congatec Application Note #7

Affected Products	x86-based products
Subject	Updating the congatec Embedded BIOS from an external BIOS flash device
Confidential/Public	Public
Author	MAN

Revision History

Revision	Date (yyyy-mm-dd)	Author	Changes
1.0	2006-05-31	OAL	Initial release.
1.1	2006-08-06	HCH	Expanded for all congatec XTX and COM Express modules.
1.2	2013-02-18	CJR	Added COM Express and Qseven modules, added SPI flash update procedure, renamed AN to AN7_External_BIOS_Update.
1.3	2015-01-13	GDA	Added section on making a bootable FreeDOS USB stick, added 128Mbit Winbond SPI flash chip.
1.4	2017-04-12	GAD	Completely reworked and updated to new template.
1.5	2020-06-25	CJR	Updated for 32MB flash device support and new template.
1.6	2021-01-25	GAD	Added note regarding APL update
1.7	2023-08-08	MAN	Updated template Added TEVA2, GEVA, HEVA to sections 2.1 and 6 Updated link to AN31 in section 3.2 Added link to AN01 in section 4.2 Minor improvements throughout the document
1.8	2023-08-31	MAN	Added packages and supported SOIC16 Flashes to section 2.3 Added SOIC16 package to section 4.1 Updated “≥32Mbyte” in section 4.1 and 4.2 Added packages to section 6 Added note for 1.8V SOIC8 package to section 6.6

Preface

This application note describes how to proceed if the congatec Embedded BIOS needs to be updated from a SPI flash device when the image on the internal flash is corrupt and no longer functioning.

Software Licenses

Notice regarding Open Source software

The congatec products contain Open Source software that has been released by programmers under specific licensing requirements such as the "General Public License" (GPL) Version 2 or 3, the "Lesser General Public License" (LGPL), the "ApacheLicense" or similar licenses.

You can find the specific details at https://www.congatec.com/en/licenses/. Search for the revision of the BIOS/UEFI or Board Controller Software (as shown in the POST screen or BIOS setup) to get the complete product related license information. To the extent that any accompanying material such as instruction manuals, handbooks etc. contain copyright notices, conditions of use or licensing requirements that contradict any applicable Open Source license, these conditions are inapplicable.

The use and distribution of any Open Source software contained in the product is exclusively governed by the respective Open Source license. The Open Source software is provided by its programmers without ANY WARRANTY, whether implied or expressed, of any fitness for a particular purpose, and the programmers DECLINE ALL LIABILITY for damages, direct or indirect, that result from the use of this software.

OEM/ CGUTL BIOS

BIOS/UEFI modified by customer via the congatec System Utility (CGUTL) is subject to the same license as the BIOS/UEFI it is based on. You can find the specific details at https://www.congatec.com/en/licenses/.

Disclaimer

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

congatec GmbH 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 GmbH 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 GmbH 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 GmbH products are electrostatic sensitive devices and are packaged accordingly. Do not open or handle a congatec GmbH product except at an electrostatic-free workstation. Additionally, do not ship or store congatec GmbH 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 GmbH Limited Warranty.

Technical Support

congatec GmbH 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 GmbH, 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
COM	Computer on Module
SBC	Single board computer

Contents

1 Introduction

congatec embedded computer modules and single board computers use congatec embedded BIOS stored in an onboard SPI flash device. It is based on AMIs Aptio UEFI firmware solution.

This application note describes how to update a congatec BIOS from the external SPI flash located on the evaluation carrier board for the respective module or on the debug adapter for SBCs.

Updating from an external flash device may be necessary if the BIOS on the onboard flash is corrupt and no longer bootable.

The conga-TS170 and the BIOS binary file BQSLR011.bin is used as an example.

2 Required Equipment

The following equipment is required to perform a BIOS update from an external flash device.

