Honeywell

Interpret Redundant Node Behavior

L61529
8/99

TotalPlant

Notices and Trademarks

This module supports **TotalPlant** Solution (TPS) system network.

TPS is the evolution of TDC 3000^{X}.

Honeywell Inc.
Industrial Automation and Control
Automation College
2820 West Kelton Lane
Phoenix, AZ 85053-3028
1-800 852-3211

Table of Contents

Module Objective 5

Theory of Redundancy Operation 6

How Database is Synchronized 6

Redundancy Relationships 6

HG/PLCG Backup 7

HG/PLCG Failover 7

NIM Redundancy 10

Lab Exercise 13

Part 1 13

Part 2 13

Appendix B 15

HG Failure Scenarios 15

HG Failover Scenarios 17

Reasons for HG Failure 17

Case 1—Primary and Secondary Communicating OK 19

Case 2—Primary and Secondary Not Communicating on LCN 20

Case 3—Primary Alone in Ring 21

Case 4—Secondary Alone In Ring 22

Case 5—Secondary “Hung Up” or LCN Transmitter Failure 23

Case 6—Primary Cannot Communicate On Hiway 24

Case 7—Secondary Cannot Communicate On Hiway 25

Figures

Figure 1 PLCG Redundancy 8
Figure 2 HG Redundancy 9
Figure 3 AM Redundancy—Five-Slot Module 11
Figure 4 AM Redundancy—Dual Node Module 12
Figure 5 Primary and Secondary HG Communicating OK 19
Figure 6 Primary and Secondary Not Communicating On LCN 20
Figure 7 Primary Alone in Ring 21
Figure 8 Secondary Alone In Ring 22
Figure 9 Secondary “Hung Up” or LCN Transmitter Failure 23
Figure 10 Primary Cannot Communicate on Hiway 24
Figure 11 Secondary Cannot Communicate On Hiway 25

Module Objective

In this module, you will learn to interpret redundant behavior principles that will enable you to maximize system security.

Overview of Redundancy Operation

While there is no common redundancy logic for the different redundant node types, all the redundancy routines have a common approach. The approach depends on a separate communication path or "backdoor link" so that the primary and secondary modules can determine status and ensure that one and only one primary is operating at any given point in time, even during a loss of Local Control Network (LCN) communications. This "backdoor link" is the Data Hiway for the Hiway Gateways (HGs), the Universal Control Network for the Network Interface Modules (NIMs), and a special private path link for the Application Modules (AMs) and Programmable Logic Controller Gateways (PLCGs).

The LCN redundancy approach can be summarized as follows:

- The AM, PLCG, NIM, and HG nodes are redundant.
- The US/GUS depends on separate multiple members for redundancy.
- The HM has redundant disks but is not itself redundant.
- The CG is not redundant but multiple CGs can be connected to the same CM providing a level of independent data communications

Theory of Redundancy Operation

How Database is Synchronized

In most cases, changes to the primary node's database are transferred by the primary to the secondary upon their occurrence or periodically (once a second for HGs and Nims; twice a second for AMs). For example, if alarm disable/enable is changed from the US, the change that is made in the primary's database is sent to the secondary by the primary.

An exception to the above is how redundant nodes are loaded from the Data Entity Builder. The secondary node is loaded first, then the primary. This order ensures that invalid entries will crash the secondary and not the primary.

Redundancy Relationships

In an online system, the node's redundancy task is periodically communicating (for example, every second) back and forth between the primary and secondary, keeping the database synchronized over the LCN (or in the case of the AM over the private path). If the primary does not receive a response from the secondary that it "got the data" within a "long" time period (such as 60 seconds for an HG or NIM), it will fail the secondary.

If the secondary does not receive a message or answer from the primary, the failover time is much shorter. The secondary times out in a "short" amount of time (for example, 1.7 seconds for an HG or NIM), requests a retry(s) from the primary and times out again (for example, 0.8 second for an HG or NIM for a total of 2.5 seconds). Whether the primary or secondary fails depends on their view of the network and if communications over the "backdoor" link are successful.

While the primary is sending (or responding to) messages and is able to communicate on the LCN, it is also sending a status over the "backdoor" link indicating that the primary is "Alive and well on the LCN." If the secondary did not get an expected message over the LCN (or over the backdoor link for the AM), it checks for confirmation from the primary. If the primary is still alive and on the LCN, the secondary assumes that it is at fault and fails itself.

Let's change the scenario slightly. If the secondary does not hear from the primary over the backdoor link that the primary is alive and well on the LCN, the secondary takes over. The secondary does this by telling the primary over the backdoor link to fail, and sending a stun over the LCN.

HG/PLCG Backup

PLCG and HG redundancy are illustrated in Figures 1 and 2.

HG/PLCG Failover

Switching from an active HG/PLCG to the backup is accomplished with as little disruption to control and data acquisition as is possible. These two factors are very important in failover processing.

- Timeout handling
- Time to restore communication of the Data Hiway

It takes the backup 1 second to detect a failure in the active HG/PLCG. When it does detect a failure, it attempts to directly communicate with the active HG/PLCG. If this communication isn't re-established within 2 seconds, the backup requests the error-handling subsystem to determine whether to replace the active HG/PLCG. While waiting for this replacement, the backup proceeds with the following two functions.

1. Hiway-security checking is started by the backup and the scanning of the points with the 50 most critical (emergency priority) alarms begins.

2. The timeout gates in the boxes are updated so that control shedding doesn't occur.

When the system error handler determines that the formerly active HG/PLCG has failed, failover processing continues. The total time to complete the failover is about 5 seconds.

As failover processing continues, the following takes place.

