Application Note

congatec Application Note#1

Affected Products	Products featuring UEFI Firmware
Subject	Update the congatec embedded BIOS
Confidential/Public	public
Author	CJR

Revision History

Revision	Date (yyyy-mm-dd)	Author	Changes
1.0	2005-05-23	HCH	Initial Release
2.0	2016-12-08	CJR	Complete rework and update of existing AN revision 1.4

Preface

This Application Note provides information about updating the embedded BIOS on congatec products.

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.

Electrostatic Sensitive Device

All congatec AG products are electrostatic sensitive devices and are packaged accordingly. Do not open or handle a congatec AG product except at an electrostatic-free workstation. Additionally, do not ship or store congatec AG products near strong electrostatic, electromagnetic, magnetic, or radioactive fields unless the device is contained within its original manufacturer's packaging. Be aware that failure to comply with these guidelines will void the congatec AG Limited Warranty.

Technical Support

congatec AG technicians and engineers are committed to providing the best possible technical support for our customers so that our products can be easily used and implemented. We request that you first visit our website at www.congatec.com for the latest documentation, utilities and drivers, which have been made available to assist you. If you still require assistance after visiting our website then contact our technical support department by email at support@congatec.com

Symbols

The following are symbols used in this application note.

Note

Notes call attention to important information that should be observed.

Caution

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

Warning

Warnings indicate that personal injury can occur if the information is not observed.

Copyright Notice

Trademarks

Product names, logos, brands, and other trademarks featured or referred to within this user’s guide or the congatec website, are the property of their respective trademark holders. These trademark holders are not affiliated with congatec AG, our products, or our website.

Terminology

Term	Description
UEFI	Unified Extensible Firmware Interface
AMI	American Megatrends, Inc - congatec’s BIOS partner
Aptio	AMIs UEFI Firmware product
POST	Power On Self Test
ME	Management Engine firmware on Intel Core platforms
TXE	Trusted Execution Environment firmware on Intel Atom platforms

CGOS API	congatec operating system application programming interface
CGUTIL	congatec System Utility
COM	Computer on Module
SBC	Single board computer
GUI	Graphical user interface

1 Introduction

The BIOS firmware is stored in an onboard flash memory chip and can be updated by using the congatec system utility (CGUTIL). The flash tool can be found on the congatec web page at www.congatec.com. This application note describes how to update the BIOS and uses the conga-TS170 as an example. The BIOS update must be performed on all other CPU products in the same way as described in this application note.

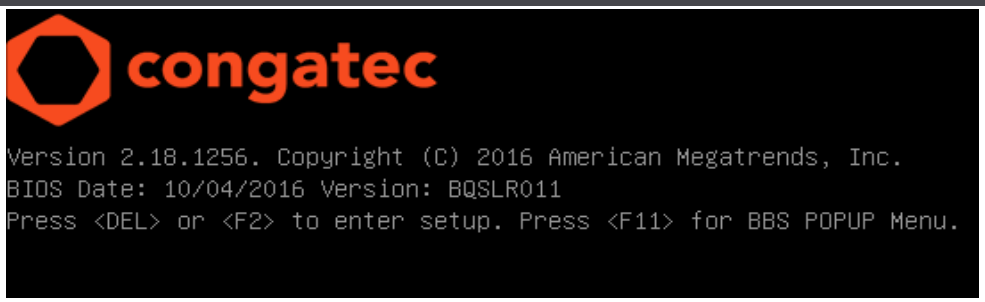
The BIOS displays a message during POST and on the main setup screen identifying the BIOS project name and a revision code. The initial production BIOS is identified as BQSLRxxx.bin, where 'BQSL' is the congatec internal BIOS project name, 'R' is the identifier for a BIOS file and 'xxx' is a sequential number that defines the revision of the BIOS file.

