congatec
the rhythm of embedded computing

congatec Application Note

Applicable Products	All congatec XTX and COM Express modules
Application Note Subject	Recovery of the congatec Embedded BIOS
Document Name	AN6_BIOS_Recovery
Usage Designation	External

Application Note #6

Revision 1.2

Revision History

Revision	Date (dd.mm.yy)	Author	Changes
1.0	26.01.06	OAL	Initial release, information has been extracted from the application note formerly known as AN1_BIOS_UPDATE
1.1	25.08.06	HCH	Added all AMI BIOS based congatec modules
1.2	04.12.06	OAL	Added AN7_FWH_BIOS_update to section 5

Preface

This application note describes how to proceed if the congatec Embedded BIOS on the congatec AG module must be restored when the image on the module's Flash Memory chip is corrupt and no longer functioning.

Disclaimer

The information contained within this Application Note, including but not limited to any product specification, is subject to change without notice.

congatec AG provides no warranty with regard to this Application Note or any other information contained herein and hereby expressly disclaims any implied warranties of merchantability or fitness for any particular purpose with regard to any of the foregoing. congatec AG assumes no liability for any damages incurred directly or indirectly from any technical or typographical errors or omissions contained herein or for discrepancies between the product and the Application Note. In no event shall congatec AG be liable for any incidental, consequential, special, or exemplary damages, whether based on tort, contract or otherwise, arising out of or in connection with this Application Note or any other information contained herein or the use thereof.

Intended Audience

This Application Note is intended for technically qualified personnel. It is not intended for general audiences.

Symbols

The following symbols may be used in this Application Note:

Warning

Warnings indicate conditions that, if not observed, can cause personal injury.

Caution

Cautions warn the user about how to prevent damage to hardware or loss of data.

Note

Notes call attention to important information that should be observed.

Terminology

Some of the following terms may be used throughout this document.

Term	Description
BIOS	BIOS: Basic Input Output System. BIOS is actually firmware, the software that is programmed into a ROM (Read-Only Memory) chip built onto the motherboard of a computer
Flash	A special type of EEPROM (Electrically Erasable Read Only Memory) that can be erased and reprogrammed in blocks instead of one byte at a time. Many modern PCs have their BIOS stored on a flash memory chip so that it can easily be updated if necessary.
POST	Power-on Self Test. A diagnostic testing sequence run by a computer's BIOS as the computer's power is initially turned on. The POST will determine if the computer's RAM, disk drives, peripheral devices and other hardware components are properly working.
ATAPI	AT Attachment Packet Interface: An extension to EIDE (also called ATA-2) that enables the interface to support CD-ROM players and tape devices.
USB	Universal Serial Bus provides a serial bus standard for connecting computers and peripherals.
ISO9660	Is a specification of the International Organization for Standardization. It specifies the volume and file structure of compact read-only optical disks (CD-ROM) for the information interchange between information processing systems.
FWH	FHW: Firmware Hub. FWH is a LPC memory flash device that contains software such as the PC's BIOS.

Copyright Notice

Some of the information found in this application note has been extracted WITH EXPRESS PERMISSION from the following COPYRIGHTED American Megatrends, Inc documents:

- AMIBIOS8_HDD_Security.pdf
- AMIBIOS8-Flash-Recovery-Whitepaper.pdf
- AMIBIOS8_SerialRedirection.pdf
- AMIBIOS8 Set-up users Guide

congatec AG has made every attempt to ensure that the information in this document is accurate yet the information contained within is supplied "as-is".

