12. Remote System Upgrades with Stratix III Devices

SIII51012-1.5

This chapter describes the functionality and implementation of the dedicated remote system upgrade circuitry. It also defines several concepts related to remote system upgrade, including factory configuration, application configuration, remote update mode, and user watchdog timer. Additionally, this chapter provides design guidelines for implementing remote system upgrades with the supported configuration schemes.

System designers sometimes face challenges such as shortened design cycles, evolving standards, and system deployments in remote locations. Stratix® III devices help overcome these challenges with their inherent re-programmability and dedicated circuitry to perform remote system upgrades. Remote system upgrades help deliver feature enhancements and bug fixes without costly recalls, reduce time-to-market, and extend product life.

Stratix III devices feature dedicated remote system upgrade circuitry. Soft logic (either the Nios® II embedded processor or user logic) implemented in a Stratix III device can download a new configuration image from a remote location, store it in configuration memory, and direct the dedicated remote system upgrade circuitry to initiate a reconfiguration cycle. The dedicated circuitry performs error detection during and after the configuration process, recovers from any error condition by reverting back to a safe configuration image, and provides error status information. This dedicated remote system upgrade circuitry is unique to the Stratix series and helps to avoid system downtime.

Remote system upgrade is supported in fast active serial (FAS) Stratix III configuration schemes. You can also implement remote system upgrade in conjunction with advanced Stratix III features such as real-time decompression of configuration data and design security using the advanced encryption standard (AES) for secure and efficient field upgrades.

Functional Description

The dedicated remote system upgrade circuitry in Stratix III devices manage remote configuration and provides error detection, recovery, and status information. User logic or a Nios II processor implemented in the Stratix III device logic array provides access to the remote configuration data source and an interface to the system's configuration memory.

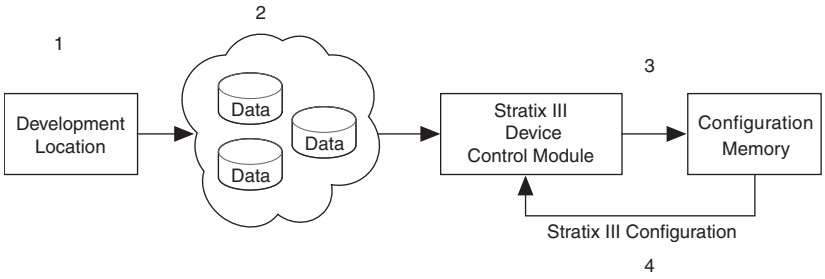
Stratix III devices have remote system upgrade processes that involves the following steps:

1. A Nios II processor (or user logic) implemented in the Stratix III device logic array receives new configuration data from a remote location. The connection to the remote source uses a communication protocol such as the transmission control protocol/Internet protocol (TCP/IP), peripheral component interconnect (PCI), user datagram protocol (UDP), universal asynchronous receiver/transmitter (UART), or a proprietary interface.
2. The Nios II processor (or user logic) stores this new configuration data in non-volatile configuration memory.

3. The Nios II processor (or user logic) initiates a reconfiguration cycle with the new or updated configuration data.
4. The dedicated remote system upgrade circuitry detects and recovers from any error(s) that might occur during or after the reconfiguration cycle, and provides error status information to the user design.

Figure 12–1 shows the steps required for performing remote configuration updates. (The numbers in the figure below coincide with the steps above.)

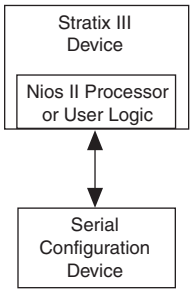
Figure 12–1. Functional Diagram of Stratix III Remote System Upgrade



Stratix III devices only support remote system upgrade in the single device Fast AS configuration scheme.

Figure 12–2 shows the block diagrams for implementing a remote system upgrade with the Stratix III Fast AS configuration scheme.

Figure 12–2. Remote System Upgrade Block Diagram for Stratix III Fast AS Configuration Scheme



You must set the mode select pins (`MSEL[2..0]`) to Fast AS mode to use the remote system upgrade in your system. Table 12–1 lists the `MSEL` pin settings for Stratix III devices in standard configuration mode and remote system upgrade mode. The following sections describe the remote update of remote system upgrade mode.

For more information about standard configuration schemes supported in Stratix III devices, refer to the *Configuring Stratix III Devices* chapter in volume 1 of the *Stratix III Device Handbook*.

