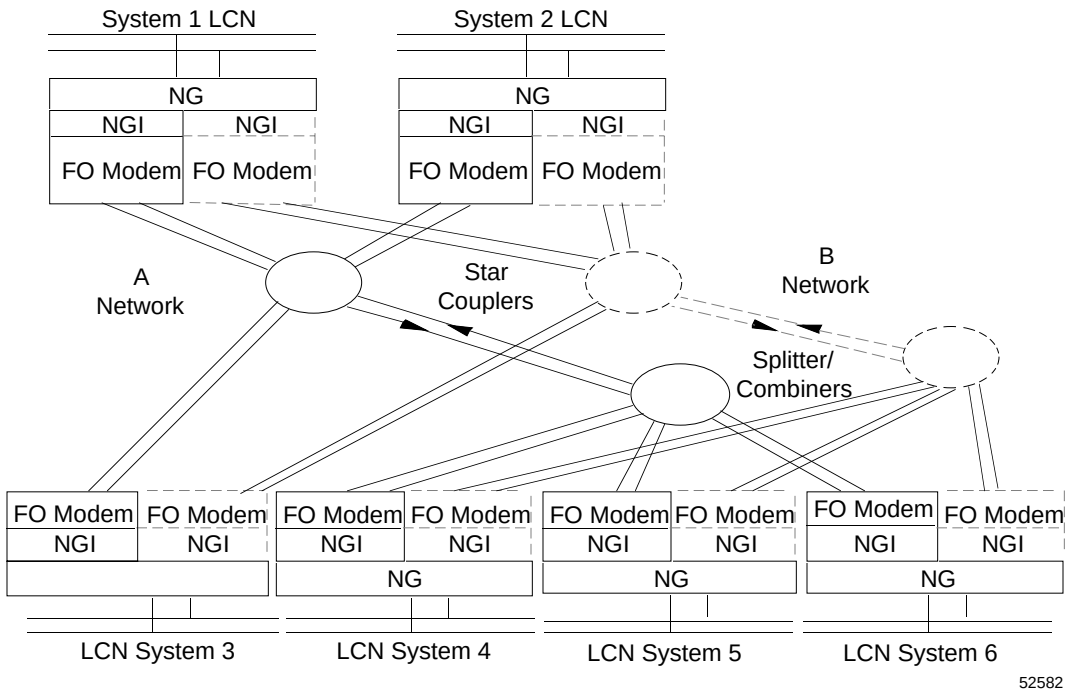

Figure 1-3 — Block Diagram of a Typical PIN Implementation

Figure 1-3 shows a broader application of the PIN. It illustrates how more than two LCNs could be interconnected. Note that this example still shows only two NGs on each LCN. The LCN software supports up to 10 NGs per LCN, thus permitting a wide variety of possible communications paths.

1.3 HOW THE NG AND PIN WORK TOGETHER

1.3.1 Rules and Limitations

- Each LCN can communicate with every other LCN on the PIN.
- An NG on an LCN can be connected to only one PIN.
- An LCN can be connected to a PIN by up to 10 Network Gateways.
- There can be up to 64 NGs per PIN.
- Use of multiple NGs on LCNs reduces the number of LCNs that can be connected to a PIN since each NG takes one of the 64 available network addresses. For example, a 16-LCN network with 4 NGs on each LCN would require all 64 of the available PIN addresses.

CAUTION

Do not attempt to access removable media on a remote system. This functionality is not supported, and will cause NG's to crash in releases prior to R430.

1.3.2 Local and Global PIN Addressing

Each node (NG) connected to the PIN must be configured with a unique "PIN address." This NG Local PIN Address is physically pinned on the NG's PIN interface board. If the NG node is connected to a two-cable PIN, both of the PIN interface boards in the node must be pinned to the same PIN address.

An additional PIN address feature provides for added security on multi user PIN's. This additional PIN addressing feature is called Global Addressing and is optional. With "Global Addressing" enabled, all messages will carry a "Global Address" in addition to the normal PIN address. NG personality software will insist that all incoming messages match a unique (configured in NCF) "Global Address value" and the physically pinned "PIN address" before it is accepted (See step 2 at heading 3.2 for software configuration details).

Note that global addresses are not fully implemented as of Release 500 and should be left blank on all data entry displays where PIN address information is entered.

The global form of address uses a 48-bit number which is required to be unique throughout the world. These numbers are assigned in blocks of one million by IEEE. Honeywell has obtained a block of these numbers and assigns each customer a subset of numbers from this block. The global address number is divided into two parts to reduce the number of digits entered during configuration and thus reduce the chance for errors. The upper part is known as the "PIN Global Vendor Number" and is common to all NGs on a given network. The lower part is known as the "PIN Global Vendor Number Offset" and is specific to a single NG on the network.

1.3.3 LCN Data Security

Each local LCN defines its own data access read/write security through restrictions placed on remote access to local data. During configuration of each local LCN you will establish specific limitations on each remote system; whether it can both read and write, read only, or have no access at all to the LCN being configured. You then can establish exceptions to these access limitations (either more or less restrictive) that will apply to individual files and nodes on the local LCN.

Security is only checked on requests coming in to the LCN from the PIN, not on requests going to the PIN from the LCN.

1.3.4 Network Load Leveling

Input to an LCN can be load leveled by having different LCNs use different NGs as receivers at a target LCN.

Output from an LCN can be load leveled by having different NGs associated with various remote systems.

When dual cables are used, a primary cable for output from the local LCN to each individual remote system is specified. By dividing the load between Cable A and Cable B, throughput is increased and response time diminished.

1.3.5 Tag Name Length Restrictions

The following limitations affect transfers between LCNs that use different tag name lengths:

- A point data request from an LCN using the short name form (eight characters or less) sent to an LCN using the long name form (up to 16 characters) will be honored. The target LCN will use the short name (padded with trailing spaces to long form length) to attempt a match.

- A point data request from an LCN using the long name form sent to an LCN using the short name form will result in a "Point Not Found" response message if the tag name has more than eight nonblank characters (e.g., ABCDEFGH is an acceptable tag name for this purpose, but ABCDEFGHI is not).

1.3.6 Software Configuration Choices/Options

In order to establish communication between two LCNs on a common PIN, the NG (or NGs) on each LCN has/have to be separately configured as LCN nodes.

Each LCN is individually configured as local to itself and as a remote system to all other LCNs on the PIN. (This could mean going through the software configuration steps up to 64 times for one network—once for each LCN on the network.) To prepare a hypothetical 4-LCN network (consisting of systems 1, 2, 3, and 4), you would individually configure the four LCNs:

"Local" system	"Remote" systems
1	2, 3, 4
2	1, 3, 4
3	1, 2, 4
4	1, 2, 3

Thus, when LCN 1 is being configured, LCNs 2, 3, and 4 are considered to be "remote" systems. And when the other LCNs are being configured, LCN 1 is considered to be a remote system to each of them.

During software configuration you specify the characteristics of the local LCN (system), then describe how it relates to each other system on the PIN. At the local LCN you define communication routing with each other system, and define data access restrictions to be placed on each of the other systems.

For each remote system (LCN) that will be communicated with, you must be prepared to describe it by a Local System Number, Local System Title, and Local System Description.

You then must specify which local NG and which PIN cable (A or B) will be used to transmit to each individual remote system. When the local LCN has more than one NG, you can define a second NG as an alternate transmitter to be used if the responsible (primary) NG becomes unavailable.

You also must identify (by PIN "local" address) which NG on the remote system will be the primary receiver. If the remote system has more than one NG, you can also specify an alternate receiver. Use of the optional PIN "global" address is not yet implemented.

Section 2 of this manual will take you through the detailed steps required for the planning of a PIN network that connects two or more LCNs via Network Gateways.

1.4 REFERENCES

The initiation of communications that use the NG is by other nodes on the LCN such as the AM or US. How these nodes initiate these data transfers and how they use the information gathered is documented in the user manuals associated with individual LCN node types such as the AM, CG, and US and with CM50S. Details of how these functions are used can be found within these publications:

- Application Module Control Functions, AM09-502
- Application Module Implementation Guidelines, AM12-510
- Control Language/Application Module Reference Manual, AM27-510
- CM50S User Manual, CM11-530
- Computer Gateway User Manual, CG11-510
- Process Operations Manual, SW11-501

Other publications that contain information that you will need in implementing a Plant Information Network are:

- Network Data Entry, SW11-505
- Network Forms, SW88-505
- Network Form Instructions, SW12-505
- Network Gateway Site Planning and Installation, NG02-500

PLANNING THE NETWORK
Section 2

This section provides you with the information necessary to plan the layout of a PIN that will connect two or more LCNs.

2.1 DEFINE NETWORK CHARACTERISTICS

Start by preparing a diagram similar to Figure 1-3 that shows the following network characteristics:

- The number of LCNs to be connected by this Plant Information Network. (2-64)
- The number of NGs on each LCN. (1-10)
- Single or dual (A/B) cables connecting each NG to the PIN.

When there is more than one NG per LCN and/or more than one cable connecting nodes to the PIN, you will need to plan for the various combinations of communication routing that the configuration will allow. The primary variable is the number of NGs connected to each LCN.

2.1.1 Local LCN with Multiple NGs

When there are multiple NGs connected to an LCN, you will have to define at each "local" LCN which local NG will be the responsible and which will be the alternate NG for communications with each "remote" system. For example, let's go back to the hypothetical 4-LCN network defined in Section 1.

"Local" LCN	"Remote" LCNs
1	2, 3, 4
2	1, 3, 4
3	1, 2, 4
4	1, 2, 3

Let's further assume that each LCN has four NGs on the network:

"Local" LCN	Connected NGs
1	17, 18, 19, 20
2	21, 22, 23, 24
3	25, 26, 27, 28
4	29, 30, 31, 32

Then, one possible way of configuring the network would be:

"Local" LCN	Primary NG	Alternate NG	"Remote" LCN
1	17	18	2
1	18	19	3
1	19	20	4
2	21	22	1
2	22	23	3
2	23	24	4
3	25	26	1
3	26	27	2
3	27	28	4
4	29	30	1
4	30	31	2
4	31	32	3

Thus far, we have only identified each remote node by its Local System Number. The next step is to add NG addresses for each remote system.