Trademarks

Intel and Pentium are registered trademarks of Intel Corporation. Expresscard is a registered trademark of Personal Computer Memory Card International Association (PCMCIA). PCI Express is a registered trademark of Peripheral Component Interconnect Special Interest Group (PCI-SIG). I²C is a registered trademark of Philips Corporation. CompactFlash is a registered trademark of CompactFlash Association. Winbond is a registered trademark of Winbond Electronics Corp. AVR is a registered trademark of Atmel Corporation. ETX is a registered trademark of Kontron AG. AMICORE8 is a registered trademark of American Megatrends Inc. XpressROM is a registered trademark of Insyde Technology, Inc. Microsoft®, Windows®, Windows NT®, Windows CE and Windows XP® are registered trademarks of Microsoft Corporation. VxWorks is a registered trademark of WindRiver. conga, congatec and XTX are registered trademark of congatec AG. All product names and logos are property of their owners.

Contents

1 Introduction

The congatec Embedded Computer Modules use a congatec embedded BIOS, which is based on an AMI BIOS (AMIBIOS8) or Insyde XpressROM BIOS, that is stored in an onboard Flash Memory chip. The BIOS displays a message during POST and on the main setup screen identifying the BIOS project name and a revision code. The initial production BIOS is identified as P852R1xx, where P852 is the congatec internal project name, R is the identifier for a BIOS ROM file, 1 is the so called feature number and xx is the major and minor revision number.

For description purposes section 2 to 4 will use the conga-X852 CPU module with AMI BIOS core as an example. These recovery scenarios will not work with the conga-XLX and conga-CLX CPU modules due to a restriction of the Insyde XpressROM BIOS. If you are using one of these CPU modules you must switch to Section 5. This section describes a BIOS recovery via external FWH and uses the conga-XLX CPU module as an example.

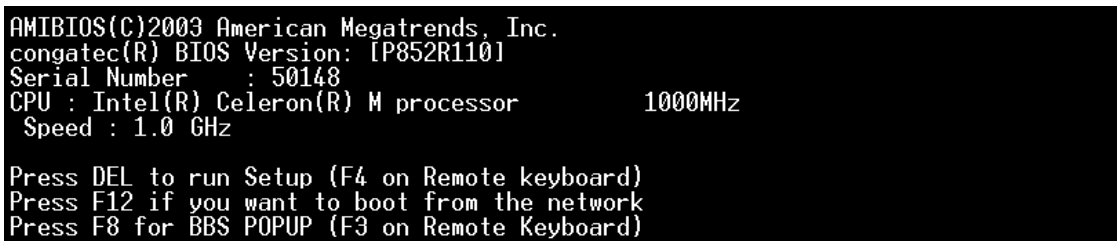


Figure 1 conga-X852 Post Screenshot

2 BIOS Recovery

The 'BIOS recovery' scenario is recommended for situations when the normal flash update fails or the BIOS image on the module has been damaged and the user can no longer boot back to an OS to re-flash the BIOS. The code that handles the BIOS recovery resides in a section of the Flash ROM chip referred to as 'bootblock', which should not be reprogrammed during a standard flash update.

Flash Memory chips used to store the BIOS on the module are divided into multiple segments. Some segments are for general data storage while others have special purposes. The bootblock segment of a Flash Memory chip contains critical BIOS code, including memory detection and “recovery” code used to flash a new BIOS image in case the main BIOS image is corrupted. The bootblock code is executed first when the system is powered on and once completed the main BIOS code takes over system initialization.

The congatec embedded BIOS supports one or all of the following BIOS recovery methods:

- From Storage Devices (3.5" floppy drive, ATAPI CD-ROM and USB floppy drive)
- Via Serial Port (COM1)
- Via external Firmware Hub (FWH)

3 BIOS Recovery via Storage Devices

In order to make a BIOS recovery from a floppy disk, CD-ROM (ISO9660) or USB floppy the BIOS file must be copied into the root directory of the storage device and renamed in *'AMIBOOT.rom'*. No additional files or utilities are required.

The bootblock recovery can be started manually by pressing and holding the <*Ctrl*> and <*Home*> keys down while turning the power on (<*Strg*> and <*Pos1*> on a German keyboard). Continue to hold the keys down until the BIOS accesses the drive (LED on the drive being used is on), then the keys can be released. The BIOS issues a series of 4 beeps that indicate that the system BIOS ROM file has successfully been updated. After that the system will automatically reset and reboot.