Table 12–1. Stratix III Remote System Upgrade Modes

Configuration Scheme	MSEL[2..0]	Remote System Upgrade Mode
Fast AS (40 MHz) *(1)*	011	Standard
	011	Remote update

Note to Table 12–1:

(1) The EPCS16, EPCS64, and EPCS128 serial configuration devices support a DCLK up to 40 MHz. For more information, refer to the *Serial Configuration Devices (EPCS1, EPCS4, EPCS16, EPCS64, and EPCS128) Datasheet* chapter in volume 1 of the *Configuration Handbook*.

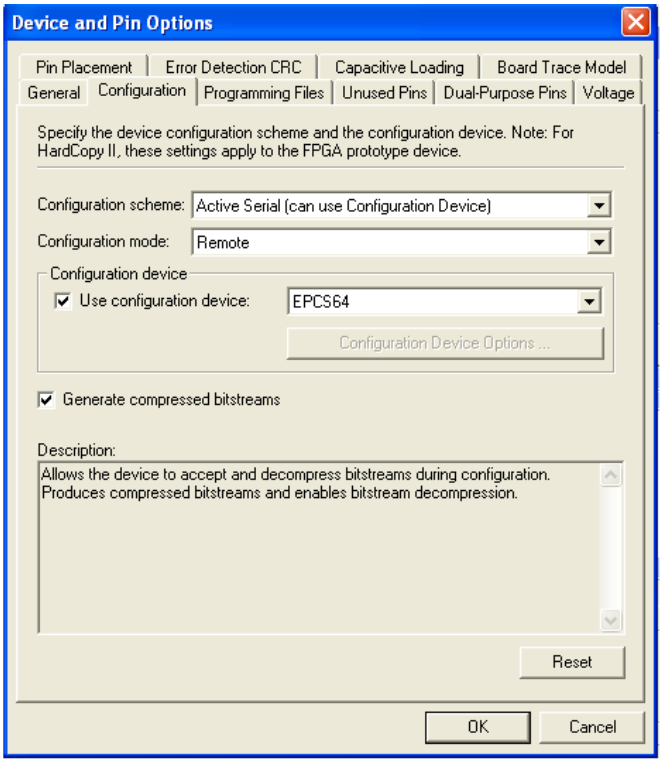
When using the Fast AS mode, you must select the **Remote Update** mode in the Quartus® II software and insert the ALTREMOTE_UPDATE megafunction to access the circuitry. Refer to "ALTREMOTE_UPDATE Megafunction" on page 12–13 for more information.

Enabling Remote Update

You can enable remote update for Stratix III devices in the Quartus II software before design compilation (in the Compiler Settings menu). To enable remote update in the project's compiler settings, perform the following steps in the Quartus II software:

1. On the Assignment menu, click **Device**. The **Settings** dialog box appears.
2. Click **Device and Pin Options**. The **Device and Pin Options** dialog box appears.
3. Click the **Configuration** tab.
4. From the Configuration scheme list, select **Active Serial** (can use **Configuration Device**) (Figure 12–3).
5. From the Configuration Mode list, select **Remote**. (Figure 12–3).
6. Click **OK**.
7. In the **Setting** dialog box, click **OK**.

Figure 12–3. Enabling Remote Update for Stratix III Devices in Compiler Settings



Configuration Image Types

When using a remote system upgrade, Stratix III device configuration bitstreams are classified as factory configuration images or application configuration images. An image, also referred to as a configuration, is a design loaded into the Stratix III device that performs certain user-defined functions.

Each Stratix III device in your system requires one factory configuration image or the addition of one or more application configuration images. The factory configuration image is a user-defined fall-back, or safe configuration, and is responsible for administering remote updates in conjunction with the dedicated circuitry. Application configuration images implement user-defined functionality in the target Stratix III device. You may include the default application configuration image functionality in the factory configuration image.

A remote system upgrade involves storing a new application configuration image or updating an existing one through the remote communication interface. After an application configuration image is stored or updated remotely, the user design in the Stratix III device initiates a reconfiguration cycle with the new image. Any errors during or after this cycle are detected by the dedicated remote system upgrade circuitry and cause the device to automatically revert to the factory configuration image. The factory configuration image then performs error processing and recovery. The factory configuration is written to the serial configuration device only once by the system manufacturer and should not be remotely updated. On the other hand, application configurations may be remotely updated in the system. Both images can initiate system reconfiguration.