2.1.2 Remote System with Multiple NGs

When a remote system has multiple NGs, you can specify both the responsible and an optional alternate server for communication with each "local" system. Note: The responsible/alternate servers are specified in terms of their PIN local address. The following tables show the PIN local address for the responsible and alternate servers, with the LCN node address in parentheses. Let's extend the previous example to add primary and alternate server NGs to our hypothetical network configuration:

"Local" LCN	Primary NG	Alternate NG	"Remote" LCN	Responsible Server	Alternate Server
1	17	18	2	5(NG 21)	6(NG 26)
1	18	19	3	9(NG 25)	10(NG 26)
1	19	20	4	13(NG 29)	14(NG 30)
2	21	22	1	1(NG 17)	2(NG 18)
2	22	23	3	10(NG 26)	11(MG 27)
2	23	24	4	14(NG 30)	15(MG 31)
3	25	26	1	2(NG 18)	3(NG 19)
3	26	27	2	6(NG 22)	7(NG 23)
3	27	28	4	15(NG 31)	16(NG 32)
4	29	30	1	3(NG 19)	4(NG 20)
4	30	31	2	7(NG 23)	8(NG 24)
4	31	32	3	11(NG 27)	12(NG 28)

2.1.3 Cable Selection at the Local LCN

For each "local" NG responsible and alternate pair, you will have to define which cable, A/B, is primary for transmission. This adds the final element to our hypothetical configuration:

"Local" LCN	Primary Cable	Primary NG	Alternate NG	"Remote" LCN	Responsible Server	Alternate Server
1	A	17	18	2	5(NG 21)	6(NG 22)
1	A	18	19	3	9(NG 25)	10(NG 26)
1	A	19	20	4	13(NG 29)	14(NG 30)
2	B	21	22	1	1(NG 17)	2(NG 18)
2	B	22	23	3	10(NG 26)	11(NG 27)
2	B	23	24	4	14(NG 30)	15(NG 31)
3	A	25	26	1	2(NG 18)	3(NG 19)
3	A	26	27	2	6(NG 22)	7(NG 23)
3	A	27	28	4	15(NG 31)	16(NG 32)
4	B	29	30	1	3(NG 19)	4(NG 20)
4	B	30	31	2	7(NG 23)	8(NG 24)
4	B	31	32	3	11(NG 27)	12(NG 28)

The preceding example is not intended to be a recommendation. Rather, it was chosen to show the type of planning that must go into your preparation as size and complexity of a network increases.

2.2. ASSIGN IDENTIFIERS TO NETWORK ELEMENTS

To each LCN system— Assign a "Local System Number" (1-64) that uniquely defines this LCN system within the network. This number is used in LCN configuration and in some LCN displays.

Assign a "System Title" (1 or 2 alphanumeric characters) that uniquely defines this LCN within the network. The System Title must have at least one alpha (non-blank, non-numeric) character. The System Title is used to identify the LCN in the extended point.parameter name form used in addressing remote data. The System Title is separated from the point name by a backslash delimiter. For example: `id\pt_nam.param_nm`

Assign a 20-character "System Description" that will further identify that LCN on Universal Station displays.

To each NG— Assign a PIN local (hardware) address (1-64), to be pinned into the PIN interface board (NGIO, NIM MODEM, or fiber optic interface board). Optionally, each NG may, in the future, have a PIN global (software) address as well.

Assign the LCN node address that will be given to the NG during LCN configuration.

2.3. DETERMINE REMOTE ACCESS CONTROLS

On each LCN you need to define what access to its data will be granted to each other remote system on the PIN. The configuration procedure allows you to set access controls either one system at a time or to set access controls for all systems collectively and then establish exceptions on a system by system basis.

The levels of access to local LCN data that can be assigned to a remote system are:

- No Access (the default condition for all remote systems and all data)
- Read Only
- Read and Write

The first level of selection, per individual remote system or for all remote systems, are for these categories of data:

- System Volumes (files on the HM)
- User Volumes (files on the HM)
- Parameter Access (point data obtained from or through the CG, AM, HG, and NIM nodes)

For example, you can allow parameter read access for all connected systems (leaving the default condition of no access to System Volumes and User Volumes), and then allow read access of User Volumes to a specified LCN (or LCNs).

Further access exceptions then can be made for specific system and user volumes and for data from specific LCN nodes—either for individual remote systems or for all remote systems. Thus, the parameter read access granted in the example above could be extended to allow, for example, one or more remote systems to have write access to local UCN point data.

You may want to begin by providing read-only access to all data, then add or delete specific access exceptions as required.

NG INSTALLATION AND CONFIGURATION
Section 3

This section introduces you to characteristics of the Network Gateway and how it is used in connecting a number of LCNs to a Plant Information Network. It also includes references to other publications needed or useful for preparation of a Plant Information Network.

3.1 HARDWARE INSTALLATION AND PINNING

As previously mentioned, each NG requires the pinning of two hardware addresses. One is its PIN local address, which is located on the PIN interface board (NGIO, NIM MODEM, or fiber optic board). The other is its LCN address, which is located on the K2LCN board in dual node modules. For necessary information on NG installation and board pinning, see the *Network Gateway Site Planning and Installation* manual.

3.2 SOFTWARE CONFIGURATION STEPS

Each LCN on the Plant Information Network has to be configured individually using the information you prepared during the conceptual steps above. At each LCN you will have to enter information about

- each NG on the LCN being configured, and
- each remote system that the local LCN will communicate with.

Refer to the *Network Data Entry* manual for additional information about the displays used in the following software configuration steps.

Step 1—Define common characteristics of the local LCN that apply to all of its NGs. This is done through the "NG Local System ID" menu (reached from the Main Menu via the System Wide Values Menu). Note that this step must be completed before the system will allow you to add any NGs to its NCF. The local LCN characteristics entered at this step are

- the Local System Number (1-64),
- the System Title (2 characters—at least one of which must be an alpha),
- the System Description (20 characters),
- the first half of the optional PIN "global" address (future).

You can use form SW88-415, page 7, to record this data in advance of the configuration session at the US. You will need one copy of this form for each LCN on the network. (Sample forms suitable for copying are located in the publication *Network Forms*, SW88-405.)

Step 2—Add each individual local NG to the system's NCF through the NETWORK GATEWAY MODULE display (reached from the Main Menu via the LCN NODES and SELECT NODE TYPE displays). During this process you will, for each local NG, assign

- the local LCN node address (for communications on the LCN),
- the PIN local address (for communications on the PIN),
- the second half of the optional PIN "global" address (future), and
- the PIN cables (A or B, or A and B).

You can use the form SW88-409, page 10, to record this data in advance of the configuration session at the US. You will need one copy of this form for each NG on the network.

Step 3—Identify the remote components of the network through the "NG Remote Systems" menu (reached from the Main Menu via the System Wide Values Menu). The components to be specified for **each** remote system (LCN) are

- the remote system's identification number (1-64),
- the remote system's PIN title (2 characters—the first character must be an alpha),
- the remote system's description (20 characters),
- the local system's primary cable (A/B) for output to the remote,
- the local system's primary NG (by LCN address) for output to the remote,
- the local system's alternate NG (by LCN address) for output to the remote,
- the remote system's primary server NG (by PIN address), and
- the remote system's alternate server NG (by PIN address).

You can use the form SW88-415, page 8, to record this data in advance of the configuration session at the US. This form provides space for three remote systems, thus, for each local LCN you will need one copy of this form for every three remote systems. (A two-LCN network would require 2 copies of this form—one for each local LCN—while a 32-LCN network would require 352 copies—11 for each local LCN.)

It is recommended, but not required, that you enter the PIN addresses for the remote NGs during local LCN configuration. If you do not provide this information, the system will obtain it from each remote NG as communications are established. If you do provide this information, it will be used for verification that messages have originated from a configured server. This checking protects the local LCN from the unacceptable event of two remote systems sharing the same Local System Number due to a configuration error.

IMPORTANT: If you do specify remote NG PIN addresses, then these are the only addresses that your responsible or alternate NG will talk to. Therefore, if you locally configure remote NG (server) PIN addresses that are not the same as the actual PIN addresses of the responsible and alternate NGs on the remote LCN, you will not be able to communicate with that LCN (at least not until the addresses do match). Let's compare two examples:

	"Local" LCN	"Remote" LCN	Resp. NG	Alt. NG	Resp. Server	Alt. Server
"YOU"	1	2	10	20	3(NG 30)	4(NG 40)
"HIM"	2	1	30	40	1(NG 10)	2(NG 20)

In this case, when talking to LCN 2, LCN 1 is going to transmit through the NGs with PIN addresses 1 and 2—as expected by LCN 2. Likewise, LCN 1 is expecting to hear from LCN 2 through PIN addresses 3 and 4—as LCN 2 is configured to do. Thus, communication is possible.

	"Local" LCN	"Remote" LCN	Resp. NG	Alt. NG	Resp. Server	Alt. Server
"YOU"	1	2	10	20	5(NG 35)	6(NG 45)
"HIM"	2	1	30	40	1(NG 10)	2(NG 20)

In this second case, communication is not possible because LCN 1 expects LCN 2 messages to come from PIN addresses 5 and 6, but LCN 2 will be transmitting to LCN 1 from PIN addresses 3 and 4.

Step 4—Establish the NG Security Database to control what access of the local LCN's data is allowed to each of the remote systems.

The first levels of file access restrictions are established through the NETWORK GATEWAY SECURITY DATABASE AUTHORIZATION display (reached from the MAIN MENU via the SYSTEM WIDE VALUES menu).