Caution

Do not interrupt the BIOS flash process until it has fully completed.

4 BIOS Recovery via Serial Port

The Serial Flash method allows for bootblock recovery to load a BIOS image via a serial port (COM1). This method can be used by many headless embedded systems, which rely on a serial port as a debug and utility console port.

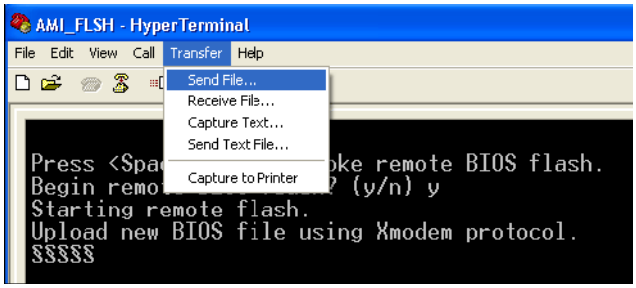
Serial Flash Requirements:

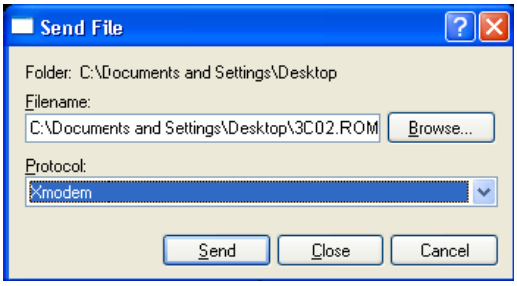
- Host system with serial port running a terminal program that supports XMODEM transfer protocol (HyperTerminal for Microsoft Windows, minicom for Linux/FreeBSD, etc.)
- Null-modem cable

The following section describes how to use Serial Flash:

1. Attach a null-modem cable to the serial port COM1 of the system that requires the update ('target'). Attach the other end of the null modem cable to a system running the terminal program (“host”).
2. Make sure the new BIOS image file is accessible from the host system.
3. Start the terminal program on the host and open a new session. The session should use the following communication parameters: 115200, 8, n, 1, Hardware.
4. Start the target system. The terminal on the host should display the following message: '*Press <SpaceBar> to invoke remote BIOS flash*'. Immediately press the space bar on the host to confirm. If the space bar is not pressed within a few seconds, the system will skip the flash update and perform a normal boot procedure.
5. You will be prompted to confirm the BIOS update. A second string will appear on the host terminal: '*Begin remote BIOS flash? [y/n]*'. Press the <*Y*> key on the host to continue. If the <*N*> key is pressed, the system will skip the flash update and perform a normal boot procedure.

6. You will be prompted to upload the new BIOS file using the XMODEM protocol. Use the host terminal program to select the proper BIOS image and transfer it to the target.





7. If the transfer from host to target is successful, the target will update the BIOS and indicate success. The system will then reboot using the new BIOS image

Caution

Do not interrupt the BIOS flash process until it has fully completed.

HyperTerminal for Microsoft Windows is the most common terminal program available today. XMODEM transfers can be initiated using the *'Send File'* dialog under the *'Transfer'* menu. Serial Flash will work with any terminal communication program that supports VT-100 and XMODEM protocols. This includes products designed for GNU/LINUX and BSD, such as minicom. It is recommended that the terminal program be configured to use the *'CR/LF'* style of line termination.

4.1 BIOS Integrity Test

An additional function of the bootblock code is to test the integrity of the BIOS image in the Flash Mermory chip. If a damaged BIOS image is detected the BIOS recovery mode will be initiated automatically.