Remote System Upgrade Mode

Remote system upgrade has one mode of operation: remote update mode. The remote update mode allows you to determine the functionality of your system upon power-up and offers different features.

In remote update mode, Stratix III devices load the factory configuration image upon power up. The user-defined factory configuration determines which application configuration is to be loaded and triggers a reconfiguration cycle. The factory configuration may also contain application logics.

When used with serial configuration devices, the remote update mode allows an application configuration to start at any flash sector boundary. This translates to a maximum of 128 pages in the EPCS64 device and 32 pages in the EPCS16 device, where the minimum size of each page is 512 KBits. Additionally, the remote update mode features a user watchdog timer that determines the validity of an application configuration.

Remote Update Mode

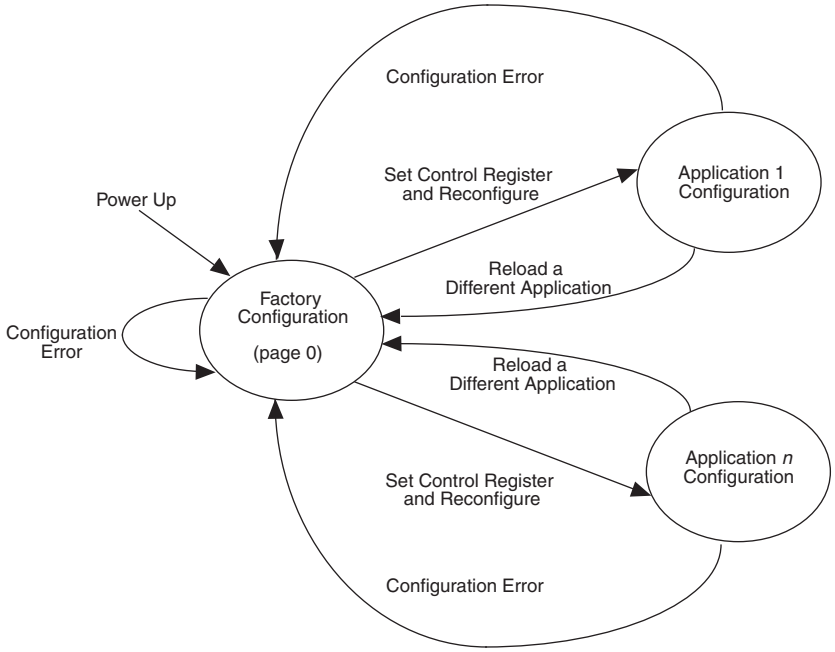
When a Stratix III device is first powered-up in remote update mode, it loads the factory configuration located at page zero (page registers `PGM[23:0] = 24'b0`). You should always store the factory configuration image for your system at page address zero. This corresponds to the start address location 0×000000 in the serial configuration device.

The factory configuration image is user-designed and contains soft logic to do the following:

- Process any errors based on status information from the dedicated remote system upgrade circuitry
- Communicate with the remote host and receive new application configurations and store this new configuration data in the local non-volatile memory device
- Determine which application configuration is to be loaded into the Stratix III device
- Enable or disable the user watchdog timer and load its time-out value (optional)
- Instruct the dedicated remote system upgrade circuitry to initiate a reconfiguration cycle

Figure 12–4 shows the transitions between the factory and application configurations in remote update mode.

Figure 12–4. Transitions Between Configurations in Remote Update Mode



After power up or a configuration error, the factory configuration logic is loaded automatically. The factory configuration also needs to specify whether to enable the user watchdog timer for the application configuration and if enabled, to include the timer setting information as well.

The user watchdog timer ensures that the application configuration is valid and functional. The timer must be continually reset within a specific amount of time during user mode operation of an application configuration. Only valid application configurations contain the logic to reset the timer in user mode. This timer reset logic should be part of a user-designed hardware and/or software health monitoring signal that indicates error-free system operation. If the timer is not reset in a specific amount of time, for example, the user application configuration detects a functional problem or if the system hangs, the dedicated circuitry updates the remote system upgrade status register, triggering the loading of the factory configuration.

The user watchdog timer is automatically disabled for factory configurations. For more information about the user watchdog timer, refer to "User Watchdog Timer" on page 12–11.