3. The backup (secondary) becomes active (primary).

4. All functions that receive event messages are notified that failover has occurred and the distribution of the highest priority alarms begins.

5. Requests for data from the hiway are processed according to these priorities:

    - Control-function requests
    - Operator-initiated requests
    - Display updates

6. Alarms other than the 50 critical alarms are processed.

7. Remaining requests for data from the hiway are processed.

8. All remaining functions resume, including checkpointing of HG/PLCG data, history

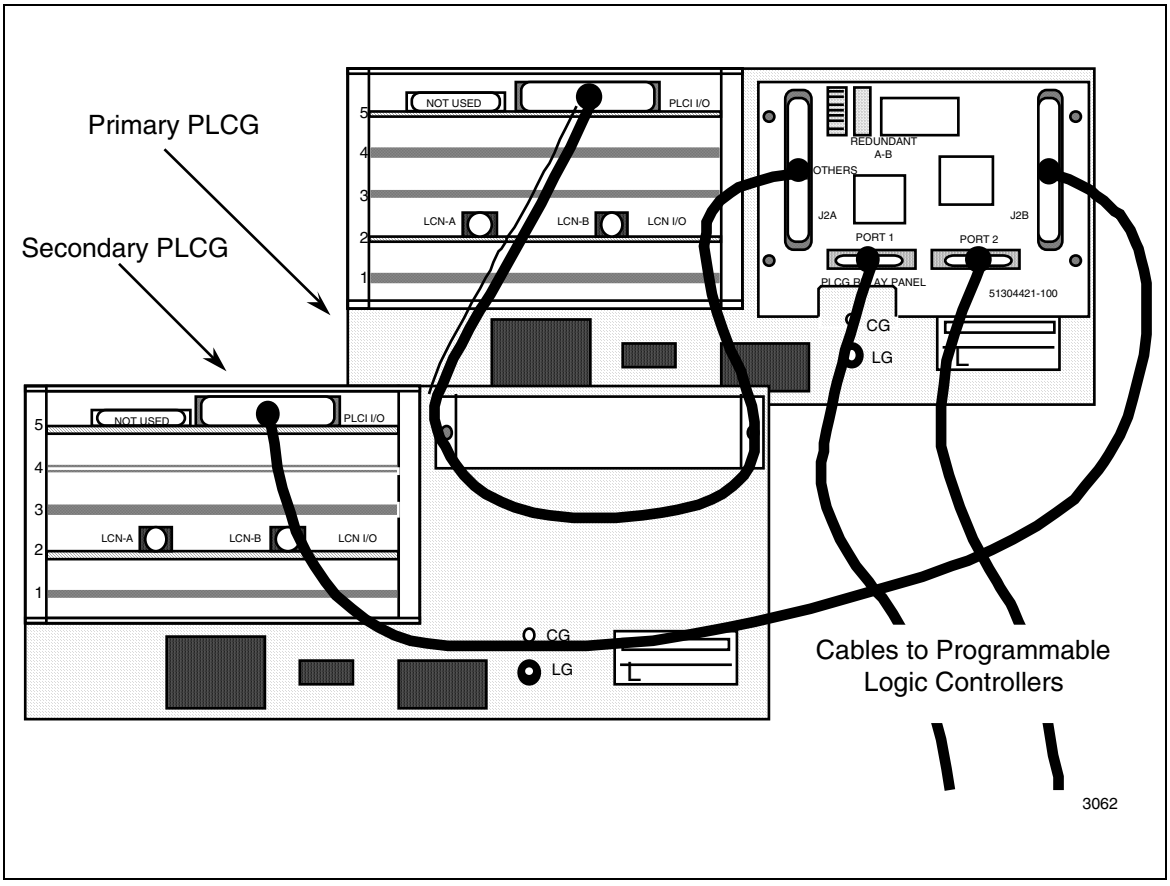

Figure 1 PLCG Redundancy

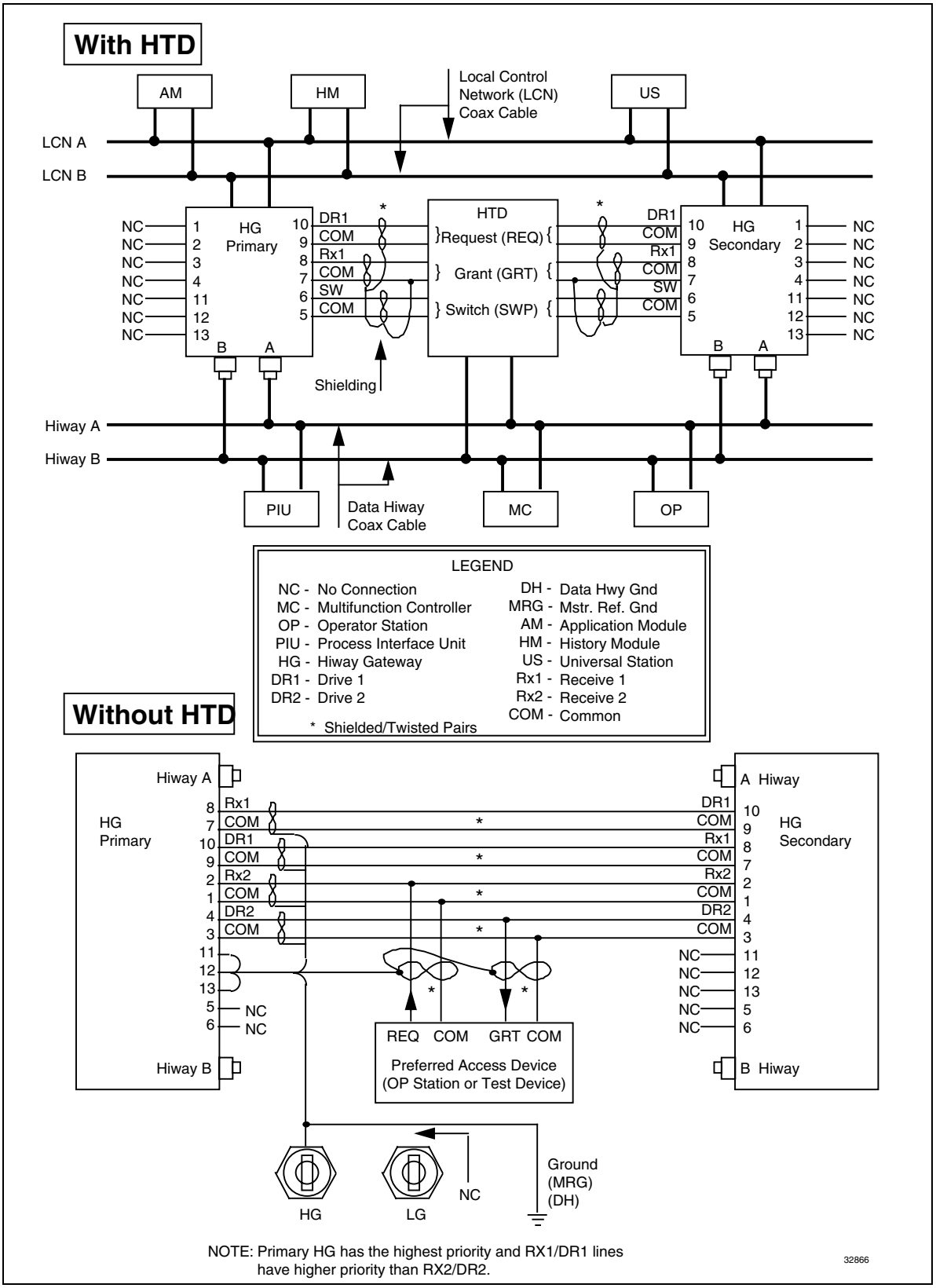

Figure 2 HG Redundancy

AM Redundancy

AM redundancy (Figures 3 and 4) is a purchased option for AMs with HPMU 68020 or 68040 microprocessors. Figure 3 shows the five-slot chassis configuration. Figure 4 shows dual node chassis configuration (redundant AMs in the lower nodes of adjacent modules).

AM redundancy includes hardware and software that allow a secondary AM to back up the operation of the primary AM. To do this, all of the application data in the primary AM is transferred to the secondary AM, where an exact copy of the data is maintained if the primary AM should become inoperative.

When a hardware fault is detected in the primary AM, the secondary AM takes over within approximately 5 seconds. No external accesses to the AM are lost during the transfer (Failover).

NIM Redundancy

NIMs are intended to operate as redundant pairs. To do this, all of the data in the primary NIM is transferred to the secondary NIM, where an exact copy of the data is maintained if the primary NIM should become inoperative.