During the recovery mode the BIOS will output the POST codes *'Eb'* and *'E9'* on port 80 (can be verified with a standard PCI POST card). Additionally, the message *'BIOS checksum error detected'* will be displayed via the serial port COM1 if a serial connection is established to a host system (section 4 of this document explains how to enable a serial connection to the congatec CPU module). Also, while in the recovery mode the BIOS will continually search peripheral devices such as floppy drive or CD-ROM for a copy of the BIOS file named *'AMIBOOT.rom'.*

Once in the recovery mode the congatec Embedded BIOS can now be restored by inserting a storage device with the BIOS file named *'AMIBOOT.rom'* in the available drive (see section 3 for details). The BIOS recovery will start automatically without a reboot of the system. The BIOS issues a series of 4 beeps that indicate that the system BIOS ROM file has successfully been updated. After that the system will automatically reset and reboot.

To restore the BIOS via the serial port, reboot the system and follow the steps described in section 4 of this document.

5 BIOS Recovery via external FWH

This section briefly describes how to do a BIOS update from the external Firmware Hub (FWH) located on a congatec evaluation carrier board. This may be necessary if the BIOS on the module's Flash Memory chip is corrupt and the module is no longer bootable.

5.1 Required Equipment

The following items were used in this example of how to perform a BIOS update from an external FWH.

- conga-XEVAL (congatec XTX evaluation carrier board)
- conga-XLX CPU module
- LPC FWH, LPC flash memory device (SST-49LF008A or Winbond W39V080FAP2) with current BIOS version preprogrammed by congatec AG
- Boot device, DOS formatted USB-Stick or CF-Card
- BIOS ROM file (contact the congatec AG technical support team for current version)
- congatec System Utility (cgutlcmd.exe, DOS command line version) available for download at www.congatec.com.

The above list of required equipment applies when updating congatec XTX CPU models. When updating congatec COM Express CPU modules the first two entries in the Required Equipment list would be replaced with the following. All other items listed would remain the same.

- conga-CEVAL (congatec COM Express evaluation carrier board)
- COM Express CPU module