If there is an error while loading the application configuration, the cause of the reconfiguration is written by the dedicated circuitry to the remote system upgrade status register. Actions that cause the remote system upgrade status register to be written:

- nSTATUS driven low externally
- Internal CRC error
- User watchdog timer time out

- A configuration reset (logic array nCONFIG signal or external nCONFIG pin assertion to low)

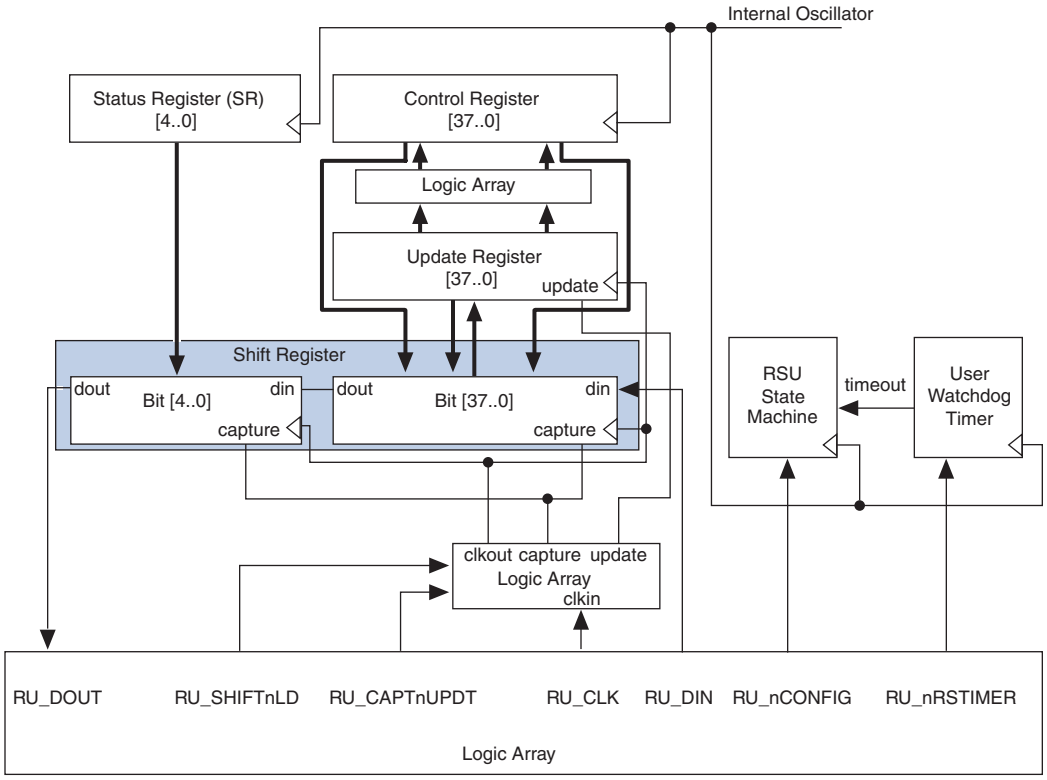
Stratix III devices automatically load the factory configuration located at page address zero. This user-designed factory configuration reads the remote system upgrade status register to determine the reason for the reconfiguration. The factory configuration then takes appropriate error recovery steps and writes to the remote system upgrade control register to determine the next application configuration to be loaded.

When Stratix III devices successfully load the application configuration, they enter into user mode. In user mode, the soft logic (Nios II processor or state machine and the remote communication interface) assists the Stratix III device in determining when a remote system update is arriving. When a remote system update arrives, the soft logic receives the incoming data, writes it to the configuration memory device, and triggers the device to load the factory configuration. The factory configuration reads the remote system upgrade status register and control register, determines the valid application configuration to load, writes the remote system upgrade control register accordingly, and initiates system reconfiguration.

Dedicated Remote System Upgrade Circuitry

This section explains the implementation of the Stratix III remote system upgrade dedicated circuitry. The remote system upgrade circuitry is implemented in hard logic. This dedicated circuitry interfaces to the user-defined factory and application configurations implemented in the Stratix III device logic array to provide the complete remote configuration solution. The remote system upgrade circuitry contains the remote system upgrade registers, a watchdog timer, and a state machine that controls those components. Figure 12–5 shows the remote system upgrade block's data path.