At this display, you specify for an individual remote system (or optionally for all remote systems) the level of access (none, read only, or read and write) for three types of data:

- System Volumes
- User Volumes
- Parameters

You can use the form SW88-415, page 9, to record this data in advance of the configuration session at the US. This form provides space for four remote systems, thus for each local LCN you will use one copy of this form for every four remote systems depending on whether you can set the defaults for all LCNs or choose to handle each one separately. (A two-LCN network would require 2 copies of this form—one for each local LCN—while a 32-LCN network would require 256 copies—8 for each local LCN.)

Next, you can define file-specific and node-specific exceptions to the access levels just established. This is done through the NETWORK GATEWAY SECURITY DATABASE EXCEPTIONS display (reached by selecting the DEFINE EXCEPTIONS target on the NETWORK GATEWAY SECURITY DATABASE display).

Page 1 of the Define Exceptions display is used to redefine remote system access to specific files by name (Volume ID) within the categories of System Files and User Files. This access can be set for a single remote system or for all remote systems on the PIN.

You can use the form SW88-415, page 10, to record file exceptions data in advance of the configuration session at the US. This form provides space for recording five local System Files and five local User Files that you wish to establish exceptions for. The number of copies of this form that you will need will vary depending on the number of remote systems that will be granted exceptions and the number of local files for which these exceptions are to be granted.

Page 2 of the Define Exceptions display is used to redefine remote system access to data obtained from or through specific AM, CM, HG, and NM nodes on the local LCN. The specific nodes are identified by node type and the hiway/network number (HGs and NMs) or process unit ID (AMs and CMs). This access can be set for a single remote system or for all remote systems on the network.

You can use the form SW88-415, page 11, to record file exceptions data in advance of the configuration session at the US. This form provides space for recording 10 local nodes for two different remote systems (or for all LCNs) that you wish to establish exceptions for. The number of copies of this form that you will need will vary depending on the number of remote systems that will be granted exceptions (and possibly the number of local LCN nodes) for which these exceptions are to be granted.

3.3 NETWORK GATEWAY MODEM DEFINITION (BROADBAND PIN ONLY)

In broadband PINs, the modem frequency definition must match the assigned frequency band of the PIN. The frequency band information must be obtained from the PIN vendor. The modem frequency selection is made on the “NG Modem Definition” display (reached from the Main Menu by way of the System Wide Values Menu).

Redefinition of the values for the broadband network parameters is an additional step that may be necessary in the configuration of an NG. For networks over 10 miles long, it is essential to recalculate the value for the parameter "SLOT TIME," otherwise the network may collapse. Change of network parameters should not be necessary for cable lengths up to 10 miles (16 kilometers) and with up to 10 repeaters per branch of the network.

Incorrect recalculation and change of the network parameters can cause network collapse. Thus it is recommended that these changes be made only by the Honeywell services group responsible for the network configuration.

The information necessary for recalculation of network parameters is located in Appendix A of this document. Network parameter redefinition is done through the NG MODEM DEFINITION display (reached from the MAIN MENU by way of the SYSTEM WIDE VALUES menu).

CAUTION

Following a change to values in the modem definition, you must shut down all NG nodes on the PIN that have modems of the same frequency. Only after all of these NGs have been shut down and configured to the same parameters (both on the local LCN and on all the remote systems) can the NGs be restarted.

3.4 NETWORK STARTUP

Startup or restart of a PIN requires some coordination between the local LCN and each remote system. The establishment of communications between any pair of LCNs on the PIN—following NG configuration at both—requires that each LCN must request connection with the other.

Whenever an NG comes into operation, it attempts automatic connection of the local LCN to any remote LCNs on the PIN that it is the "responsible NG" for. Successful connection of the local LCN to each remote LCN requires PIN address assignment validations at both the local and the remote LCN.

Operator connection of LCNs via the PIN can be done through the NG REMOTE SYSTEM COMMUNICATION STATUS display (reached from the MAIN MENU by way of the SYSTEM STATUS display). From this display you can connect to (or disconnect from) all remote systems by a single request, or connect selectively to an individual remote system.

Additional information about the NG Remote System Communication Status display can be found in the network operation section of this manual.

3.5 NETWORK RECONFIGURATION

The following restrictions apply to PIN-related NCF configuration changes:

- An LCN's Local System Number can be assigned on-line only once. See caution below.

CAUTION

Once a nonzero Local System number has been configured, that LCN's Local System number must be changed off-line. This means that, following the update, every node on the local LCN must be shut down and restarted.

- Modification to the configuration of an existing NG node is not allowed. You can add new nodes and delete existing nodes (when the node state is Pwr On or Qualified).
- New remote systems can be added on-line by selecting "System Wide Values," then "NG Remote Systems," and adding the remote LCN by specifying the necessary data.
- A remote system can only be deleted off-line. Additionally, the Local System Number, System Title, or System Description of a remote system can only be changed off-line.
- Modification of the NG Security Database occurs without the need to disconnect the remote systems. The effect of these security changes is immediate, and can result in file/parameter access timeouts.
- (Broadband only) Modification of the NG Modem definition causes the affected NG to disconnect from all of its remote systems. Following a change to values in the modem definition, you must shut down all NG nodes on the PIN that have modems of the same frequency. Only after all of these NGs have been shut down and configured to the same parameters (both on the local LCN and on all the remote systems) can the NGs be restarted.
- Change in the selection of PIN network (cable A or B) to be used for sending messages to a particular remote does not cause disconnection from the remote system. All NGs on the system are notified as part of the installation, and respond by sending the next message on the specified cable.

CAUTION

When making on-line NCF changes that affect "NG Remote Systems" it is important to reload all local nodes showing "moderate" or "high" impact after the new NCF has been installed. Use the System Menu's NCF STATUS display to determine which local nodes show "moderate" or "high" impact. As each of these nodes are reloaded they will be synchronized with the new NCF. Also, depending what changes are made, the NG(s) residing on the OTHER LCN(s) may also have to be reloaded to incorporate the changes.

NETWORK OPERATION
Section 4

This section introduces you to the Universal Station displays that provide detailed information about the current status of the PIN and this LCN's connections to it.

4.1 INTRODUCTION

There are two sets of displays that show current operating status of the PIN as it relates to the local LCN:

- Network Gateway Status Detail displays—these displays provide information about the local LCN's PIN connections and communications.

- NG Remote System Communication Status display—this display provides an overview of the PIN network as seen from the local LCN.

4.2 NETWORK GATEWAY STATUS DETAIL DISPLAYS

The NG Status Detail displays consist of the following:

- Status Detail Display for (NG) node nn,
- NG Object Detail Status Display (used to select a detailed view of one remote system),
- NG xx's View of Connections to Remote LCN yy (detail view of a local LCN's connections to a selected remote system), and
- NG Status Messages Pending Against Remote LCN yy (configuration error message log for the local LCN).

4.2.1 NG Node Status Detail Display

Access method:

From the Main Menu	select SYSTEM STATUS
From System Status	select GATEWAYS
From Gateways	select an NG, then select STATUS DETAIL

This display (Figure 4-1) contains configuration and communications information about the selected NG node's connection to the PIN. Select ROLL RIGHT to view the portion of these messages not initially visible (Figure 4-2).

When you select either the "PIN Comm" or "PIN Config" line (the first or second line of this display) a VIEW OBJECT DETAIL target appears. Use that target to select the NG Object Detail display.