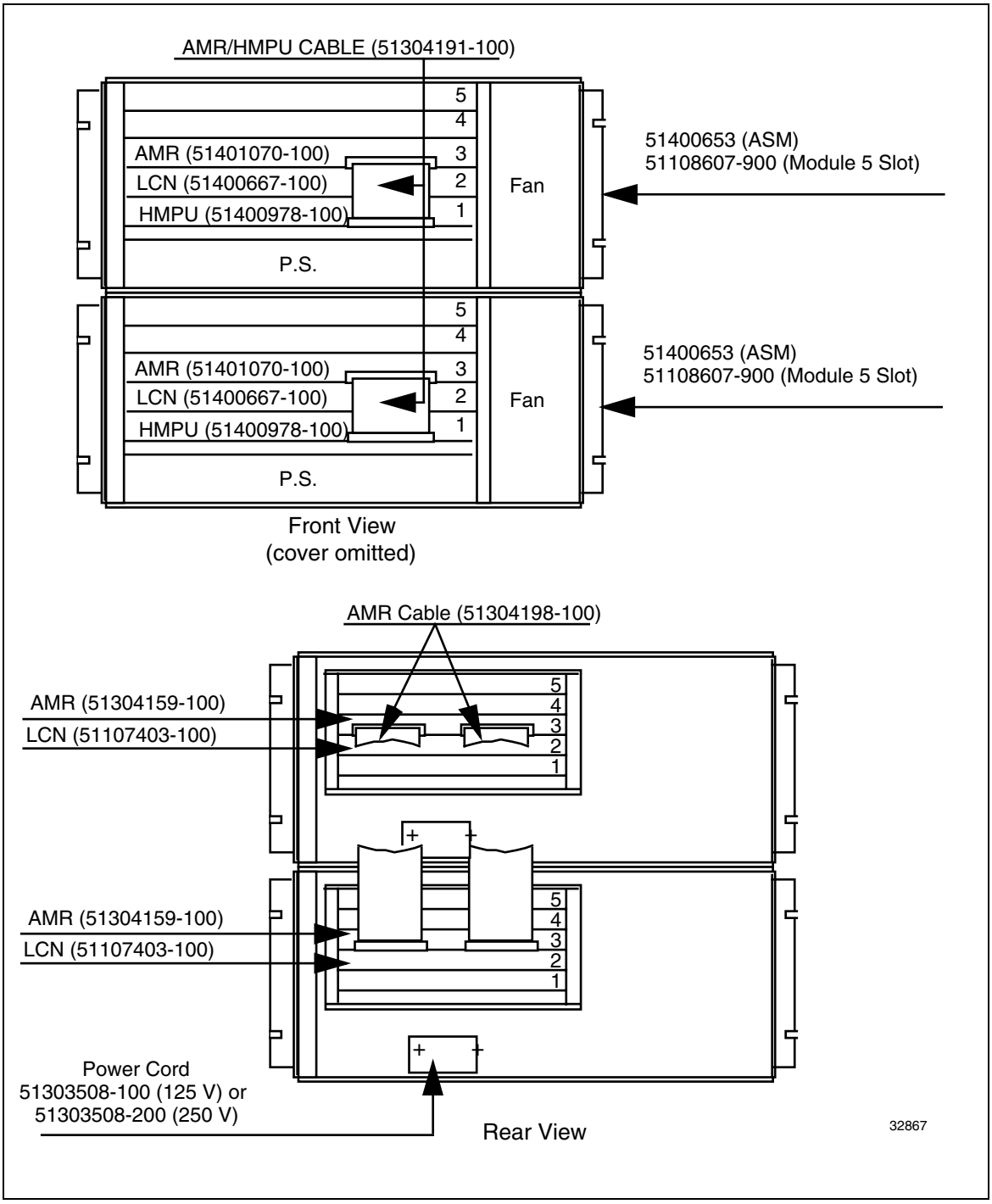

Figure 3 AM Redundancy—Five-Slot Module

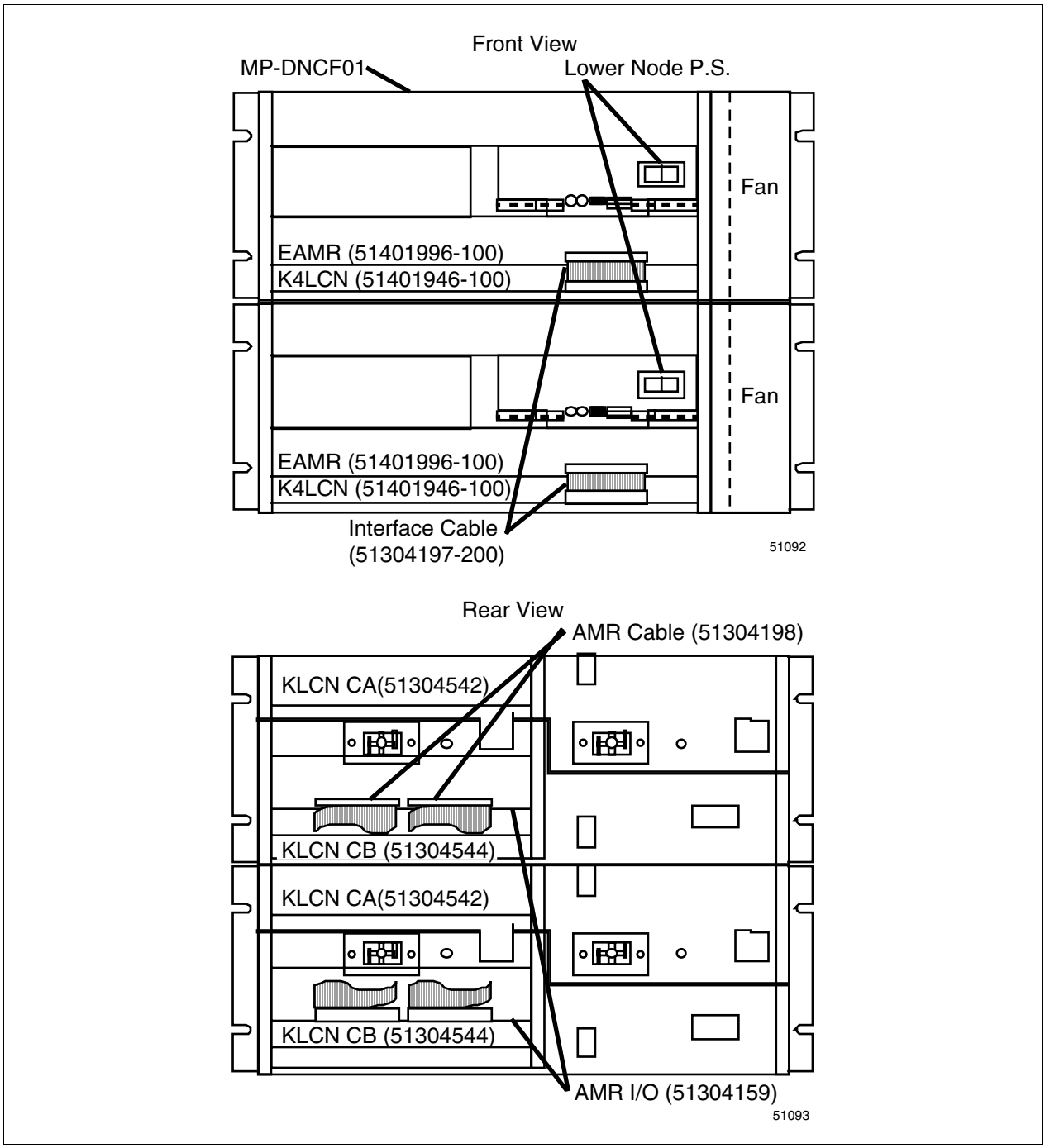

Figure 4 AM Redundancy—Dual Node Module

LAB TIME ≈30 Minutes

Use your US

Take with you:

- This course module

Lab Exercise

This lab consists of two parts. The first part is hardware identification, the second part will have you cause a failover from the primary device to the secondary device.

Your course manager will provide additional details on the lab instructions.

Part 1

Identify the redundant communication path for the device your course manager has assigned to you.

_____

Part 2

1. After your lab colleagues have completed Part 1 of the lab exercise, proceed to cause a redundancy failover.
2. Restart the previously failed node.
3. Monitor and identify LEDs and Status display that indicate the node's status as a primary or secondary.