2.1 Equipment for Modules Only

- congatec evaluation carrier board
  - conga-TEVAL or TEVAL/COMe 3.0 for COM Express type 6 modules
  - conga-X7/EVAL for COM Express type 7 modules
  - conga-MEVAL for COM Express type 10 modules
  - conga-QEVAL/Qseven 2.0 for Qseven modules
  - conga-SEVAL for SMARC modules
  - conga-HPC/EVAL-Server for COM-HPC Server modules
  - conga-HPC/EVAL-Client for COM-HPC Client modules
- congatec CPU module

2.2 Equipment for Single Board Computers Only

- conga-MITX/debug card (PN047858)
- congatec Mini-ITX SBC

2.3 Additional Equipment

- Power Supply
- USB Keyboard
- Display
- SPI flash device with the current BIOS preprogrammed (see section 4 for instruction on how to preprogram an external BIOS flash device)
  - Examples of supported SPI flashes are
    - SOIC8 package
      - Macronix MX25L25645GM2I for 256Mbit (32MByte) 3.3V
      - Winbond W25Q128FV for 128Mbit (16MByte) 3.3V
      - Winbond W25Q64CV for 64Mbit (8MByte) 3.3V
      - Winbond W25Q32BV for 32Mbit (4MByte) 3.3V
      - Winbond W25Q64FWSSIQ for 64Mbit (8MByte) 1.8V
    - SOIC16 package
      - MX25L25645GMI-08G
      - MX25L51245GMI-08G

    - W25Q256JVFQ
    - W25Q512JVFQ
  - Check the module's user's guide for the BIOS binary size, operating voltage and additional parameters like SFDP.

Note

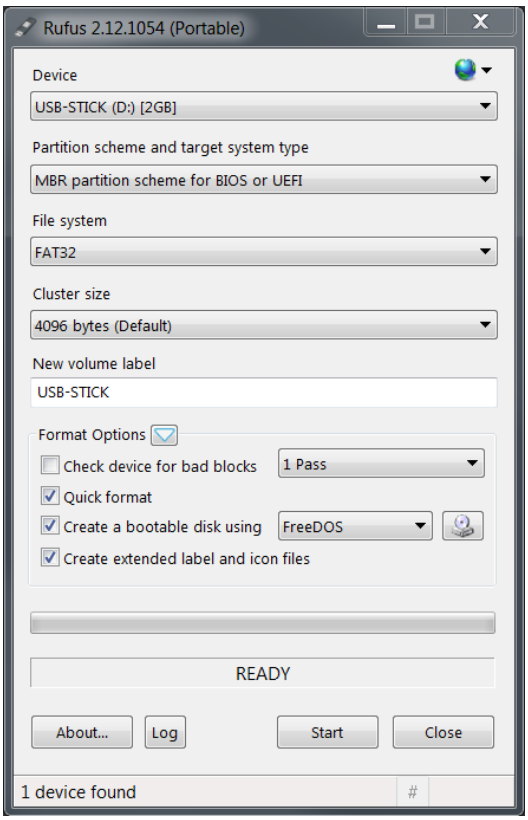
The external BIOS flash chip must be the same size as the BIOS .bin file. An external flash chip larger than the BIOS file size might not work.

- Bootable DOS or UEFI shell USB memory stick (refer to section 3)
- BIOS binary file (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.)
- Congatec System Utility, available for download at www.congatec.com
  - cgutlcmd.exe (DOS command line version)
  - cgutlcmd.efi (UEFI shell command line version)

3 Creating a Bootable USB Stick

3.1 Creating a Bootable FreeDOS USB Stick

1. Download Rufus from http://rufus.akeo.ie/
2. Insert the USB stick.
3. Launch and set up Rufus as shown in the screenshot below:



4. Click Start.
5. Download the latest version of the congatec system utility (cgutil.zip) from www.congatec.com
6. Copy the DOS command line version of the congatec system utility (cgutlcmd.exe) from cgutil.zip to the root directory of this FreeDOS USB stick.
7. Copy the desired BIOS binary file (*.bin file) for your product to the root directory of this FreeDOS USB stick.

3.2 Creating a Bootable UEFI Shell USB Stick

Refer to AN31_Creating_an_UEFI_Stick on how to create a bootable UEFI shell stick.

After the UEFI shell stick is ready:

1. Download the latest version of the congatec system utility (cgutil.zip) from www.congatec.com
2. Copy the expanded UEFI shell command line version of the congatec system utility (cgutlcmd.efi) from cgutil.zip to the \efi directory of this UEFI shell USB stick.
3. Copy the desired BIOS binary file (*.bin file) for your product to the \efi directory of this UEFI shell USB stick.

4 Pre-Programming the SPI Flash Device

There are two ways for pre-programming the external SPI flash device.

4.1 Programming with a Flash Programmer

This is a general overview of the key points you need to be aware of when programming the SPI flash with a flash programmer.

The flash devices have a SOIC8 or SOIC16 footprint and need the corresponding adapter.