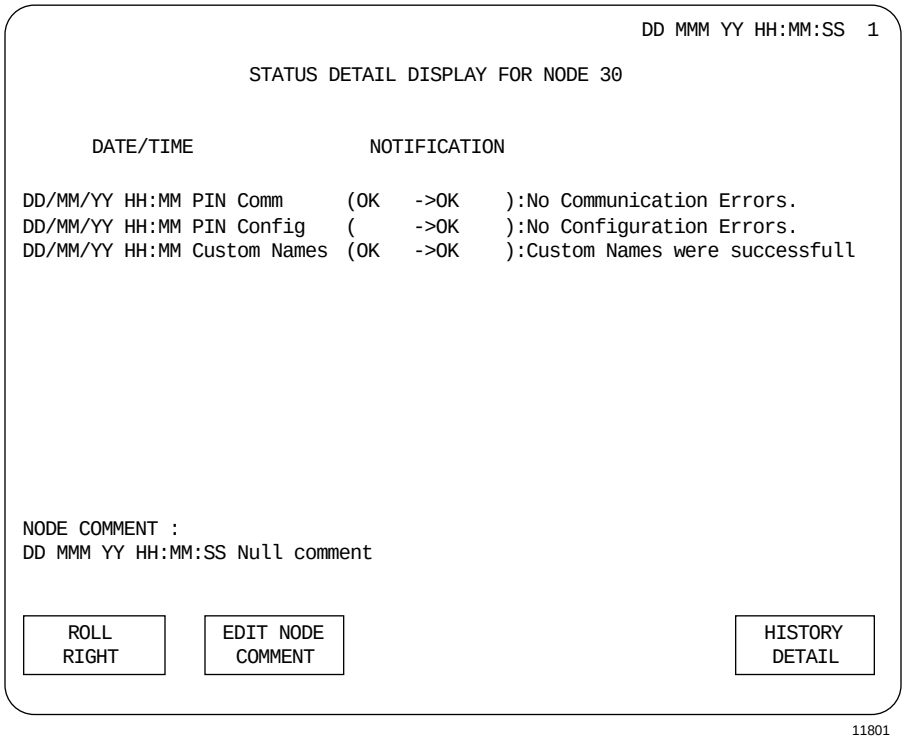

Figure 4-1 — NG Status Detail Display

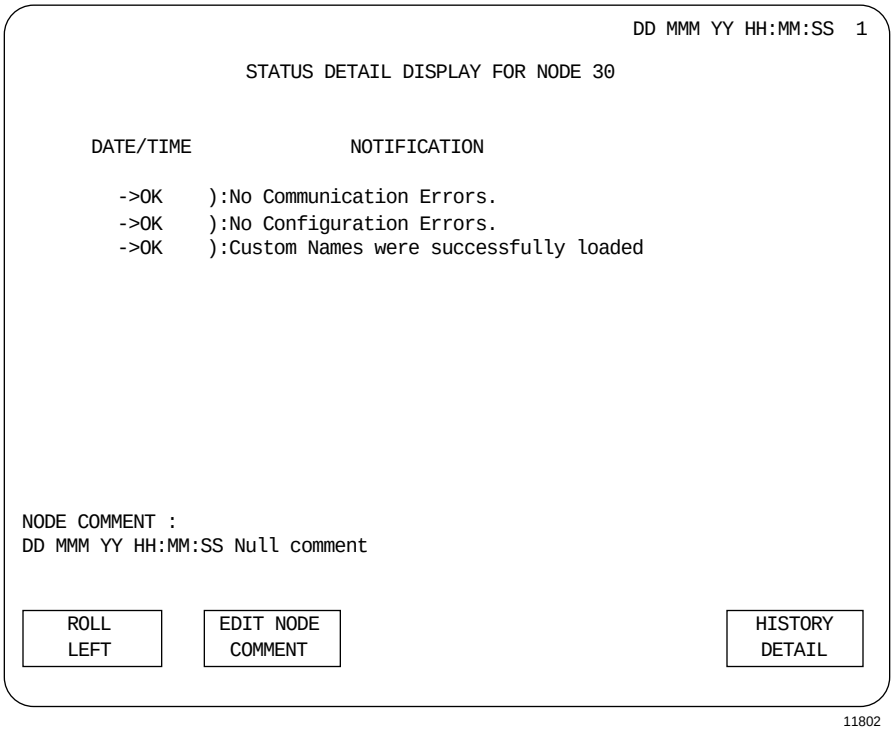

Figure 4-2 — "Roll Right" View of NG Status Detail Display

4.2.2 NG Object Detail Status Display

Access method:

From the Main Menu	select SYSTEM STATUS
From System Status	select GATEWAYS
From Gateways	select an NG, then select STATUS DETAIL
From Status Detail	select PIN COMM, then select VIEW OBJECT DETAIL

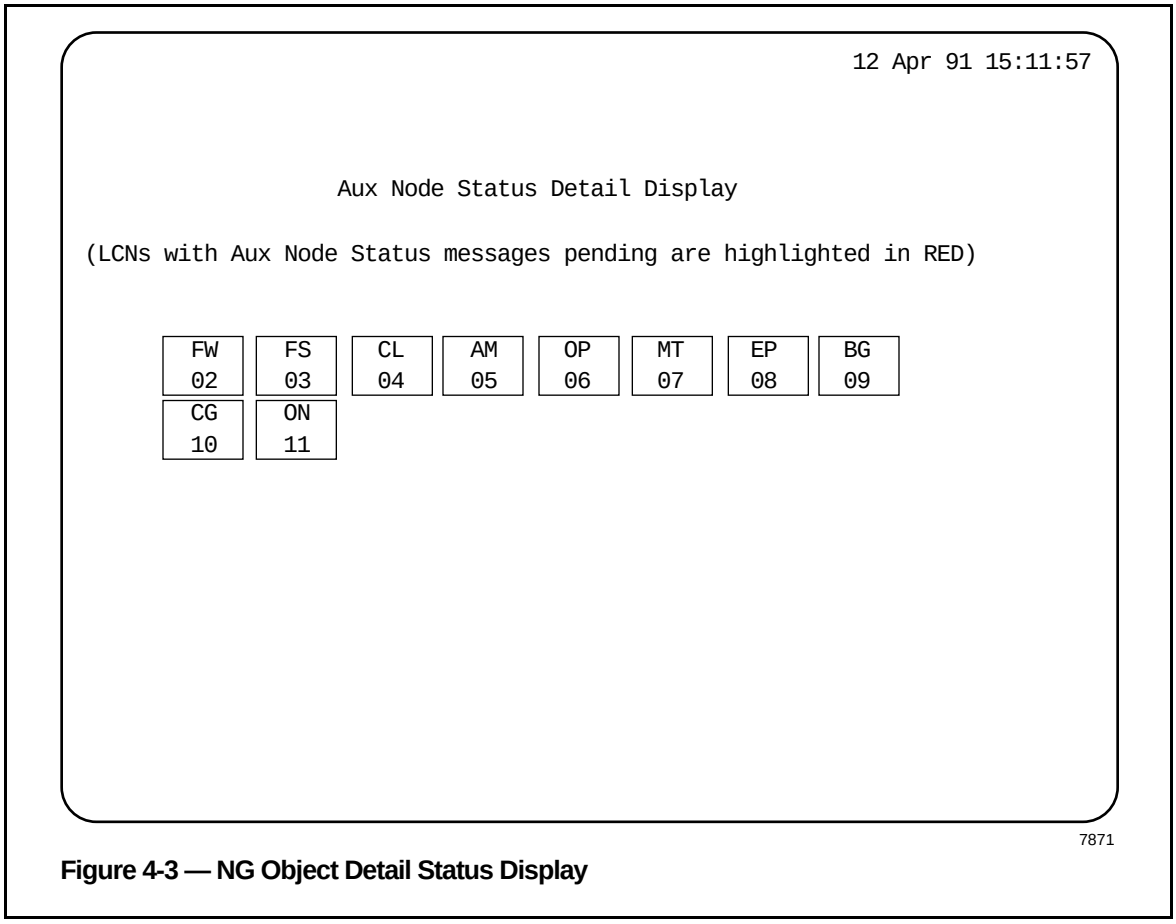

Figure 4-3 — NG Object Detail Status Display

This display shows each of the configured remote systems on this PIN. Each is identified by its System Title and its Local System Number. The box for an individual remote system shows in red if there are any status messages pending that concern that LCN.

Selecting one of the remote system boxes produces the display showing the local LCN's view of that remote LCN.

4.2.3 View of Connections to Remote LCN

Access method:

From the Main Menu	select SYSTEM STATUS
From System Status	select GATEWAYS
From Gateways	select an NG, then select STATUS DETAIL
From Status Detail	select PIN COMM, then select VIEW OBJECT DETAIL
From View Object Detail	select a Remote LCN

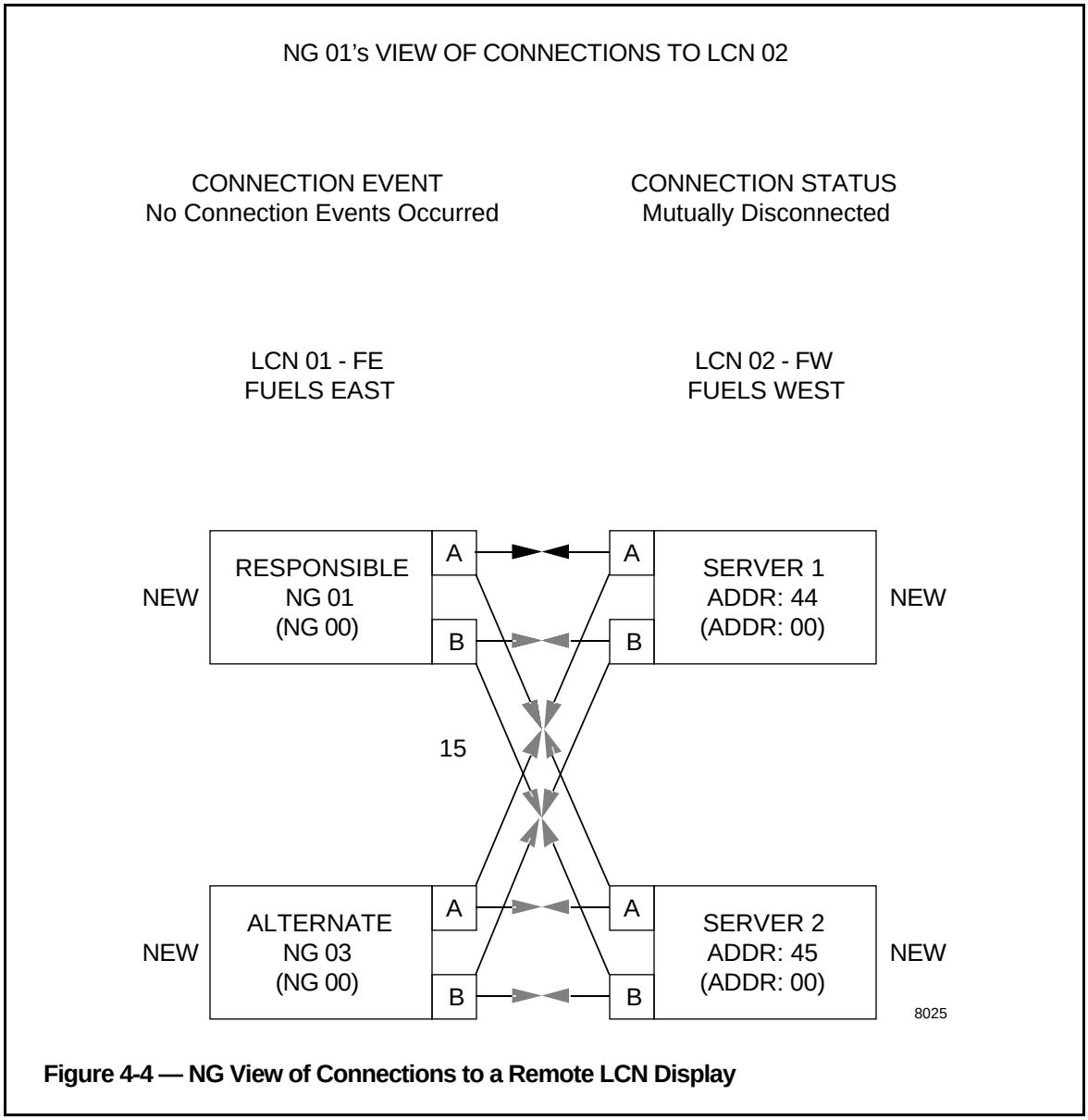

Figure 4-4 — NG View of Connections to a Remote LCN Display

This display presents a comprehensive view of the connection status between the local "responsible" and "alternate" NGs and the responsible (Server 1) and alternate (Server 2) NGs at the selected remote system.