Figure 12–5. Remote System Upgrade Circuit Data Path *(Note 1)*



Note to Figure 12–4:

(1) RU_DOUT, RU_SHIFTnLD, RU_CAPTnUPDT, RU_CLK, RU_DIN, RU_nCONFIG, and RU_nRSTIMER signals are internally controlled by the ALTREMOTE_UPDATE megafunction. For more information about the ALTREMOTE_UPDATE megafunction, refer to the *ALTREMOTE_MUPDATE Megafunction User Guide*.

Remote System Upgrade Registers

The remote system upgrade block contains a series of registers that store the page addresses, watchdog timer settings, and status information. These registers are detailed in Table 12–2.

Table 12–2. Remote System Upgrade Registers (Part 1 of 2)

Register	Description
Shift register	Accessible by the logic array and allows the update, status, and control registers to be written and sampled by user logic. Write access is enabled in remote update mode for factory configurations to allow writes to the update register.
Control register	Contains the current page address, the user watchdog timer settings, and one bit specifying whether the current configuration is a factory configuration or an application configuration. During a read operation of an application configuration, this register is read into the shift register. When a reconfiguration cycle is initiated, the contents of the update register are written into the control register.

Table 12–2. Remote System Upgrade Registers (Part 2 of 2)

Register	Description
Update register	Contains data similar to that in the control register. However, it can only be updated by the factory configuration by shifting data into the shift register and issuing an update operation. When a reconfiguration cycle is triggered by the factory configuration, the control register is updated with the contents of the update register. During a capture in a factory configuration, this register is read into the shift register.
Status register	Written to by the remote system upgrade circuitry on every reconfiguration to record the cause of the reconfiguration. This information is used by the factory configuration to determine the appropriate action following a reconfiguration. During a capture cycle, this register is read into the shift register.

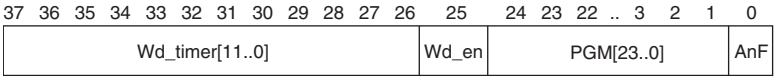
The remote system upgrade control and status registers are clocked by the 10-MHz internal oscillator (the same oscillator that controls the user watchdog timer). However, the remote system upgrade shift and update registers are clocked by the user clock input (`RU_CLK`).

Remote System Upgrade Control Register

The remote system upgrade control register stores the application configuration page address and user watchdog timer settings. The control register functionality depends on the remote system upgrade mode selection. In remote update mode, the control register page address bits are set to all zeros (`24'b0 = 0×000000`) at power up in order to load the factory configuration. A factory configuration in remote update mode has write access to this register.

The control register bit positions are shown in Figure 12–6 and defined in Table 12–3. In the figure, the numbers show the bit position of a setting within a register. For example, bit number 8 is the enable bit for the watchdog timer.

Figure 12–6. Remote System Upgrade Control Register



The application-not-factory (`AnF`) bit indicates whether the current configuration loaded in the Stratix III device is the factory configuration or an application configuration. This bit is set low by the remote system upgrade circuitry when an error condition causes a fall-back to the factory configuration. When the `AnF` bit is high, the control register access is limited to read operations. When the `AnF` bit is low, the register allows write operations and disables the watchdog timer.

In remote update mode, factory configuration design sets this bit high (1'b1) when updating the contents of the update register with the application page address and watchdog timer settings.

Table 12–3. Remote System Upgrade Control Register Contents (Part 1 of 2)

Control Register Bit	Remote System Upgrade Mode	Value *(2)*	Definition
`AnF` *(1)*	Remote update	1'b0	Application not factory
`PGM[23..0]`	Remote update	24'b0×000000	AS configuration start address (`StAdd[23..0]`)

Table 12–3. Remote System Upgrade Control Register Contents (Part 2 of 2)

Control Register Bit	Remote System Upgrade Mode	Value *(2)*	Definition
Wd_en	Remote update	1'b0	User watchdog timer enable bit
Wd_timer[11..0]	Remote update	12'b000000000000	User watchdog time-out value (most significant 12 bits of 29-bit count value: {Wd_timer[11..0], 17'b0})

Notes to Table 12–3:

(1) In remote update mode, the remote configuration block does not update the AnF bit automatically (you can update it manually).

(2) This is the default value of the control register bit.

Remote System Upgrade Status Register

The remote system upgrade status register specifies the reconfiguration trigger condition. The various trigger and error conditions include in the following:

- Cyclic redundancy check (CRC) error during application configuration
- nSTATUS assertion by an external device due to an error
- Stratix III device logic array triggers a reconfiguration cycle, possibly after downloading a new application configuration image
- External configuration reset (nCONFIG) assertion
- User watchdog timer time out

Figure 12–7 and Table 12–4 specify the contents of the status register. The numbers in the figure show the bit positions within a 5-bit register.