Note

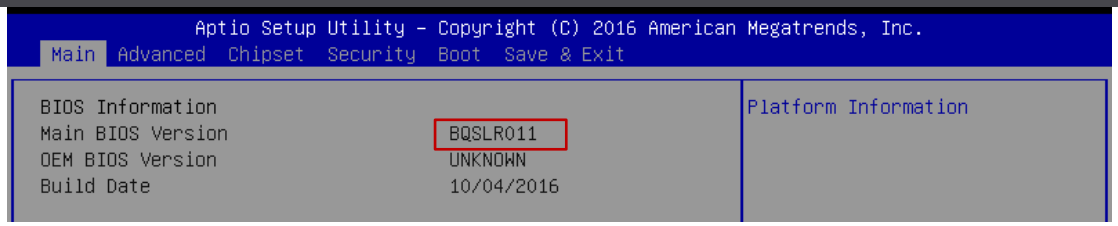
The file extension ".bin" is default for all new UEFI based products. The handling within the command line or GUI version of the congatec system utility does not change as a result of different file extension. Most new BIOS binary files include supplementary parts of the products firmware in addition to the UEFI firmware itself. For Intel based BIOS versions this is referred to as ME or TXE binary.

The BIOS can be determined during BIOS POST and in the BIOS Setup (Main Menu):

BIOS POST



BIOS Setup



2 Using CGUTIL for BIOS Update

There are several ways to update the BIOS of a congatec product. This application note describes the Windows GUI as well as the DOS, UEFI and Linux command line version of the congatec System Utility.

When using the Windows GUI version, some additional drivers must be installed:

1. The required driver package can be found at www.congatec.com
2. Select the software section of the regarding product and download the CGOS API as well as the congatec System Utility.
3. Extract the zip files.
4. Follow the instructions in the readme.txt to install the required driver packages.

The DOS and UEFI based version of the congatec System Utility do not require any additional software or driver packages. It can be run in the command line from a computer started by a DOS or UEFI shell equipped USB memory stick.

The BIOS updating process within the UEFI Shell is very similar to how it's done in DOS.

It is necessary to download and install the actual version of the congatec System Utility as well as the CGOS API in order to perform the steps explained in the subsections 2.1 and 2.3.

Section 2.1 illustrates how to update the BIOS when using the Windows GUI version of CGUTIL. The sections 2.2 and 2.3 are showing the BIOS update process when using the DOS, UEFI and Linux version of CGUTIL.

Caution

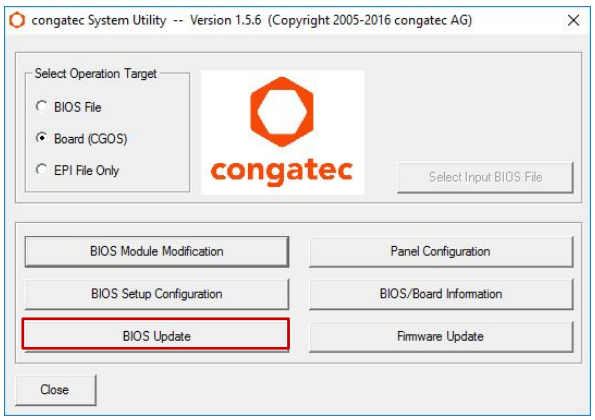
Do not interrupt the congatec System Utility during the BIOS Update procedure regardless of the version used. Otherwise, this will lead to a corrupted BIOS in the flash chip causing the CPU module to be no longer bootable.

Note

Do not use the congatec System Utility to save a BIOS binary from flash to a file as explained in previous revisions of this document. UEFI firmware is writing to the flash a lot during boot-up and even at runtime. The image read back would never be the original BIOS binary. It must not be used to update additional CPU products.

2.1 BIOS update in Windows

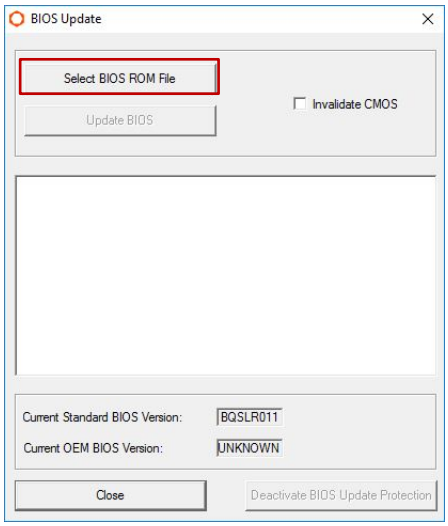
1. Firstly, either contact the congatec technical support or visit the restricted area on the congatec web page to get the latest BIOS revision for the CPU product you are using. Store the appropriate BIOS in a temporary folder.