The following figure repeats the preceding detail display and adds reference numbers that identify its key fields.

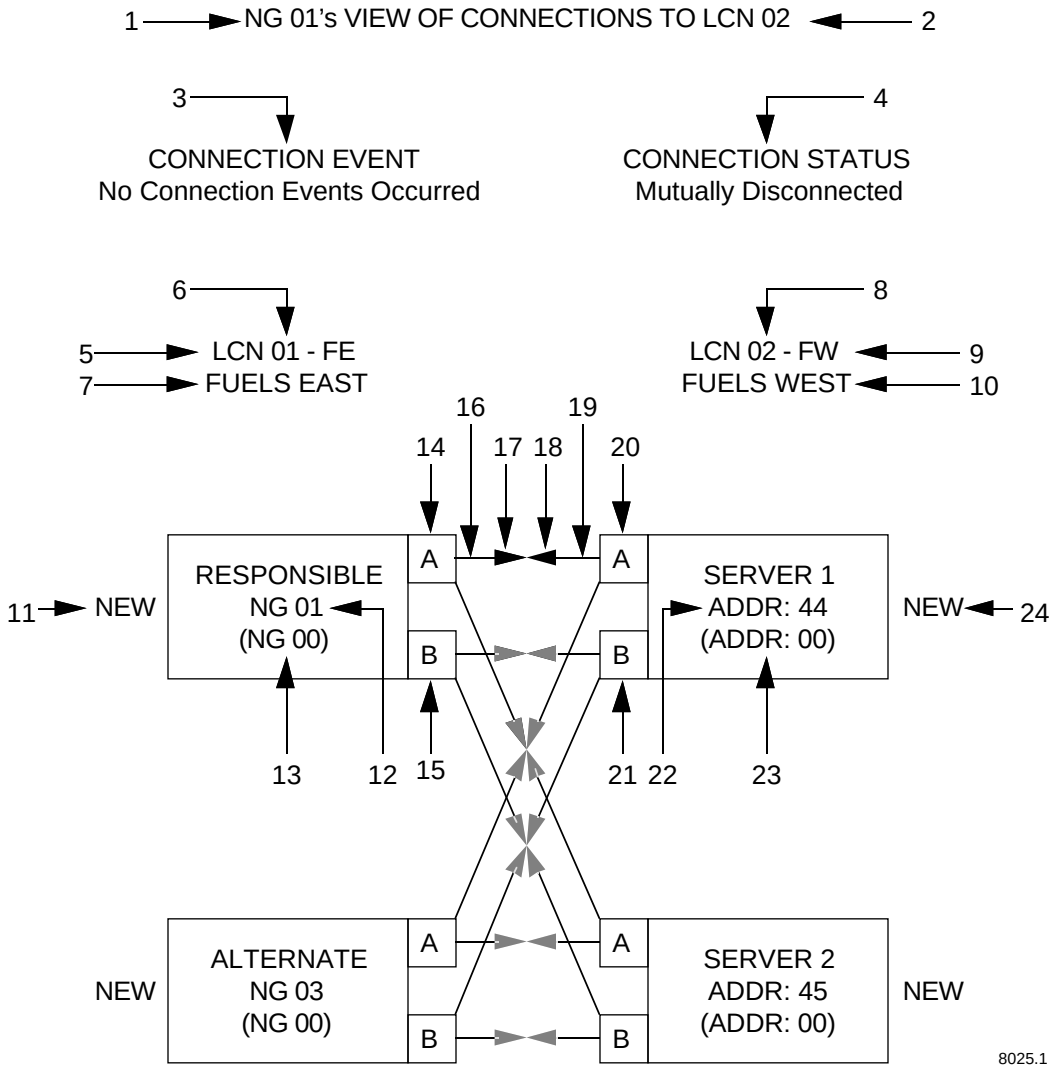

Figure 4-5 — NG View of Connections to a Remote LCN Display with Callouts Added

The reference numbers in Figure 4-3 correspond to the following field definitions.

1. The Local System Number of the local NG that is supplying the data for this display and corresponds to the NG you selected before you selected STATUS DETAIL on the Gateways display.

2. The Local System Number of the remote system you selected on Page 1 of the Aux Node Status Detail display.

3. Under the heading "CONNECTION EVENT," is a message that identifies the most recent connection event that has occurred relative to this local-remote system pair. The event messages that can appear here are:

    - No Connection Events Occurred
    - Disconnected By Request
    - Disconnected By System
    - Connection Rerouted By User
    - Connection Rerouted By System
    - Connection By User
    - Remote Requested Connection
    - Requesting Connection

4. Under the heading "CONNECTION STATUS," is a message that identifies the status of the connection between the local LCN and the remote system. The status messages that can appear here are:

    - Connected To Remote
    - Remote Connected to this LCN
    - Mutually Connected
    - Mutually Disconnected

5. The "Local System Number" assigned to the local LCN.

6. The "System Title" assigned to the local LCN.

7. The "System Description" assigned to the local LCN.

8. The "Local System Number" assigned to the remote system.

9. The "System Title" assigned to the remote system.

10. The "System Description" assigned to the remote system.

11. Indicates any change of the responsible NG assignment for the local LCN since the previous configuration. The possible values are:

    - [blank]—no changes since the last configuration activity
    - NEW—there was not a responsible NG and one has been assigned
    - CHANGED—a different responsible NG has been assigned
    - DELETED—there was a responsible NG but it has been de-assigned

12. The LCN node address of the current responsible NG at the local LCN.

13. The previous responsible NG for the local LCN. This value will not appear if no changes have occurred.

14. Indicates that cable "A" has been configured for the local NG.

15. Indicates that cable "B" has been configured for the local NG.

16. This line from the local NG provides two indications. First, its presence indicates that a connection to the remote NG using this path is possible. Second, its color indicates the transmission quality of the communication path:

    • Black = cable quality information not available
    • Green = good
    • Yellow = suspect/degraded
    • Red = failed

17. The arrow, if present, indicates that the last message in the direction indicated by the arrow occurred on this cable. The arrowhead will be the same color as the line leading from the local NG.

18. The arrow, if present, indicates that the last message in the direction indicated by the arrow occurred on this cable. The arrowhead will be the same color as the line leading from the remote NG.

19. This line from the remote NG provides two indications. First, its presence indicates that a connection to the local NG using this path is possible. Second, its color indicates the transmission quality of the communication path:

    • Black = cable quality information not available
    • Green = good
    • Yellow = suspect/degraded
    • Red = failed

20. Indicates that cable "A" has been configured for the remote NG.

21. Indicates that cable "B" has been configured for the remote NG.

22. The PIN local address of the current responsible NG (Server 1) at the remote system.

23. The previous responsible NG for the remote system. This value will not appear if no changes have occurred.

24. Indicates any change of the responsible NG (Server 1) assignment for the remote system. The possible values are:

    • NEW
    • CHANGED
    • DELETED

The definitions for the local Alternate and remote Server 2 NG blocks are almost identical to those for the local Responsible and remote Server 1 NG blocks.

Use the "DISP FWD" key to move to the next node detail display.

4.2.4 NG Status Messages Display

Access method:

From the Main Menu	select SYSTEM STATUS
From System Status	select GATEWAYS
From Gateways	select an NG, then select STATUS DETAIL
From Status Detail	select PIN COMM, then select VIEW OBJECT DETAIL
From View Object Detail	select a Remote LCN
From the Remote LCN display	press the DISP FWD key

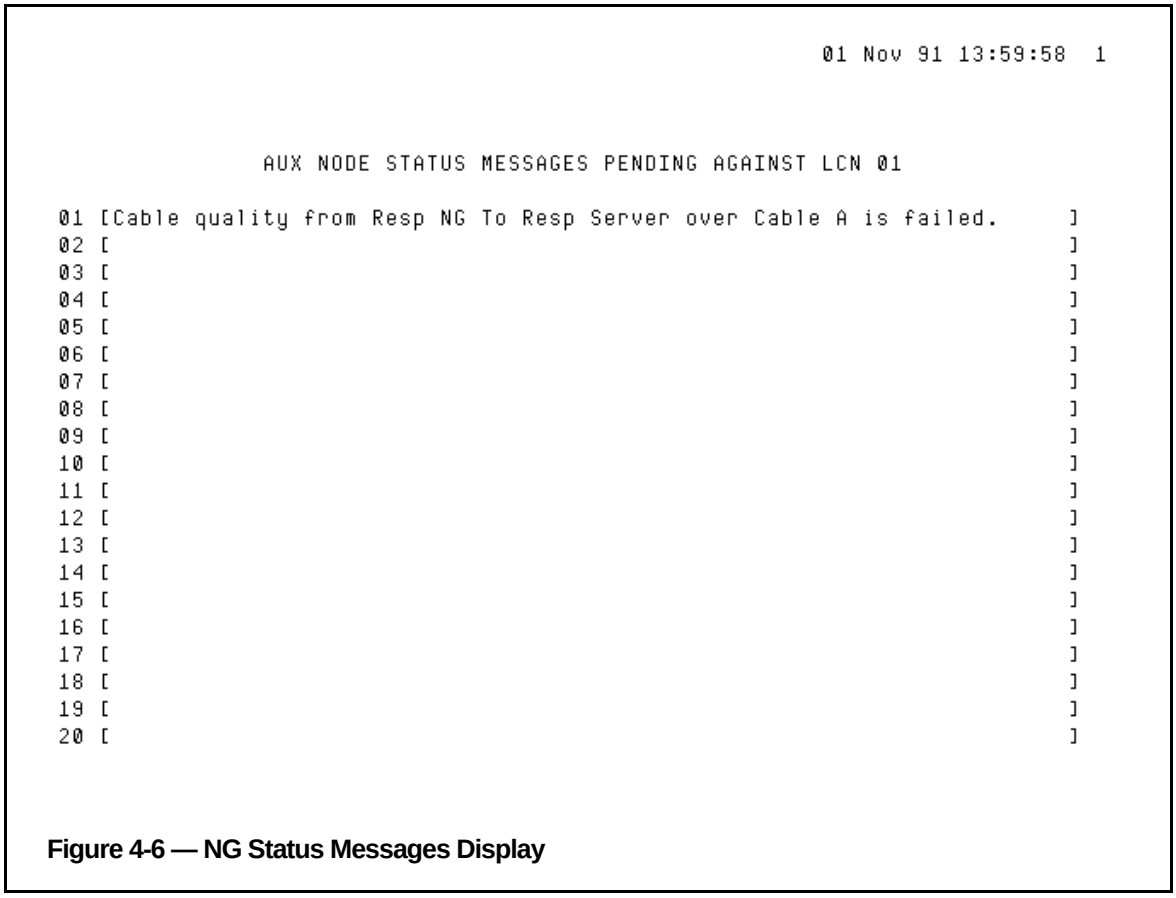

Figure 4-6 — NG Status Messages Display

This detail display provides up to 20 current network status messages resulting from configuration or operation errors at the local LCN. Each message is specific to the problem and is intended to be self-explanatory. Each of these messages is due to one of four types of error:

