WP155 (v1.1) April 22, 2002

Triple DES Encryption in Selected Virtex-II Devices

This white paper describes Triple DES Encryption for the Virtex™-II devices listed in the following table:

Device	Engineering Sample (ES) (JTAG IDCODE Version Number)	Production (JTAG IDCODE Version Number)
XC2V40	0001	N / A
XC2V1000	0001 or 0010[1]	0010
XC2V3000	0001	N / A
XC2V6000	0001 or 0010	0011

Notes:

1. Some production mask set devices may be marked ES prior to Production release.

Other Virtex-II Family members not listed in the above table support Triple DES Encryption without any workarounds. In the future, production versions of the devices listed (identified by new JTAG version numbers) will also support Triple DES Encryption as identified in the Virtex-II handbook.

Why a Workaround is Needed

Figure 1 and Figure 2 describe the normal loading configuration sequence. The GHIGH signal is used during configuration to disable input pins and to keep the FPGA logic in a known, static state.

When GHIGH = 1, the FPGA logic is isolated from the Look-Up Table (LUT) configuration bits and flip-flops (FFs). During this time, the LUT configuration bits and FFs are loaded with logic 0 or 1. After the loading process is complete, the GHIGH signal toggles from 1 to 0 to drive the LUT configuration bits and the FFs values into the FPGA. In the end, DONE is asserted High to indicate the completion of the entire configuration process.

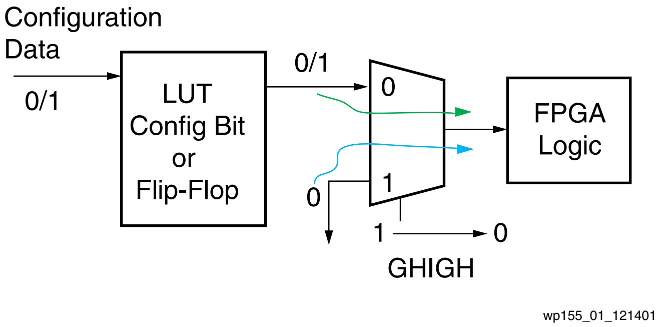

Figure 1: **Normal Bitstream Loading Sequence**

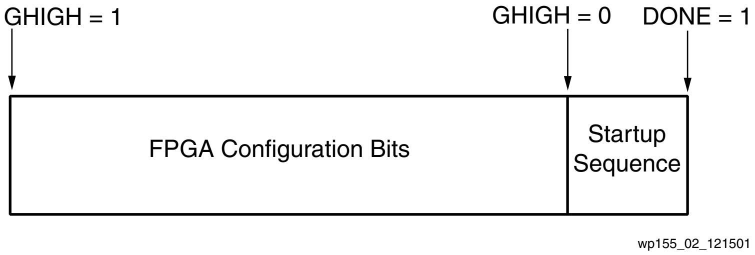

Figure 2: **An example of How FPGA Logic is Configured**

Through extensive device characterization, the GHIGH signal was found to be sensitive to some process corners. When GHIGH toggles from 1 to 0, the MUX 0 and 1 paths are *both* open momentarily, allowing the 0 value to potentially pass through the MUX and overwrite a logic 1 at the output of the LUT configuration bit or FF. See Figure 3. This would pass on an incorrect value to the FPGA logic.

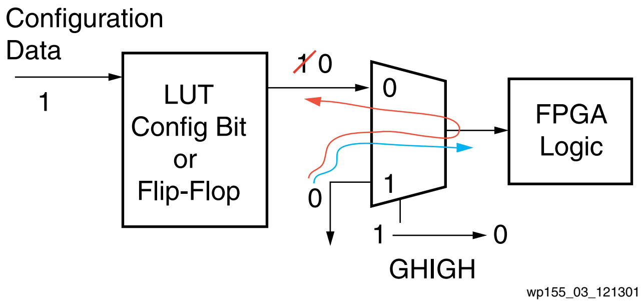

Figure 3: **Incorrect FPGA Configuration Caused by Sensitivity to Process Corners**

Even though the probability of incorrect FPGA configuration is low, steps can be taken to ensure the LUT configuration bits and FFs are loaded correctly. By rewriting the LUT configuration bits and FFs after GHIGH toggles to 0, the correct logic values are loaded into the FPGA. See Figure 4. This methodology is implemented as standard for the Virtex-II devices listed in the table on page 1.

