



Controller Redundancy

This document explains the behavior of controller redundancy in a DeltaV system.



© Emerson Process Management 1996—2007 All rights reserved.

DeltaV, the DeltaV design, SureService, the SureService design, SureNet, the SureNet design, and PlantWeb are marks of one of the Emerson Process Management group of companies. All other marks are property of their respective owners. The contents of this publication are presented for informational purposes only, and while every effort has been made to ensure their accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. All sales are governed by our terms and conditions, which are available on request. We reserve the right to modify or improve the design or specification of such products at any time without notice.





Contents

Introduction	4
Switchovers	6
Conditions that cause switchovers	6
What happens during a switchover?	7
Data Transfer from Active to Standby	8
Upgrading Redundant Controllers	8



Figures

Figure 1. Redundant controller pair	4
Figure 2. Simplex controller, illustrating redundancy link	5

Introduction

The DeltaV system includes redundant controllers. A redundant controller comprises a pair of standard controllers (version M3 or later) on separate 2-wide power/controller carriers that are connected together. Each controller requires its own power supply mounted on its carrier. One of the controllers in the pair is the active controller and the other controller is the standby controller. (see Fig. 1). There is no physical difference between the active and standby, nor is there a preferred position for the active controller. The controller that boots first becomes the active controller.



Figure 1. Redundant controller pair

The redundant controllers communicate with each other via a dedicated high-speed (1Mbaud) serial bus (see Fig. 2). This bus is automatically formed when the two 2-wide carriers are joined together.



Figure 2. Simplex controller, illustrating redundancy link

The standby controller contains the same configuration as the active controller and tracks the operation of the active controller. When an active controller fails, the standby controller takes over, providing uninterrupted control operation without initialization or user intervention. When the previously active controller recovers to a healthy state or is replaced, the two controllers automatically become a redundant pair again.

Even though each controller in a redundant pair has its own network address, a redundant controller counts as a single node on the DeltaV control network in terms of network capacity. The commissioning and decommissioning function in the DeltaV Explorer affects both controllers in the pair.

You can connect a standby controller to an existing simplex controller to introduce redundant control without interrupting your process. The system automatically commissions a standby controller when you install it. It is not necessary to remove or decommission the active controller. The active controller continues to operate without interruption. The system automatically assigns the standby with an address and downloads the standby controller with the latest download and with any online changes made to the active controller. **This process must be implemented according to the procedure outlined in DeltaV Books Online.**



Switchovers

Conditions that cause switchovers

A switchover from the active to the standby controller can occur for the following reasons:

- **Hardware failure**

A **hardware fault** analysis of the controller circuitry ensures that the failure of a component is detected.

- **Communications failure between the active controller and the I/O sub-system**

Both controllers monitor their ability to communicate with the I/O. If the active controller does not talk to the I/O for more than 1 second, a switchover will occur if the standby has the ability to communicate with the I/O.

- **Communications failure of both the primary and secondary network connections in the active controller**

Every 10 seconds, both controllers check their ability to communicate with other nodes on the control network. If the active controller detects a loss of communications, a switchover will occur if the standby has the ability to communicate on at least one (primary or secondary) of its control networks.

- **Removal of the controller from the carrier**

If the active controller is physically removed from the carrier, a switchover will occur.

- **Manual switchover request**

A user with Control privilege can initiate a manual switchover from DeltaV Diagnostics. Three conditions must be satisfied before a manual switchover can be done.

1. The standby controller is physically present (indicated by diagnostic parameter **Pexist**)
2. The standby controller has received a download and is ready to take over (indicated by diagnostic parameter **Pavail**)
3. Redundancy has been enabled for the pair (indicated by diagnostic parameter **RedEnb**). In order for redundancy to be enabled, the active controller must have received a download.

The **Status** parameter provides additional details about the redundancy sub-system.

- **Power failure of the active controller**

A switchover will occur so long as the standby is available.

- **Memory failures**

To detect memory-related problems, the controller executes CRC (cyclic redundancy check) tests on the flash ROM and a RAM test. The ROM CRC test runs continually in the background, as a low priority task. RAM tests are executed every time the controller is rebooted. If the active controller detects a failure in either the RAM or ROM test, a reset will occur, resulting in a switchover to the standby controller.

- **Runaway software**

The controller has protection mechanisms for detecting “runaway software,” for example “infinite loops.” These mechanisms include a watchdog timer and processor exception handling.



What happens during a switchover?

When a switchover occurs, a system event is generated and a message is sent to the operator stations. The system stores a record of each switchover and the reason it occurred in the Event Chronicle. Further information can be obtained by analyzing the log file on the controller that failed. If DeltaV Diagnostics is running, the switchover is also logged in the Integrity History window. The switchover generates no disturbances to the field output signals.

After the switchover has occurred, the new active controller prepares to begin executing the modules. This phase can take up to ½ second, depending on the size of the configuration. During this phase, all outputs remain at the last value. The new active controller then begins executing the modules from the exact point where the old active controller left off.

All clients (graphic displays, etc.) that need controller parameters must re-register for those parameters. The time needed for this activity can be several seconds. This is dependent on the number of clients and the number of parameters requested.

© Emerson Process Management 1996—2007 All rights reserved.

DeltaV, the DeltaV design, SureService, the SureService design, SureNet, the SureNet design, and PlantWeb are marks of one of the Emerson Process Management group of companies. All other marks are property of their respective owners. The contents of this publication are presented for informational purposes only, and while every effort has been made to ensure their accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. All sales are governed by our terms and conditions, which are available on request. We reserve the right to modify or improve the design or specification of such products at any time without notice.





Data Transfer from Active to Standby

The redundancy link ensures that the standby is updated efficiently and quickly, to provide a bumpless switchover.

When a configuration is downloaded, the standby receives an “initial update” that transfers all the current parameters. Thereafter, the redundancy link goes into “change” reporting mode. In this mode the standby controller is updated with changes only that have taken place in the active controller.

The following events happen in the order below during the “change” update mode:

- Module executes.
- Module packages data that has changed during execution. This includes state information that allows the standby to begin execution from where the active left off.
- Module packages parameters of other modules that it changed during its execution.
- Redundancy data package is sent to the standby.

In general, system parameters (module/function block) are transferred when they change. However, some system parameters (MSTATUS, ABNORMAL_ACT, etc.) are not sent to the standby because they will be updated when the module executes. All user-created module parameters, at the module level and at the composite level, are transferred if they change. If outputs are changed during module execution, then the changes are sent after every module execution. Modules that are driving outputs will always have some redundancy data to be sent after every scan, even if the associated function blocks do not.

For Function block modules, state information about each function block is transmitted to the standby. This information allows execution to resume after a switchover, without bumping the output of the block.

For SFC’s all state-related information (active step(s), step timers(s), status of each action) is communicated to the standby on each scan of the module. State information about phases is also included in the redundancy packet. This information ensures that SFC’s resume execution exactly where they left off in the active. Information about the switchover is available to phases in the new active controller. This may be used to set the phase failure index, as desired by the user.

For unit modules the redundancy data includes information about all active phases. When a phase is loaded, all the initial values for the phase are sent to the standby. This is followed by updates of changed data on subsequent executions of the unit module. When a phase is unloaded the standby is informed that data will no longer be received for that phase on that unit module.

Upgrading Redundant Controllers

If the redundant controllers require an upgrade, the controllers contain flash ROM that allows an update of the firmware while the process is running. Simply upgrade the standby controller, then perform a manual switchover from DeltaV Diagnostics. Then upgrade the controller you recently switched to standby.