   Call up the Event History Journals and Detailed Module Errors for both the primary and secondary nodes.

End of Lab Exercise

Appendix B

HG Failure Scenarios

HG Failover Scenarios

Reasons for HG Failure

Primary Failure

The reasons for HG primary failure are

- HG hardware failure (such as DHI, LCNI, or EMPU),
- •HG software failure (such as range error or illogical condition),
- Secondary does not hear from the primary within 2.5 seconds over the LCN.
- Primary cannot complete a Local Data Access call within 60 seconds.
- Primary has hiway failure for more than 12 seconds and secondary does not have hiway failure.

Secondary Failure

The reasons for HG secondary failure are:

- HG hardware failure (such as DHI, LCNI, or EMPU),
- •HG software failure (such as range error or illogical condition),
- Primary does not receive at least one LCN acknowledgement from the secondary within 60 seconds,
- Secondary does not hear from primary over the LCN in 2.5 seconds, but can hear from the primary over the hiway.

ATTENTION

In the following diagrams, nodes that are highlighted by “shading” are the nodes that will fail.

Case 1—Primary and Secondary Communicating OK

Problem: None

Scenario:

1. Primary transmits an "I am alive and on the LCN" at least once a second over the Data Hiway (because primary is On Net).
2. Primary transmits redundancy message at least once a second over LCN (because primary is On Net).
3. Secondary transmits an acknowledgement to primary redundancy message if there is redundant data to process or every 20 messages received. It also resets the "I'm alive and on the LCN" flag.

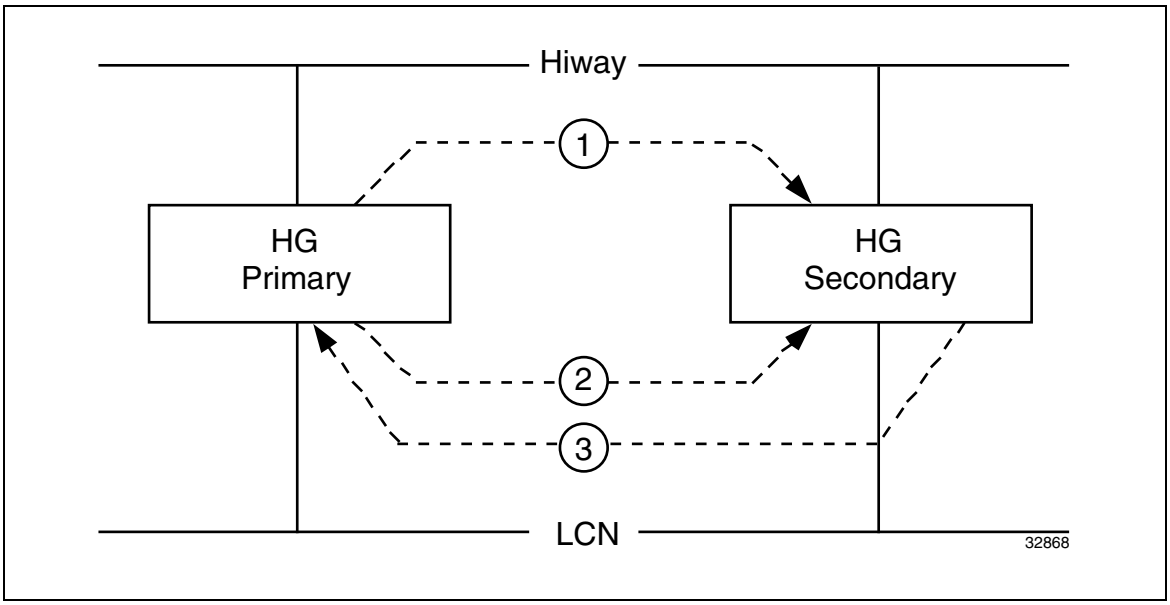

Figure 5 Primary and Secondary HG Communicating OK

Case 2—Primary and Secondary Not Communicating on LCN

Problem: The primary and secondary are both able to transmit data, but cannot communicate with each other. This may be caused by a physical break between them or reflection problems.

Scenario:

1. Primary transmits an "I am alive and on the LCN" at least once a second over the Data Hiway (because primary is On Net).
2. Primary transmits redundancy message at least once a second over LCN (because primary is On Net).
3. Secondary does not hear from the primary for 1.7 seconds and transmits three requests to the primary to resend the redundancy message.
4. After 0.8 seconds, secondary determines (from the primary's "I am alive" message) that the primary can still communicate on the LCN. Secondary writes to primary across the hiway to detect if primary is still alive.
5. Secondary fails itself.