Figure 12–7. Remote System Upgrade Status Register

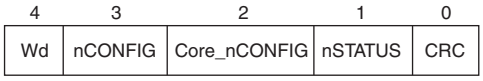


Table 12–4. Remote System Upgrade Status Register Contents

Status Register Bit	Definition	POR Reset Value
CRC (from configuration)	CRC error caused reconfiguration	1 bit '0'
nSTATUS	nSTATUS caused reconfiguration	1 bit '0'
CORE_nCONFIG *(1)*	Device logic array caused reconfiguration	1 bit '0'
nCONFIG	nCONFIG caused reconfiguration	1 bit '0'
Wd	Watchdog timer caused reconfiguration	1 bit '0'

Note to Table 12–4:

(1) Logic array reconfiguration forces the system to load the application configuration data into the Stratix III device. This occurs after the factory configuration specifies the appropriate application configuration page address by updating the update register.

Remote System Upgrade State Machine

The remote system upgrade control and update registers have identical bit definitions, but serve different roles (refer to Table 12–2). While both registers can only be updated when the device is loaded with a factory configuration image, the update register writes are controlled by the user logic; the control register writes are controlled by the remote system upgrade state machine.

In factory configurations, the user logic sends the AnF bit (set high), the page address, and the watchdog timer settings for the next application configuration bit to the update register. When the logic array configuration reset (RU_nCONFIG) goes high, the remote system upgrade state machine updates the control register with the contents of the update register and initiates system reconfiguration from the new application page.

To ensure the successful reconfiguration between the pages, assert RU_nCONFIG signal for a minimum of 250 ns. This is equivalent to strobing the reconfig input of the ALTREMOTE_UPDATE megafunction high for a minimum of 250 ns.

In the event of an error or reconfiguration trigger condition, the remote system upgrade state machine directs the system to load a factory or application configuration (page zero or page one, based on the mode and error condition) by setting the control register accordingly. Table 12–5 lists the contents of the control register after such an event occurs for all possible error or trigger conditions.

The remote system upgrade status register is updated by the dedicated error monitoring circuitry after an error condition but before the factory configuration is loaded.

Table 12–5. Control Register Contents After an Error or Reconfiguration Trigger Condition

Reconfiguration Error/Trigger	Control Register Setting Remote Update
nCONFIG reset	All bits are 0
nSTATUS error	All bits are 0
CORE triggered reconfiguration	Update register
CRC error	All bits are 0
Wd time out	All bits are 0

Capture operations during factory configuration access the contents of the update register. This feature is used by the user logic to verify that the page address and watchdog timer settings were written correctly. Read operations in application configurations access the contents of the control register. This information is used by the user logic in the application configuration.

User Watchdog Timer

The user watchdog timer prevents a faulty application configuration from stalling the device indefinitely. The system uses the timer to detect functional errors after an application configuration is successfully loaded into the Stratix III device.

The user watchdog timer is a counter that counts down from the initial value loaded into the remote system upgrade control register by the factory configuration. The counter is 29-bits wide and has a maximum count value of 2^{29}. When specifying the user watchdog timer value, specify only the most significant 12 bits. The granularity of the timer setting is 2^{15} cycles. The cycle time is based on the frequency of the 10-MHz internal oscillator. Table 12–6 specifies the operating range of the 10-MHz internal oscillator.

Table 12–6. 10-MHz Internal Oscillator Specifications

Minimum	Typical	Maximum	Unit
5	6.5	10	MHz

The user watchdog timer begins counting once the application configuration enters device user mode. This timer must be periodically reloaded or reset by the application configuration before the timer expires by asserting `RU_nRSTIMER`. If the application configuration does not reload the user watchdog timer before the count expires, a time-out signal is generated by the remote system upgrade dedicated circuitry. The time-out signal tells the remote system upgrade circuitry to set the user watchdog timer status bit (`Wd`) in the remote system upgrade status register and reconfigures the device by loading the factory configuration.

To allow remote system upgrade dedicated circuitry to reset the watchdog timer, you must assert the `RU_nRSTIMER` signal active for a minimum of 250 ns. This is equivalent to strobing the `reset_timer` input of the ALTREMOTE_UPDATE megafunction high for a minimum of 250 ns.