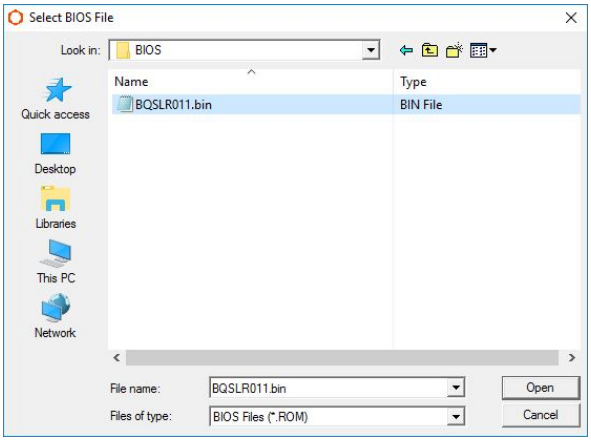
2. Open the “congatec System Utility.”

3. Select “Board (CGOS)” as operating target.

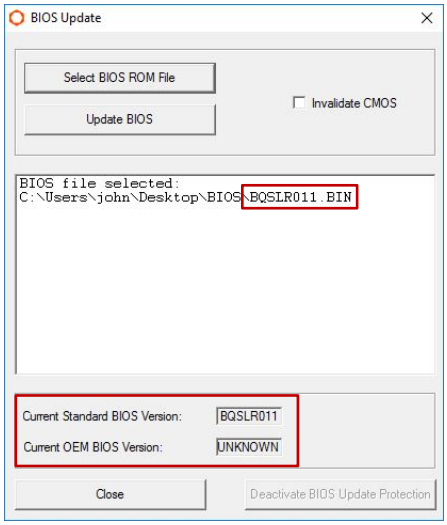
4. Push the button “BIOS Update”.



5. Click “Select BIOS ROM File”



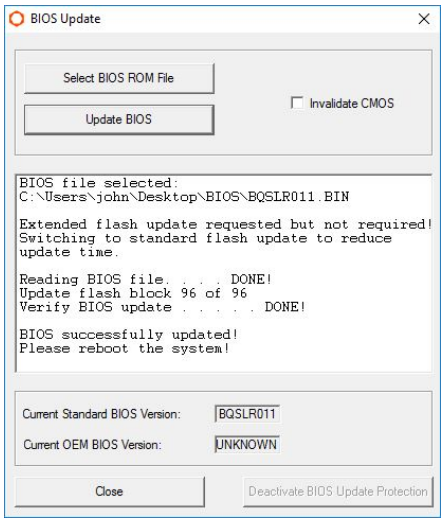
6. Browse for your designated BIOS binary file (in this example "BQSLR011.bin").



7. The selected BIOS binary file is now displayed in in the middle of the BIOS Update dialog box

8. The lower section shows the current BIOS version and if available the current OEM BIOS version, which are stored in the COM or SBC onboard flash memory chip.

9. Click on the "Update BIOS" button to start the update procedure.



10. The option "Invalidate CMOS" is deactivated by default and has no effect on UEFI based firmware.

11. Reboot the system to finish the update process.

NOTE

The BIOS update procedure may take a while. After all blocks have been updated and the BIOS update has been validated, restart the computer and enter the system BIOS setup program. Once entered, load the defaults. To do so, press 'F9' to load the defaults and 'F10' to store and exit the BIOS setup screen.

Due to the increased file size of newer BIOS BIN files, the number of flash blocks to be updated can be up to 256 for 16MB BIOS files. This will be displayed during the update process within the congatec utility and can also lead to increased update time.

The button 'Deactivate BIOS Write Protection' must be pressed if the BIOS write protection is activated. For more information (including CGUTIL DOS usage) about this congatec Embedded BIOS feature see Application Note 5 "AN5_BIOS_Update_And_Write_Protection.pdf" available at www.congatec.com

2.2 BIOS update in DOS or UEFI

1. Get the latest BIOS version of the concerned congatec CPU board.

2. Store the BIOS binary file on a DOS or UEFI bootable USB Stick. Make sure the BIOS binary file is in the same directory as the DOS or UEFI version of the congatec System Utility.

3. Enter the directory which contains the CGUTIL. The BIOS update is accomplished by entering the following command at the prompt:

```
cgutlcmd bflash BIOSNAME.bin /e
```

The parameter BIOSNAME.bin stands for the name of the BIOS file, e.g. "BQSLR011.bin".

```
cgutlcmd bflash BQSLR011.bin /e
```

4. After all blocks have been updated and the BIOS update has been validated, restart the system, enter the system BIOS setup program and load the default settings.