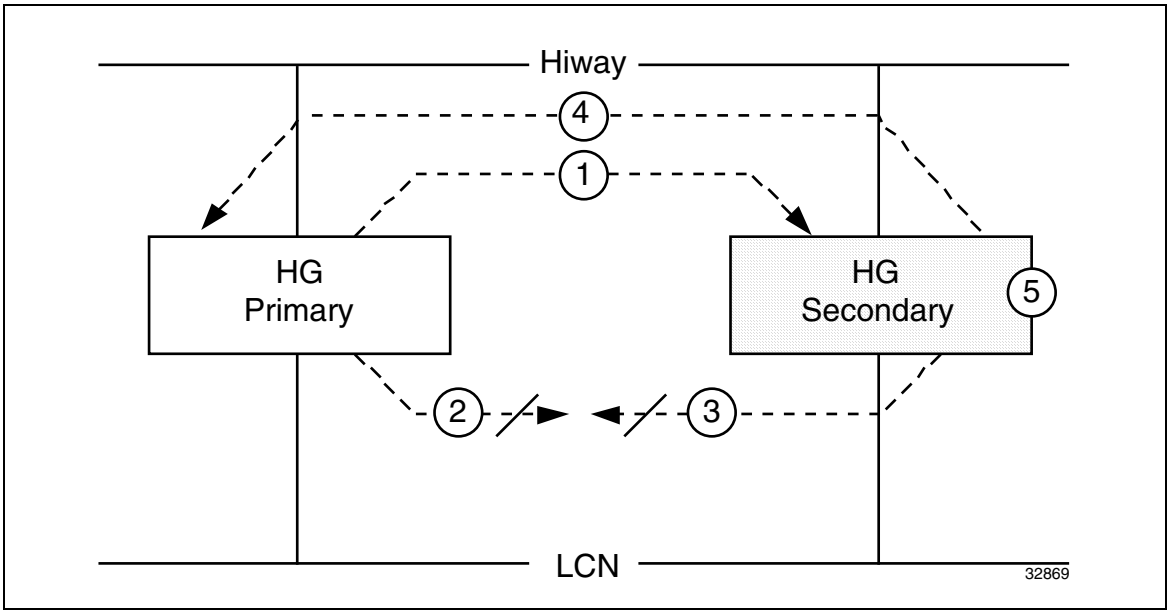

Figure 6 Primary and Secondary Not Communicating On LCN

Case 3—Primary Alone in Ring

Problem: Primary cannot get on the LCN ring, perhaps because of a bad LCNI card, someone “stomping” on its token, or reflections on the cable.

Scenario:

1. The primary does not send the “I am alive” message because it is alone in ring.
2. The primary does not transmit the redundancy message once per second over the LCN because it is along in ring.
3. Secondary does not hear from the primary for 1.7 seconds and transmits three requests to the primary to resend the redundancy message.
4. After 0.8 seconds, secondary determines that the primary cannot communicate on the LCN, because there is no “I am alive” message. Since the secondary can still communicate across the LCN, it sends a Kill Command over the hiway to the primary.
5. Secondary tries to stun the primary across the LCN.
6. Primary crashes upon receipt of Kill Command over the Hiway.

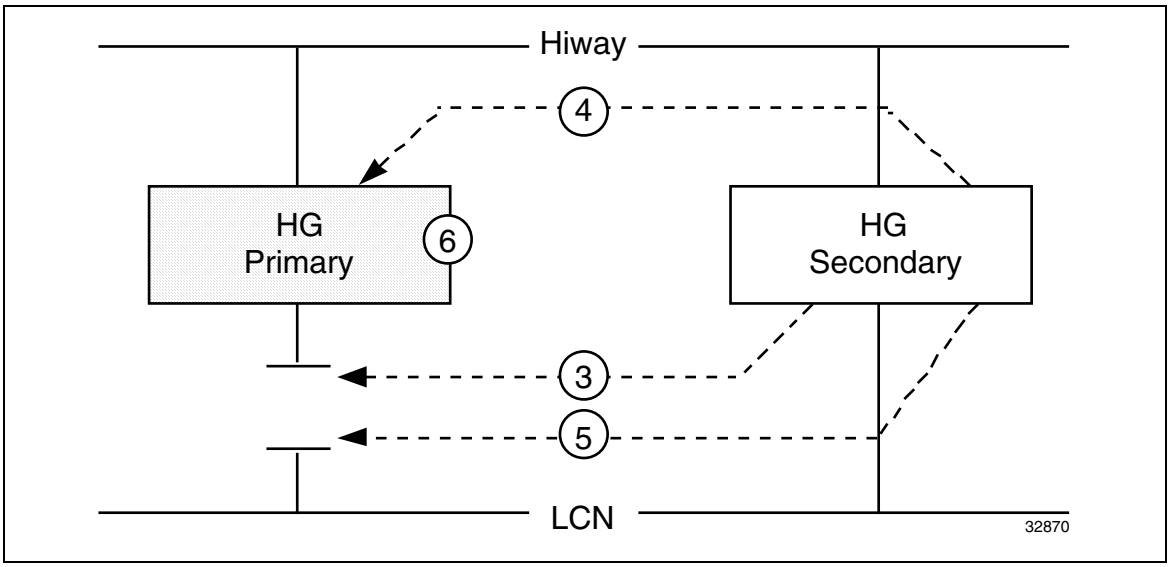

Figure 7 Primary Alone in Ring

Case 4—Secondary Alone In Ring

Problem: Secondary cannot get on the LCN ring perhaps because of a bad LCNI card, someone “stomping” on its token, or reflections on the cable.

Scenario:

1. Primary transmits an “I am alive and on the LCN” at least once a second over the Data Hiway (because primary is On Net).
2. Primary transmits redundancy message at least once a second over LCN (because primary is On Net).
3. The secondary does not acknowledge the redundancy message because it is not received.
4. Secondary does not hear from the primary for 1.7 seconds and transmits three requests to the primary to resend the redundancy message.
5. After 0.8 seconds, secondary determines that the primary can still communicate on the LCN via the "I am alive" message sent over the Hiway. Secondary writes to primary across the hiway to detect if primary is still alive.
6. Secondary fails itself.