- On-line NCF configuration error
- Mismatch of the local LCN database with remote system database values.
- An improper request (e.g., requesting "A" Cable Only when there is no "A" cable connection).
- A cable quality change on a viable communications path.

Note that some of these errors require NG shutdown and reload as part of the recovery procedure.

4.3 NG REMOTE SYSTEM COMMUNICATION STATUS DISPLAY

The NG Remote System Communication Status display presents an overview of the configured PIN network as seen by the local LCN and includes the status of all configured communication paths. Depending on the number of systems in the network, this can be a multipage display (it can show only the communication status of the local LCN with eight remote systems at a time).

Access method:

From the Main Menu	select SYSTEM STATUS
From System Status	select GATEWAYS
From Gateways	select an NG, then select NTWK STATUS

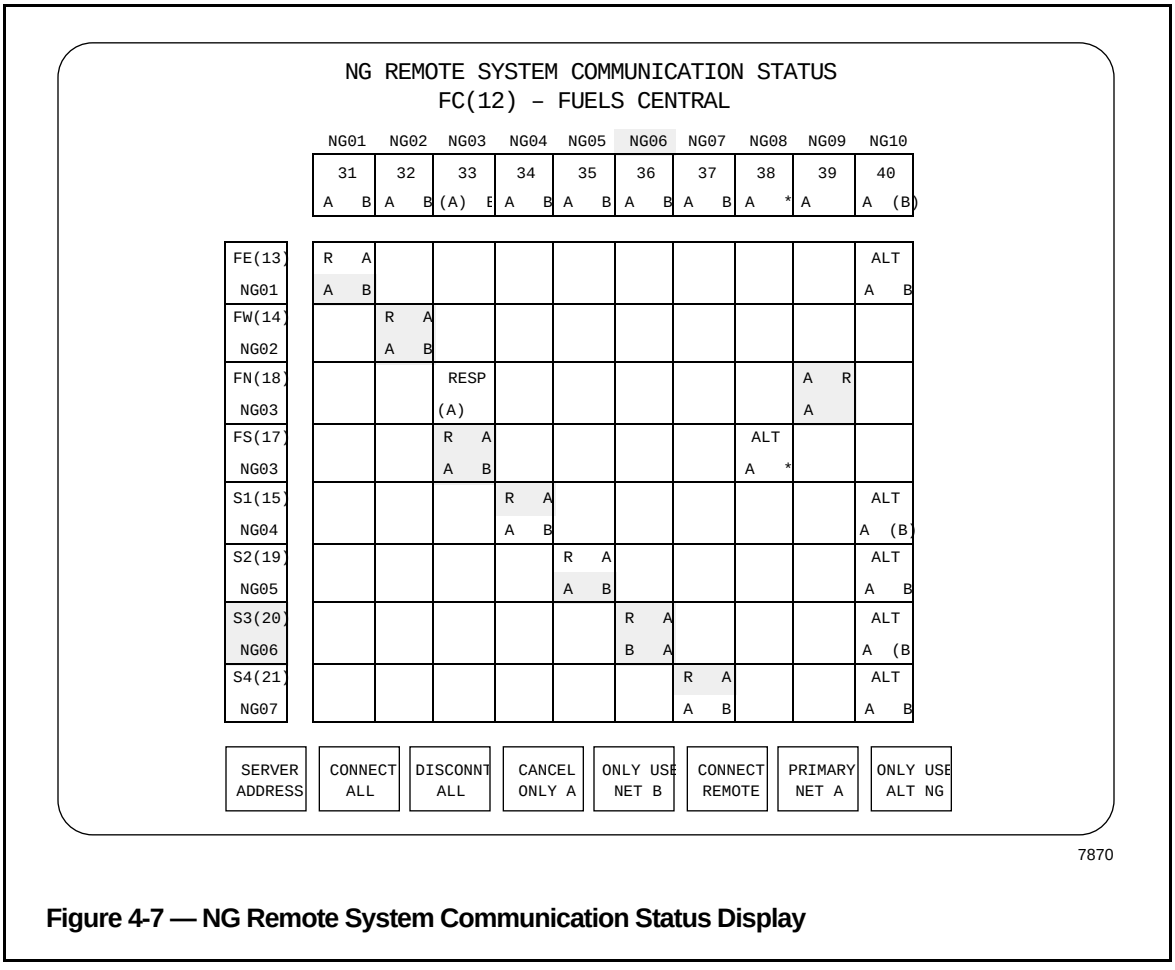

Figure 4-7 — NG Remote System Communication Status Display

To interpret contents of this display, let's first break it into its major parts:

- the heading
- the top row of boxes
- the left-hand column of boxes
- the bottom row of boxes
- the 10 column by 8 row matrix of boxes

The heading consists of fixed text (NG REMOTE SYSTEM COMMUNICATION STATUS), and a variable part, composed of the Local System Title (in the above example, FC), the Local System Number (12), and the local System Description (FUELS CENTRAL).

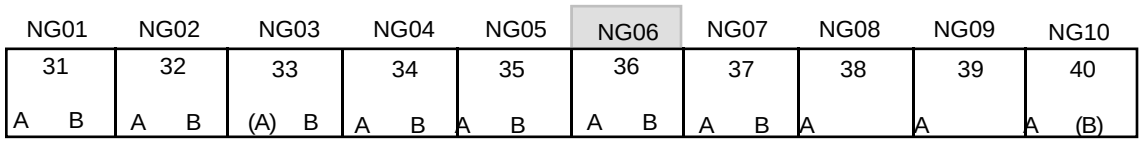

Figure 4-8 — NG Remote System Communication Status Display (top row of boxes) 6914

The top row of of boxes in this display shows the 10 possible NGs for the local LCN, each identified by its local LCN node address. The LCN node address of the NG used to call up this display is shown in reverse video. The number in the upper half of each box identifies the NG's PIN local address. The characters in the lower half represent the worst case status of communication for that NG with all other remote NGs with which it communicates.

- A—cable "A" status is good
- (A)—cable "A" status is fair
- B—cable "B" status is good
- (B)—cable "B" status is fair
- @—cable (A or B) has been disabled, status is good
- (@)—cable (A or B) has been disabled, status is fair
- *—cable (A or B) has failed

Note that in this top row, cable cable "A" status is always in the lower left-hand part of the box and cable "B" status is always shown in the lower right-hand part of the box. A blank in either the lower left-hand or lower right-hand portion of the box indicates that the associated cable (A or B) is not configured.

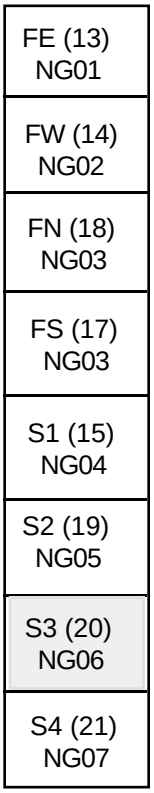

Figure 4-9 — NG Remote System Communication Status Display (left-hand column) 6913

The left-hand column of this display shows up to eight of the possible 63 remote systems that could communicate with the local LCN. Each box in this column serves as a header for the 10 by 8 matrix row to its right. Each block of the column shows the "System Name" and the "Local System Number" of a remote system, plus the LCN node address of the local NG that is assigned as the "responsible" communication path to this remote system.

Each of the row header boxes in the left-hand column is an individually selectable target. When one is selected, additional targets appear on the bottom row of the display.

To display the next eight remote systems, press "Page Fwd." The last page may not be full depending on the number of remote systems configured.

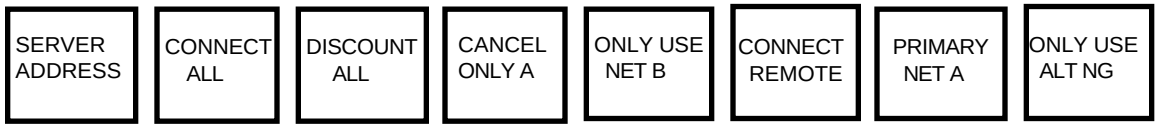

Figure 4-10 — NG Remote System Communication Status Display (bottom row of boxes) 6915

The bottom row of boxes provide the targets that cause various actions to occur. Five of the eight boxes always appear although the contents of three of them toggle with use:

- "Server Type" or "Server Address"
- "Connect All"
- "Disconnect All"
- "Only Use Net A" or "Cancel Only A"
- "Only Use Net B" or "Cancel Only B"

The remaining three target boxes on the bottom row appear only when a specific remote system has been selected by picking its box in the left-hand column. These targets show:

- "Only Use Alt NG" or "Cancel Only Alt"
- "Primary Net A" or "Primary Net B"
- "Connect Remote" or "Disconnect Remote"

The following explains the result from selecting one of the bottom row target boxes:

Server Type—(initial condition) causes boxes in the 10 by 8 matrix to show for each remote system which of its NGs, Responsible or Alternate, is active.