Note

Pay attention to the parameter "/e" within the command line in step 3. This is necessary to ensure a full flash update of new UEFI firmware BIOS files. The tool itself will clarify the need for a full update and perform it if required. A full update means that not only the UEFI firmware content will be flashed to the flash part but also any additional firmware that is required (for example ME and TXE binaries). See next chapter for more details.

2.3 BIOS update in Linux

1. Get the latest BIOS version of the concerned congatec CPU board.
2. Download the latest version of the CGOS API and congatec System Utility form www.congatec.com
3. Unzip the compressed files.
4. Follow the instructions in the .txt files and the CGUTIL User's Guide.
5. Open a command prompt and enter the following line in order to update the BIOS:

```
cgutlcmd bflash BQSLR011.bin /e
```

6. Reboot the system after the BIOS update has been validated.

Note

Make sure that the BIOS binary file is in the current working directory or reference to the absolute path. Also be aware that Linux is case sensitive. Therefore, please keep the spelling of the BIOS file. Pay attention to the parameter "/e" within the command line in step 5. See chapter 3 for more information.

3 CGUTLCMD Command Line Parameters

The command line version of the congatec System Utility supports the parameters below. It is important to understand the reason behind these parameters in order to use them in the correct way.

3.1 "/f" to force the BIOS flash update

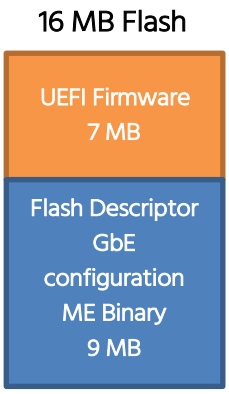
CGUTLCMD has a built-in mechanism to prevent the user from flashing a wrong BIOS file onto a CPU board. When called without "/f" only a BIOS with the same 4 letter BIOS project name as the one that is currently on the flash is accepted. For example, you can not flash the BHSLR011.BIN BIOS onto a conga-TS170 module running the BQSLR011.BIN BIOS because the BIOS project names (BQSL vs BHSL) are not identical. With the "/f" parameter, this protection mechanism is deactivated and any BIOS with the same size as the flash part can be updated.

Note

Only use /f when you know what you are doing!!!

3.2 "/e" for extended BIOS flash update

This parameter instructs CGUTLCMD to perform a full flash update and not only update the UEFI firmware in the flash chip. Especially newer Intel platforms use the BIOS flash to store additional information like TXE or ME binaries or the configuration file of the integrated Ethernet controller. The figure below explains the "/e" usage:



For most BIOS updates, only the UEFI firmware needs to be flashed because the "extended" flash content usually does not change very often.

The congatec system utility auto detects if a full flash update is necessary or not and prompts the user to use the /e parameter in case it is necessary.

On the other hand, when /e is used but the full update is not necessary because the extended flash content is the same on the new and current BIOS, the system utility skips the extended update and only flashes the flash blocks of the UEFI firmware to safe time.

3.3 "/ef" - to force an extended BIOS flash update

The /ef parameter forces the full BIOS flash update (UEFI firmware + extended area). It's only used in special cases. Such a special case is, for example, the onboard BIOS flash recovery after booting from an external flash part on the carrier board. The onboard BIOS flash might be completely empty or not have the correct extended BIOS image programmed.

Updating the BIOS with /ef should not be the preferred way of using CGUTLCMD because all flash blocks will be updated which takes a long time.

3.4 Examples

Flash UEFI firmware of BQSLR011.bin file only. In case the extended area on the flash part is different than the one in BQSLR011.bin, the utility prompts the user for the /e parameter for full BIOS flash update.

- `cgutlcmd bflash BQSLR011.bin`

In case the extended area is the same on the flash part and in BQSLR011.bin, safe time and only flash the UEFI firmware. In case the extended areas are different, perform a full flash update.

- `cgutlcmd bflash BQSLR011.bin /e`

No matter whether the extended area is different or not, always update the complete BIOS file.

- `cgutlcmd bflash BQSLR011.bin /ef`

No matter which BIOS is on the target CPU product, update the UEFI firmware with BQSLR011.bin

- `cgutlcmd bflash BQSLR011.bin /f`

No matter which BIOS is on the target system, update the complete BIOS flash (UEFI firmware + extended area) with BQSLR011.bin

- `cgutlcmd bflash BQSLR011.bin /ef /f`