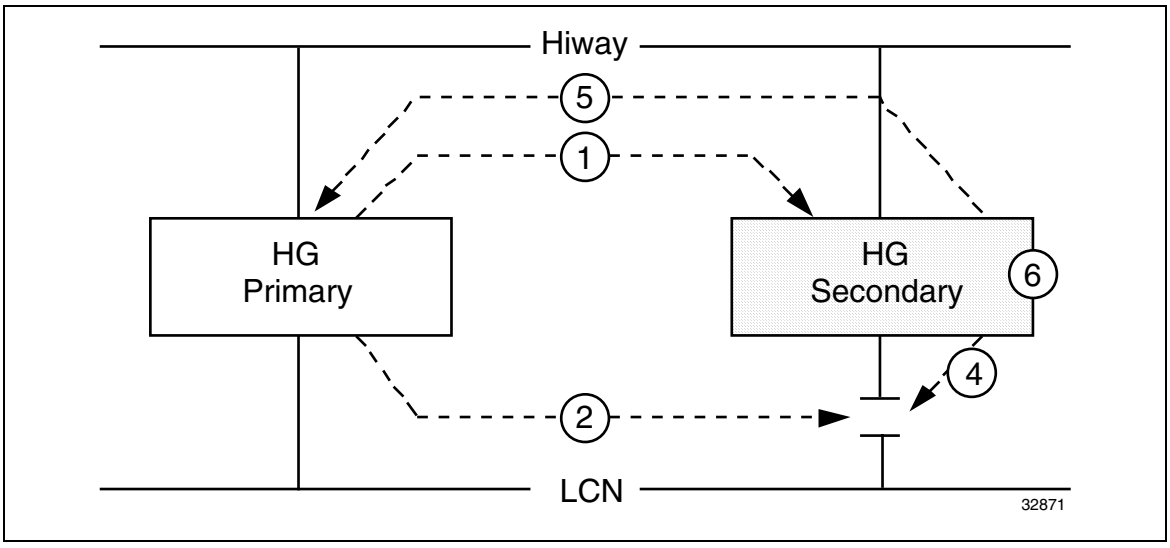

Figure 8 Secondary Alone In Ring

Case 5—Secondary "Hung Up" or LCN Transmitter Failure

Problem: Secondary either has a software problem that prevents it from responding to the primary or the LCNI has a problem transmitting, but not receiving messages.

Scenario:

1. Primary transmits an "I am alive and on the LCN" message at least once a second over the Data Hiway (because primary is On Net).
2. Primary transmits redundancy message at least once a second over LCN (because primary is On Net).
3. Secondary is either in a loop or its transmitter is broken and it cannot successfully transmit an acknowledgement to the primary upon receipt of the redundancy message.
4. Primary does not receive at least one acknowledgement from the secondary within 60 seconds and sends a Kill Command over the Data Hiway.
5. Primary stuns the secondary over the LCN.

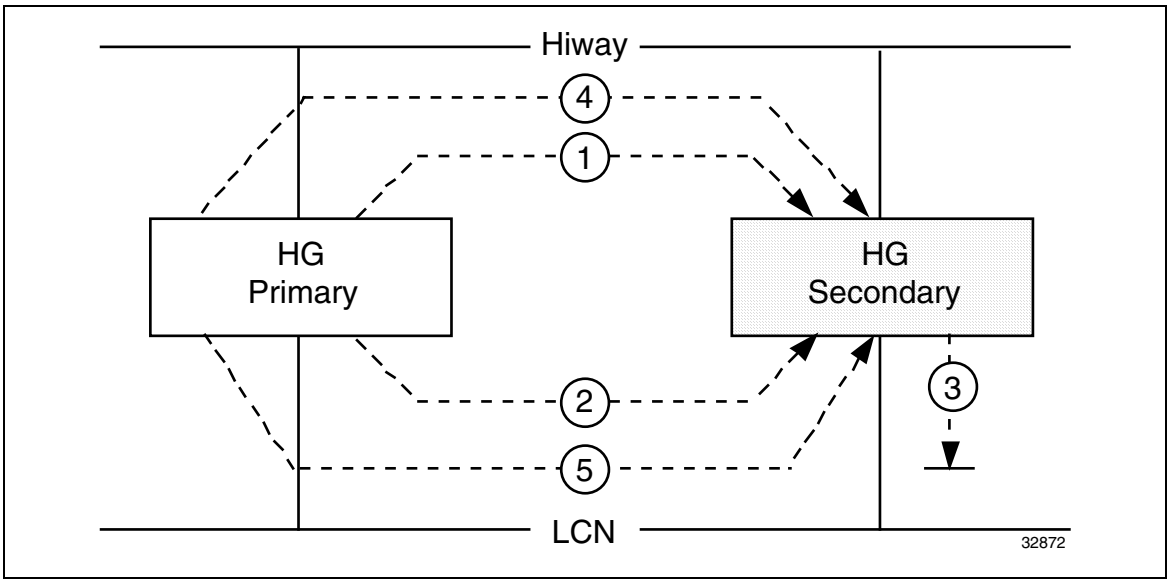

Figure 9 Secondary "Hung Up" or LCN Transmitter Failure

Case 6—Primary Cannot Communicate On Hiway

Problem: Grant line could be broken, both cables could be removed from primary or reflections on cables may not allow communications to some of the boxes.

Scenario:

1. Primary attempts to transmit an "I am alive and on the LCN" at least once a second over the Data Hiway (because primary is On Net). Message is not received.
2. Primary transmits redundancy message at least once a second over LCN (because primary is On Net).
3. Secondary transmits an acknowledgement to primary redundancy message if there is redundant data to process or every 20 messages received. It also resets the "I am alive and on the LCN" flag.
4. Primary detects that it cannot communicate on the hiway for 12 seconds and informs secondary, using the redundancy message.
5. Secondary determines that it can communicate over the hiway and informs primary of this over the LCN.
6. Primary fails itself.