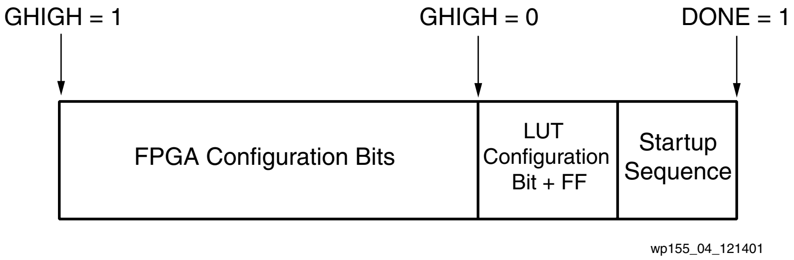

Figure 4: **New Bitstream Configuration Methodology**

For Triple DES encryption to work, the FPGA logic expects a fixed bitstream length with one write pass of configuration bits. Therefore, the configuration sequence of extended bitstream with rewriting of the LUT configuration bits and FFs at the end of configuration would not work.

Using Triple DES Encryption

For Triple DES to work on the devices in the table, the GHIGH signal has to be set to 0 before the loading of configuration bits. This enables the bitstream to meet standard length and one write pass requirements. See Figure 5.

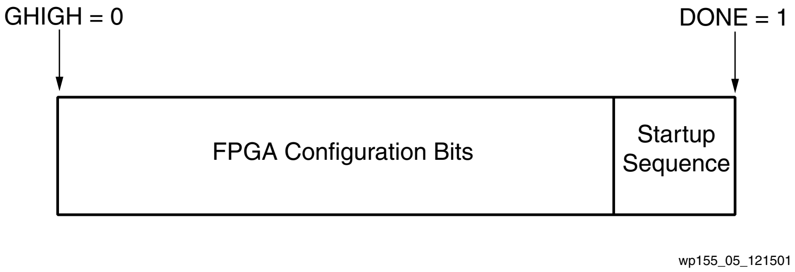

Figure 5: **Early GHIGH Configuration Bitstream**

By setting GHIGH to 0 at the beginning of the configuration bitstream, it allows the configuration bits to directly drive into the FPGA logic during configuration. This is equivalent to a "hot" FPGA configuration. Careful system management must be done to ensure a successfully encrypted bitstream.

> **WARNING**: A correct keyset must be used at all times for configuration of Virtex-II devices with this methodology (setting GHIGH to 0 at the beginning of the configuration bitstream).
>
> If an incorrectly keyed bitstream is loaded into the FPGA (i.e., wrong keys or no keys are programmed into the device), the device could draw an excessive amount of current. This could result in the device getting hot and becoming permanently damaged.

The following procedures are necessary for the Virtex-II devices described within to be configured and started up properly when using Triple DES Encryption.

1. Support for Triple DES Encryption begins in ISE/Foundation software version 4.1i. The software patch available at the following link is needed with software version 4.1i. Since it is automatically included in 4.2i software, no patch is needed. The necessary files and installation procedure for the version 4.1i "patch" software *only* is available online at: **http://support.xilinx.com/techdocs/13450.htm**

2. For software beginning with version 4.1i, use the following command to encrypt the design:
   `bitgen -g Encrypt:Yes xxxx.ncd` where xxxx.ncd is the design file

3. Digital Clock Manager (DCM) Reset Requirement – Do not use the STARTUP_WAIT feature of the DCM. Reset the DCM after the DONE signal is asserted High.

4. Digital Controlled Impedance (DCI) Matching Requirement – If the DCI feature is used on the I/O pins, wait for 600 μs after the DONE signal is asserted High to ensure complete DCI matching before FPGA startup.

5. Overall System Operation – This is very much dependent on the overall system setup and is design dependent. By setting GHIGH to 0 at the beginning of the configuration sequence (configuring FPGA “hot”), the path between the input pins and the FPGA logic is open during configuration. As recommended, I/Os should be kept in a static state during the Virtex-II configuration process. If for some reason the bitstream gets corrupted, the Cyclic Redundancy Check (CRC) would catch the corrupted bitstream and cause the INIT_b pins to toggle Low, and not complete the FPGA configuration.

Revision History

The following table shows the revision history for this document.

Date	Version	Revision
01/03/02	1.0	Initial Xilinx release.
04/22/02	1.1	Added "Warning" to page 3.