Server Address—causes boxes in the 10 by 8 matrix to display the PIN local addresses of each remote system's Responsible and Alternate NGs.

Primary Net A—forces all outgoing communications to PIN Network A, if possible. Retry on PIN Network B is permitted. This selection only affects communication with the selected remote system. Communications with any other remote systems handled by the same NG are not affected.

Primary Net B—forces all outgoing communications to PIN Network B, if possible. Retry on PIN Network A is permitted. This selection only affects communication with the selected remote system. Communications with any other remote systems handled by the same NG are not affected.

Only Use Alt NG—forces all communication with the selected remote system to be routed through the NG configured as the alternate communication path. This normally is done when the responsible NG has to be shut down for maintenance.

Cancel Only Alt—forces communication with the selected remote system to be routed through the NG configured as responsible for this communication path. Should the responsible NG be unable to communicate with the remote system, use of the alternate NG will be attempted.

CAUTION

The ONLY USE ALT NG target is supported in R410 and later releases. This target should be used with caution since it leaves the system with no alternate path. Its intended use is to provide a “bumpless” means of powering off the responsible NG. If the responsible NG is powered off without selecting the ONLY USE ALT NG target, any pending intersystem file manager activity will be suspended, and pending parameter accesses may have to be retried.

After the responsible NG is powered off, we recommend that you **immediately** select the CANCEL ONLY ALT target. Then, when the responsible NG is reloaded, it will automatically (and bumplessly) become active and the alternate NG will be used as an alternate route, if necessary. By selecting the CANCEL ONLY ALT target immediately after powering off the responsible NG, you eliminate the possibility that you might forget to do so later, which would leave you running only on the alternate NG, even though the responsible NG is available.

Connect Remote—enables communication with the selected remote system. Because communication can only occur by mutual consent, the selected remote system must also be connected to this local LCN before communication can begin.

Disconnect Remote—disables communication with the selected remote system. No further communication takes place until both the local LCN and the remote system have mutually reconnected to each other.

Connect All—enables communication with all configured remote systems. Because communication can only occur by mutual consent, each individual remote system must also be connected to this local LCN before communication can begin.

Disconnect All—disables communication with all configured remote systems. No further communication takes place until both the local LCN and the remote systems have mutually reconnected to each other. This function is provided to quickly shed load associated with remote systems during periods of system upset.

Only Use Net A—forces all outgoing communications from all NGs on the local LCN to PIN network A. Retry on PIN Network B is explicitly prohibited. The message "PIN Override: Always A" appears above the left-hand column. This function is provided to support cable maintenance on PIN network B (for example, to allow switching out an amplifier on the PIN network B cable).

Cancel Only A—allows outgoing communications from NGs on the local LCN to occur on either PIN network as configured. Retry on the redundant network is permitted.

Only Use Net B—forces all outgoing communications from all NGs on the local LCN to PIN network B. Retry on PIN Network A is explicitly prohibited. The message "PIN Override: Always B" appears above the left-hand column. This function is provided to support cable maintenance on PIN network A (for example, to allow switching out an amplifier on the PIN network A cable).

Cancel Only B—allows outgoing communications from NGs on the local LCN to occur on either PIN network as configured. Retry on the redundant network is permitted.

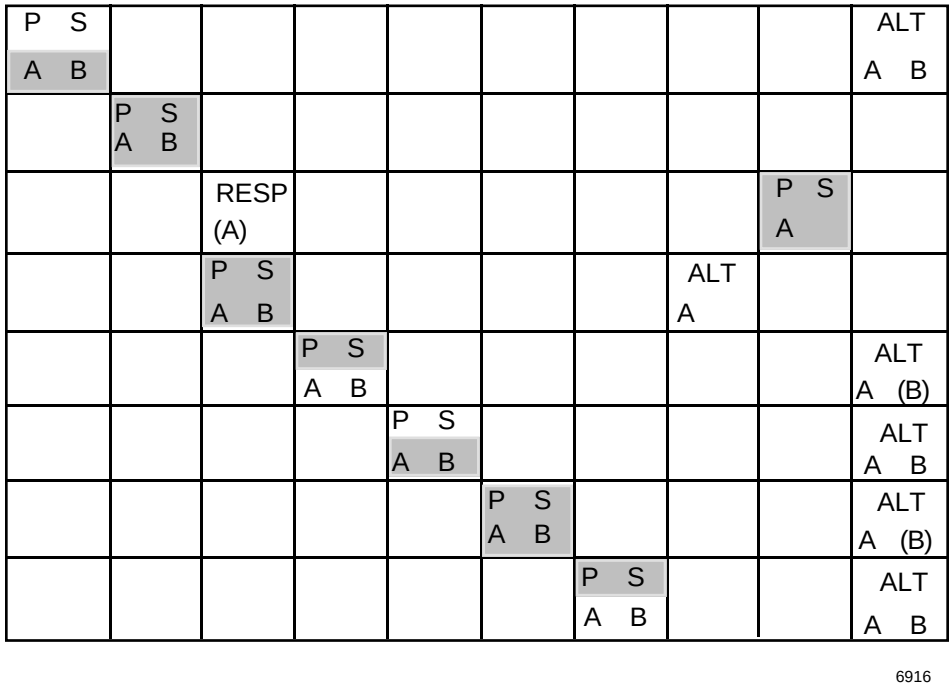

Figure 4-11 — NG Remote System Communication Status Display (10 x 8 matrix)

The 10 by 8 matrix of boxes contains information about communication status between the local LCN and remote systems. This information is contained in the boxes found at the intersections of a local NG (identified in the top row of boxes) and a remote system (identified in the left-hand column of boxes). There can be two intersections between the local LCN and each remote system, one for the "responsible" NG and one for the "alternate" NG. The remaining boxes of the matrix are void of data.

The information contained in the **upper half** of each matrix box is controlled by current status of the "Server Address"/"Server Type" target in the bottom row of this display. EXCEPTION: The box representing the inactive NG always displays either RESP or ALT centered in the top half.

When **Server Address** has been selected, the **upper half** of the box representing the active NG shows the PIN local addresses of the active and inactive remote NGs. The upper half of the box is divided in half.

- The left-hand portion shows the PIN address of the active remote NG.
- The right-hand portion shows the PIN address of the inactive NG (if one is present).

When **Server Type** has been selected, the **upper half** of the box representing the active NG shows which remote NG is active, the Responsible or the Alternate. The upper portion of the box is divided in half.

- The left-hand portion contains an "R" when the Responsible NG is active, an "A" when the Alternate is active, or is blank when the active server is unknown or unassigned.

- The right-hand portion contains an "R" when the Responsible NG is inactive, an "A" when the Alternate is inactive, or is blank if there is no Alternate.

- The characters shown in the **lower half** of each box always represent the status of the communication paths (cable A and cable B) between the remote and local NGs. Communications status on the configured primary PIN cable always appears in the left-hand quarter of the bottom half. Communication status on the backup cable appears in the right-hand quarter. The status indicators are:

  A—status of cable "A" is good
  (A)—status of cable "A" is fair
  B—status of cable "B" is good
  (B)—status of cable "B" is fair
  @—cable (A or B) has been disabled, status is good
  (@)—cable (A or B) has been disabled, status is fair
  *—status of cable (A or B) is degraded
  blank = not configured

Inverse video in the box representing the **active** local NG is used to show the status of software connection between the local and remote systems. The inactive local NG box is always shown in normal video. For the purpose of indicating connection status, each box in the matrix is divided into upper and lower halves. The rules are:

Box normal—neither the local LCN nor the remote system has requested connection and no information can be exchanged.

Upper half inverse, lower half normal—only the remote system has requested connection and no information can be exchanged. (Independent of cable quality.)

Lower half inverse, upper half normal—only the local LCN has requested connection and no information can be exchanged. (Cable quality must be good.)

Box inverse—both the local and remote systems have requested connection and information can be exchanged. (Cable quality must be good.)

MODEM PARAMETER TUNING
Appendix A

This appendix explains when the Network Gateway's modem definition parameters may need to be modified and how to calculate the new parameter values.

A.1 RECOMMENDATIONS

CAUTION

The parameter SLOT TIME must have the correct value for the network, otherwise the network will collapse. For each network, the SLOT TIME value must accommodate delays caused by cable length and repeaters.

The default values for the Network Gateway modem definition parameters should not require modification for networks with less than 10 miles of cables on each branch and 10 repeaters per branch. For networks over 10 miles long on a branch, the SLOT TIME value must be recalculated according to the formula in this appendix. Values for other, related, parameters also must be recalculated.

"Tuning" of the network parameters, based on the number of nodes and total cable length, may be necessary to ensure that, during high load conditions, the higher priority messages are transmitted before lower priority ones. If the default values are used during high load conditions, nodes can send lower priority messages while other nodes are waiting with higher priority messages. However, a high load condition is unlikely since the network is fast (10 Mbits per second) and, in most cases, the number of NGs on the network will be less than 30. Tuning of these parameters will not have any effect on network performance when the network load is not high.

To decrease the probability of errors—and resulting network collapse—it is strongly recommended that all parameter calculations be performed by the Honeywell services group responsible for the network configuration.

Any network parameters not mentioned in this appendix must **not** be modified. They are IEEE 802.4 standard-related network parameters. The cable length or number of nodes on the network does not have any impact on those parameters.

NOTE

Before attempting to use the information contained in this appendix, be sure that you have a sufficient understanding of IEEE standard 802.4.

A.2 ESTABLISHING THE SLOT TIME VALUE

Slot time is proportional to the sum of the following:

- Node latency to respond to a received message,
- Propagation delay time in the medium and repeaters connecting the source and destination nodes, and
- Message reception delay time in the destination node.