The user watchdog timer is disabled during the configuration cycle of the device. Errors during configuration are detected by the CRC engine. Also, the timer is disabled for factory configurations. Functional errors should not exist in the factory configuration since it is stored and validated during production and is never updated remotely.

The user watchdog timer is disabled in factory configurations and during the configuration cycle of the application configuration. It is enabled after the application configuration enters user mode. If you do not wish to use the user watchdog timer feature during application configuration user mode operation, turn this feature off by setting `Wd_en` bit to `1'b0` in the update register during factory configuration user mode operation.

Quartus II Software Support

The Quartus II software provides the flexibility to include the remote system upgrade interface between the Stratix III device logic array and the dedicated circuitry, generate configuration files for productions, and remote programming of the system configuration memory.

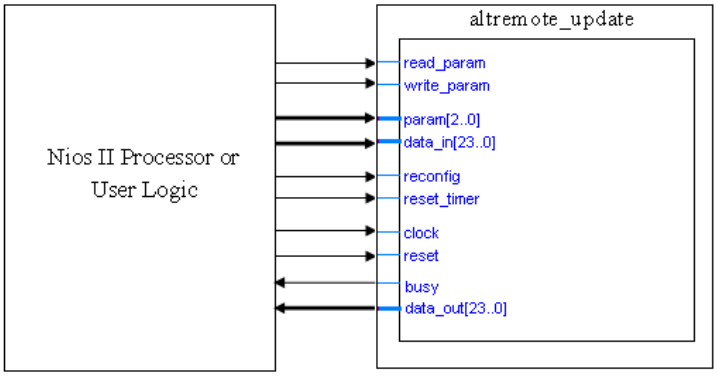
The implementation of the **ALTREMOTE_UPDATE megafunction** option in the Quartus II software is for the interface between the remote system upgrade circuitry and the device logic array interface. Using the megafunction block instead of creating your own logic saves design time and offers more efficient logic synthesis and device implementation.

ALTREMOTE_UPDATE Megafunction

The ALTREMOTE_UPDATE megafunction provides a memory-like interface to the remote system upgrade circuitry and handles the shift register read/write protocol in Stratix III device logic. This implementation is suitable for designs that implement the factory configuration functions using a Nios II processor or user logic in the device.

Figure 12–8 shows the interface signals between the ALTREMOTE_UPDATE megafunction and Nios II processor / user logic.

Figure 12–8. Interface Signals Between the ALTREMOTE_UPDATE Megafunction and the Nios II Processor



For more information about the ALTREMOTE_UPDATE Megafunction and the description of ports listed in Figure 12–8, refer to the *ALTREMOTE_UPDATE Megafunction User Guide*.

Chapter Revision History

Table 12–7 lists the revision history for this chapter.

Table 12–7. Chapter Revision History

Date	Version	Changes Made
March 2010	1.5	Updated for the Quartus II version 9.1 SP2 release: ■ Updated "Remote System Upgrade State Machine" and "User Watchdog Timer" sections. ■ Updated Table 12–6. ■ Updated Figure 12–1. ■ Removed "Conclusion" section. ■ Minor text edits.
February 2009	1.4	Removed "Referenced Documents" section.
October 2008	1.3	■ Updated "Introduction" section. ■ Updated New Document Format.
October 2007	1.2	■ Added new section "Referenced Documents". ■ Added live links for references.
May 2007	1.1	■ Minor text edits to page 4 and 5. ■ Changes to Figure 12–2. Added Figure 12–3. Added a note to Figure 12–5. Added Figure 12–8. ■ Added new section, "Enabling Remote Update" on page 12–4. ■ Removed references to "Remote System Upgrade atom" and section of same title. Removed "Interface Signals Between Remote System Upgrade Circuitry and Stratix III Device Logic Array" section. Removed Table titled "Interface Signals between Remote System Upgrade Circuitry and Stratix III Device Logic Array." Removed footnote, table titled "Input Ports of the altremote_update Megafunction," table titled "Output Ports of the altremote_update Megafunction," and table titled "Parameter Settings for the altremote_update Megafunction" in section "altremote_update Megafunction" on page 12–15. Removed "System Design Guidelines Using Remote System Upgrade With Serial Configuration Devices" section.
November 2006	1.0	Initial Release.