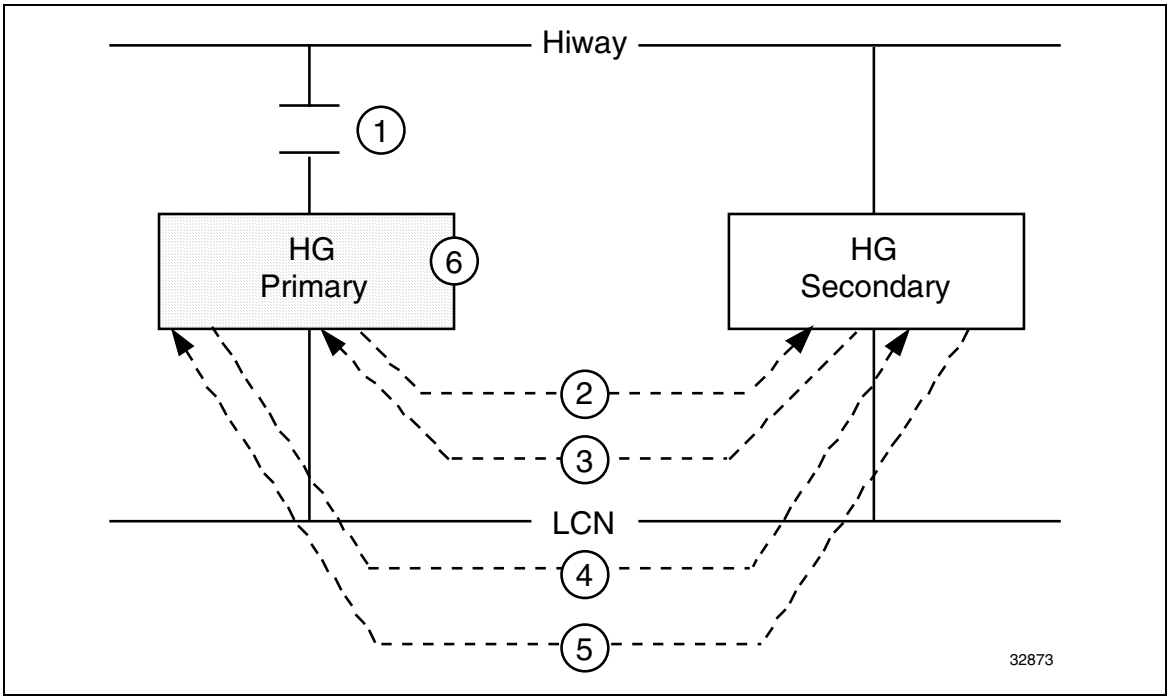

Figure 10 Primary Cannot Communicate on Hiway

Case 7—Secondary Cannot Communicate On Hiway

Problem: Both cables have possibly been removed from secondary.

Scenario:

1. Primary transmits an “I am alive and on the LCN” at least once a second over the Data Hiway (because primary is On Net).
2. Primary transmits redundancy message at least once a second over LCN (because primary is On Net).
3. Secondary transmits an acknowledgement to primary redundancy message if there is redundant data to process, or every 20 messages received. It also resets the “I am alive and on the LCN” flag.
4. Secondary stays in BACKUP mode and keeps trying to receive hiway messages.
5. The primary annunciates a box failure against the secondary because it does not hear from it on the hiway.
6. Neither node fails, because the redundancy message is still transmitted and received over the LCN. Their databases are synchronized.

Figure 11

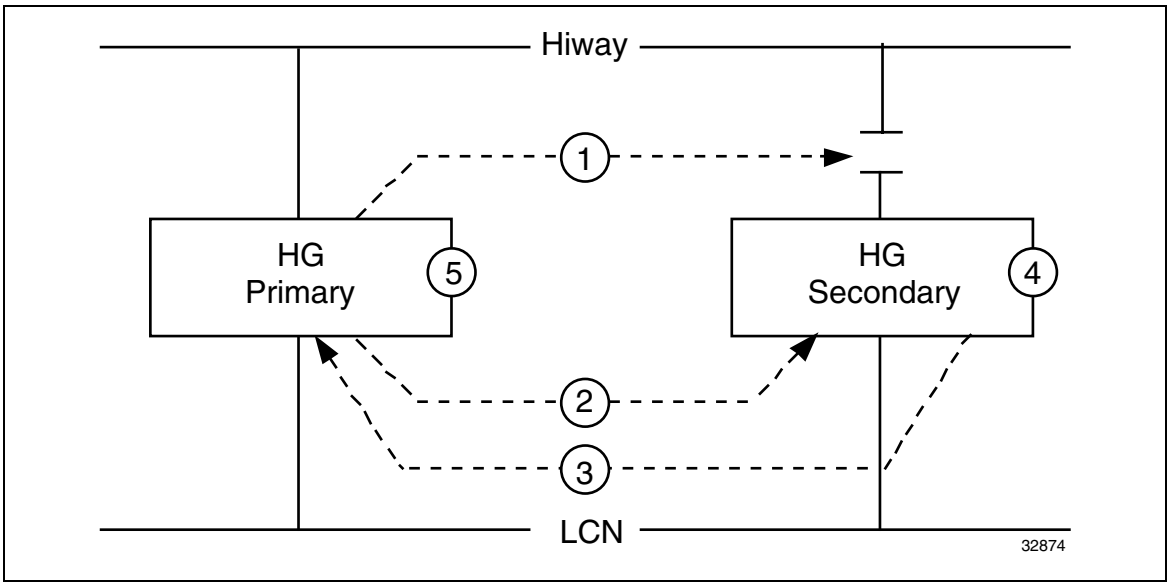

Figure 11 Secondary Cannot Communicate On Hiway

Honeywell

Industrial Automation and Control
Honeywell Inc.
2820 West Kelton Lane
Phoenix, AZ 85053-3028