NOTE

Making the value of SLOT TIME larger than necessary is always safe. However, a too small value for SLOT TIME can result in network collapse.

SLOT TIME is calculated in terms of octet times (defined as the time to transmit/receive 8 bits of data on the network). The following equation is used to derive the SLOT TIME (octet_times) for a network:

$$\text{SLOT TIME} = C + \left(4 \times \frac{(PD \times CL) + RD}{OT}\right)$$

C = 70 octet_times
"C" is the sum of node delay time to respond, modem delays to receive/transmit messages, head-end remodulator latency to receive and to retransmit messages, plus 30 octets of safety margin.

PD = Propagation delay time in microseconds per unit cable length (mile, kilometer, etc.)
The actual propagation delay time depends on the type of cable used. However, the values below are close enough that they can be used for SLOT TIME calculation for any type of cable.

PD = 8 μsec per mile (if cable length is calculated in miles)
PD = 5 μsec per kilometer (if cable length is calculated in kilometers)
PD = 1.5 μsec per 1000 feet of cable (if cable length is calculated in 1000 foot units)

CL = Cable length in the longest branch of the network from headend to the terminator
Honeywell does not offer NG in Broadband, only in Fiber (10 Mbit/second), and Carrierband (UCN 5 Mb/second).

This parameter must use the same unit of measurement (miles, kilometers, or 1000 feet units) as the cable length for the "PD" parameter as described above.

RD = Repeater(s) delay in microseconds
This is the propagation delay through the repeaters in the branch with the most repeaters.

OT = Octet Time = Octet time is the time required to transmit/receive each extra 8 bits of data on the network.

OT = .8 microsecond for 10 Mbit/second network
1.6 microseconds for 5 Mbit/second network

Default Slot Time = 625 octets

NOTE

The default slot time is large enough to accommodate long networks using Fiber or Carrierband technology. However, it can be recalculated based on the network characteristics of each site.

A.3 HIGH PRIORITY TOKEN HOLD TIME

When the node receives the token, frames are transmitted from the highest priority queue until either the HIGH PRIORITY TOKEN HOLD TIME expires or the queue is empty.

$$\text{HIGH PRIORITY TOKEN HOLD TIME} = \left(\frac{\text{1024 Octets per Frame}}{8} \right) = 128 \text{ octet-times}$$

The constant "8" is required by the Token Bus Controller. The value of this parameter should **not** be modified for specific installations since it does not depend on cable length. It should only be modified if the maximum frame length used in the Network Gateway software changes from 1024.

DEFAULT = 128 octet-time

A.4 TARGET ROTATION TIME

After the HIGH PRIORITY TOKEN HOLD TIME expires or the queue is empty, the PRIORITY 1 TARGET ROTATION TIME is checked. If the PRIORITY 1 TARGET ROTATION TIME has not expired, frames from the Priority 1 queue are transmitted until either there are no more frames in the queue or the Priority 1 timer has expired. Then, the target rotation times for priorities 2 and 3 are checked one after the other and frames from their queues are transmitted until their timers expire. This scheme allow the nodes to transmit lower priority frames only when the network load is low enough to permit all higher priority frames to be transmitted by each node on the network. Following is the general equation for target rotation times for priorities 1 through 3:

$$\text{TARGET ROTATION TIME} = \left(\frac{1}{1 - \text{Network Load}} \right) \times \left(\frac{\text{TRT}}{8} \right)$$

The constant "8" is required by the Token Bus Controller.

Network Load is the percentage of the network load above which the nodes stop transmitting frames from the designated priority.

TRT (in octet-times) is the token rotation time at zero percent network load (i.e., no data messages)

$$\text{TRT} = \text{Number of Nodes} \left(\frac{\text{SLOT TIME}}{2} + 26 \right)$$

The constant "26" represents the number of octets in a token frame.

DEFAULTS FOR TARGET ROTATION TIME:

Priority 1 = 8190 octet-times
Priority 2 = 6800 octet-times
Priority 3 = 3500 octet-times

NOTE

These times are calculated based on 64 nodes and 13 miles of copper cable on each branch (for fiber).

Honeywell recommends that the network load for priorities 1 through 3 be set at 75%, 65%, and 50%, respectively. Using these values, the target rotation times will be:

$$\text{PRIORITY 1 TARGET ROTATION TIME} = \left(\frac{1}{1 - 0.75}\right) \times \left(\frac{TRT}{8}\right) = 0.50\ TRT$$

$$\text{PRIORITY 2 TARGET ROTATION TIME} = \left(\frac{1}{1 - 0.65}\right) \times \left(\frac{TRT}{8}\right) = 0.35\ TRT$$

$$\text{PRIORITY 3 TARGET ROTATION TIME} = \left(\frac{1}{1 - 0.50}\right) \times \left(\frac{TRT}{8}\right) = 0.25\ TRT$$

IMPORTANT: The numbers derived from the above equations for the target rotation time for each priority must be an integer smaller than 8190, and should be decreasing. The 8190 limit is a Token Bus Controller requirement.

A.5 TARGET ROTATION TIME FOR RING MAINTENANCE

This parameter is calculated by using the equation for token rotation time using the network load at 40%.

$$\text{TARGET ROTATION TIME FOR RING MAINTENANCE} = \left(\frac{1}{1 - 0.40}\right) \times \left(\frac{TRT}{8}\right) = 0.20\ TRT$$

IMPORTANT: The resulting value must be an integer value smaller than 8190.

DEFAULT = 3500 octet-time

A.6 MAXIMUM INTER-SOLICIT COUNT

The MAXIMUM INTER-SOLICIT COUNT parameter controls how often the nodes on the network try to extend invitation to the other nodes to join the token ring. The value for this parameter should be selected as large as possible so that the band within an established network is not wasted. The range of values for this parameter is 16 through 255.

DEFAULT = 250

GLOSSARY
Appendix B

This appendix explains terms and acronyms unique to the Network Gateway. For a complete glossary of **TotalPlant** *Solution (TPS) System terms and acronyms, consult Appendix A of the System Overview, SW70-400.*

Alternate NG—The NG selected as the alternate communications path between the local system and a remote system connected to the same PIN. There must be at least two NGs at both the local and the remote system in order to establish responsible and alternate NGs.

Alternate NG Server—The alternate NG server is another name for the remote LCN's "alternate Network Gateway." It is described in terms of its PIN local address.

LCN node address—A two-digit number that uniquely identifies a node (e.g., an NG) on a TPS Local Control Network.

Local Control Network (LCN)—The TPS communications bus that connects multiple processing nodes. A Network Gateway (NG) is one such node type.

Local LCN—Term used to differentiate a host LCN from other (remote) systems during PIN planning and configuration. The PIN configuration information is entered separately at each individual LCN, thus each LCN is "local" for one configuration session and a "remote" for all others.

Local System Number—A two-digit number (1-64) that uniquely identifies an LCN system on a PIN.

Network Gateway (NG)—An LCN node used to exchange information between the local LCN and one or more remote systems. Currently, the list of supported remote systems is limited to TPS Local Control Networks. The NG interconnects with other systems through an "open system" Plant Information Network (PIN) running an IEEE 802.4 protocol on either a 5 Mb/s Carrierband network, a 10 Mb/s Broadband network, or a 10 Mb/s fiber optic network.

Network Gateway Server—Communication with a remote system involves the use of a local Network Gateway that communicates with a remote Network Gateway server, both of which are connected to the same PIN. When the target system is an LCN, the remote Network Gateway Server is a Network Gateway node.

NG—Abbreviation of Network Gateway.

PIN—Abbreviation of Plant Information Network.

PIN global address—An optional method of PIN node identification that is not currently supported.

PIN local address—A two-digit number that uniquely identifies each NG on the PIN. Established by physical pinning on a communications board.

Plant Information Network (PIN)—A communication bus which links all NGs together independent of the LCNs they also are connected to. The PIN often consists of two redundant networks labeled "A" and "B."

Remote LCN—see remote system.

Remote system—Nodes on the local LCN are able to exchange information with systems not attached to the local LCN. A "remote system" can be another Honeywell LCN network or another vendor's network and/or computer (future implementation). Also see "System."

Responsible NG—The NG selected as the primary communications path between the local system and a remote system connected to the same PIN.

Responsible NG Server—The responsible NG server is another name for the remote LCN's "responsible Network Gateway."

System—A computer or collection of computers with which a Network Gateway is able to exchange files and process control data. The generic term "system" is used in place of the proprietary term LCN to describe the remote systems with which the Network Gateway interfaces. This was done to provide for future phases of the NG development that are intended to allow it to operate in a multi-vendor environment where "foreign" networks and computing systems are supported.

System Description—Consists of 20 characters describing a node (system) on a PIN.

System Title—Consists of one or two alphanumeric characters that uniquely identifies a node (system) on a PIN. At least one of the characters must be an alpha character (nonblank, nonnumeric).

Index

Index

FAX Transmittal **FAX No.: (602) 313-4842**

TO: Maria Nelson **Total pages: 56**
(including this page)

Reader Comments

Title of Document: **Network Gateway Implementation and Operation**

Document Number: **NG09-510** Issue Date: **12/96**

Comments: _____

_____

_____

_____

_____

_____

Recommendations: _____

_____

_____

_____

_____

_____

FROM:

Name: _____ **Date:** _____

Title: _____

Company: _____

Address: _____

City: _____ **State:** _____ **ZIP:** _____

Telephone: _____ **FAX:** _____

You may also call 800-822-7673 (available in the 48 contiguous states except Arizona; in Arizona dial 602-313-5558, or write to:

Honeywell Inc.
Industrial Automation and Control
Automation College
2820 West Kelton Lane
Phoenix, AZ 85023-3028

Honeywell

Industrial Automation and Control

Automation College

2820 W. Kelton Lane

Phoenix, AZ 85023-3028

Helping You Control Your World