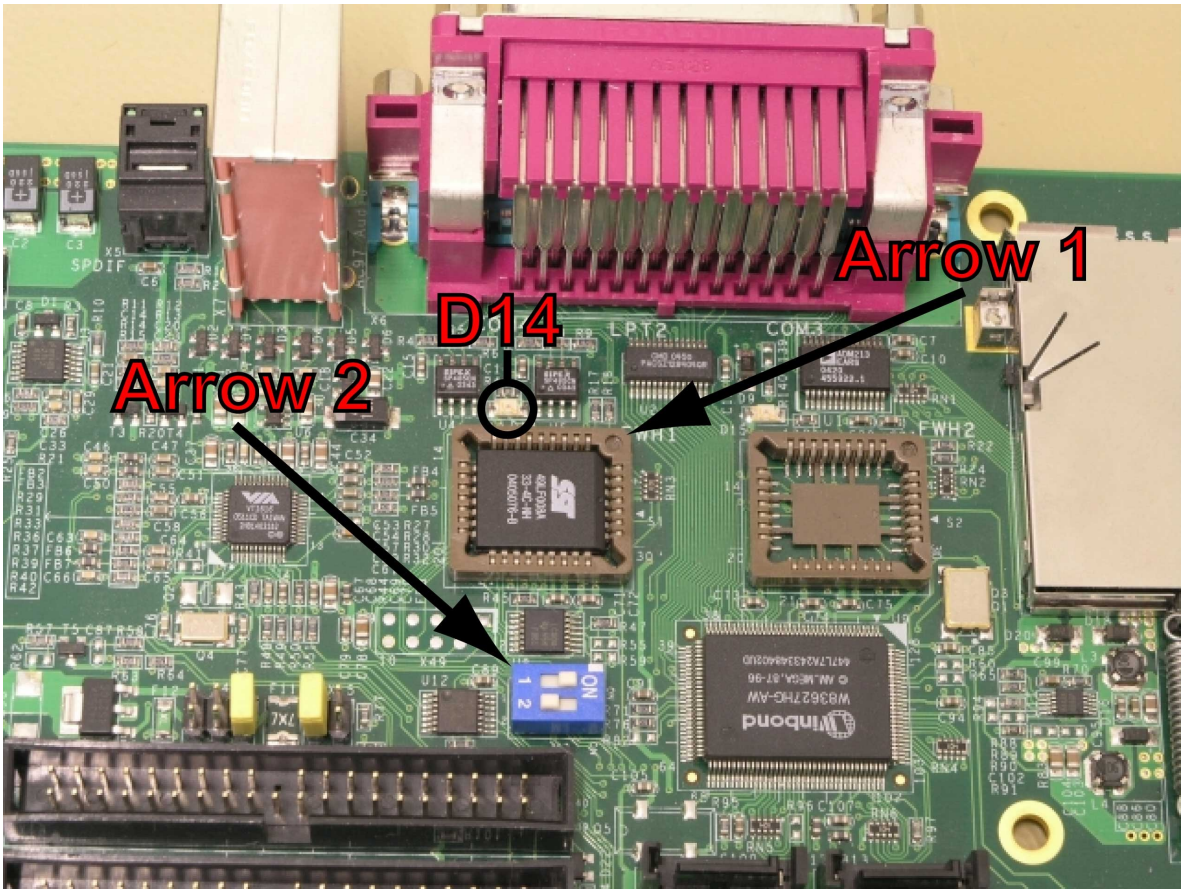
Note

The following example only explains how to perform a BIOS recovery via an external FWH when using the conga-XEVAL XTX evaluation carrier board and XTX CPU module. For information about the dip switch settings when using a conga-CEVAL COM Express evaluation carrier board and COM Express CPU module refer to the conga-CEVAL User's Guide available on the congatec web page at www.congatec.com.

5.2 BIOS Update Procedure

1. Connect the conga-XLX module to the conga-XEVAL carrier board. Insert a the preprogrammed flash memory device into the 32-lead PLCC socket (FWH 1 or FWH 2) as indicated by Arrow 1.

2. Set DIP Switch M3 on the conga-XEVAL as indicated by Arrow 2. The configuration indicated by Arrow 2 is for booting from FWH 1. See the conga-XEVAL User's Guide for exact configuration of DIP Switch when using FWH 2.



Picture 1: FWH 1 selected for BIOS update (DIP1=ON; DIP2=OFF)

3. Insert DOS formatted boot device with congatec System Utility (cgutlcmd.exe) and BIOS ROM-file. Both files must be in the same directory.

4. Push power button. System starts, LED D14 is lit. The conga-XLX module boots using the external FWH and enters DOS mode.

5. Start the congatec System Utility using the following command line:
   C:>cgutlcmd bflash X800R110.ROM /D (see congatec System Utility User's Guide for further details about command line options).

6. The system utility will start and perform the required preprocessing and will then stop and inform you that it is now safe to switch to another flash part. Now switch the DIP Switch to the off position (position 1 Off, position 2 Off).

7. Now press any key to confirm that the DIP Switch is now turned off. The BIOS update process will be performed as usual and the CPU module's onboard BIOS Flash Memory chip will be programmed. Once completed the message *'BIOS successfully updated'* will be displayed.

8. Restart system and enter the *'BIOS Setup Program'* by pressing the <*DEL*> key during POST.

9. Once the *'BIOS Setup Program'* has been entered, load BIOS CMOS defaults (AMI BIOS: press first <*F9*> key then <*Enter*>. Inside BIOS: press first the <*L*> key then <*Enter*> key). This procedure updates the RTC CMOS.

10. Save settings and exit BIOS (AMI BIOS: press first <*F10*> key then <*Enter*>. Insyde BIOS: press the <*X*> key).

11. The system restarts. BIOS has been successfully updated.