Caution

There are different voltages for different products. Applying 3.3V to a 1.8V SPI flash will destroy the chip. The SPI interface on the conga-SEVAL runs at 1.8V, while other evaluation carriers and the MITX debug card run at 3.3V.

Refer to section 2.3 “Additional Equipment” for the required SPI flash device and the correct BIOS binary file.

After making sure you got the right programmer and adapter for the SPI flash device, program the BIOS binary onto the SPI flash.

Note

Check the flash size of your product in the respective user’s guide. For products with a ≥32MByte flash device, set the flash programmer to 4-Byte address mode.

If you do not have a flash programmer, use the update procedure described in the following section.

4.2 Programming of External BIOS Flash with CGUTIL

In this step, a functioning product of the same type and with the same BIOS flash size is used together with the evaluation carrier/MITX debug card to pre-program the external SPI flash device. The procedure is similar to the actual flash update you will see in chapter 5 “Onboard BIOS Flash Update Procedure”. We recommend a product with the same part number to program the external flash. This way, it is not possible to accidently program the wrong BIOS onto the working board.

1. Connect the necessary peripherals and power supply to the system (evaluation carrier + working module or working Mini-ITX board + debug card).
2. Insert the empty SPI flash into the socket and set the DIP switches to boot from on-module BIOS. Please refer to chapter 6 for the exact position.
3. Plug in the USB boot medium with FreeDos or UEFI shell containing the BIOS flash tool cgutlcmd and the BIOS binary file. Both files should be in the same directory.

4. Start the system and boot into the operating system on the USB stick.
5. Navigate to the folder where cgutlcmd and the BIOS binary are located.

Note

When using the UEFI shell to navigate to the files, you need to select the right file system first. To do this, enter "FSx:", where x stands for the number of the file system the shell gave to the USB stick.

6. Unlock the flash part by entering the following command:

   ```
   cgutlcmd bflash /eu
   ```

   If the flash part needs to be unlocked, the system will perform a power cycle in order to unlock it. This is necessary to do a full update in the next step. 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).

Note

Check the flash size of your product in the respective user's guide. For products with a ≥32MByte flash device, follow these additional steps:

a) ***During the power cycle of step 6, switch the ATX power supply off (G3) while the main power is off (S5).***

b) ***Set the DIP switches to boot from external BIOS.***

c) ***Turn the ATX power supply on (G3 --> S5).***

d) ***Set the DIP switches back to boot from on-module BIOS.***

e) ***Press the power button for five seconds, release the button and then briefly press it again. The system should turn on.***

f) ***Wait until the system finished booting.***

7. Navigate to the folder where cgutlcmd and the BIOS binary file are located and enter the following command:

   ```
   cgutlcmd bflash BIOSNAME.bin /efm /d
   ```

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

Note

The parameter "/efm" will force a full flash update (UEFI firmware + extended area) without doing an automatic reboot after the flash update is finished. Usually, it is sufficient to only use "/em" because the congatec system utility auto detects if a full update is necessary and skips it when not, thereby saving much time. However, it is safer to force the full update when an external update is done.

The parameter "/d" allows you to switch to another flash part, in order to program the external SPI flash device.

When using a product with a different BIOS than the defective one for the external update, the "/f" parameter is needed to program the BIOS. The "/f" parameters bypasses the built-in protection mechanism that only allows the user to program BIOS binary with the same 4 letter BIOS project name.

Please refer to AN01_BIOS_Update for more information about the different parameters used.

8. After the prompt tells you that you may switch to another flash part, set the DIP switches to boot from external BIOS.
9. Confirm by pressing any key, the update process will now start. Once completed, the message "BIOS successfully updated" will be displayed.
10. Turn of the system. Your external SPI flash has been successfully prepared.

Note

On some products, including the conga-xA5 (intel® Apollo Lake) product line, the SoC writes back information to the SPI flash during the first boot. This write-back will prevent other boards from booting with the same flash. Therefore, it is important to use the /efm parameter when programming the external SPI flash, to ensure the board does not reboot automatically after the update.

5 Onboard BIOS Flash Update Procedure

In this section, the pre-programmed SPI flash device is used to boot up the product and program the on-module BIOS flash.

1. Insert the pre-programmed SPI flash into the socket and set the DIP switch to boot from external BIOS. Refer to chapter 6 "External BIOS Flash Location" for the exact position.
2. Connect the necessary peripherals and power supply to the system (eval carrier + non-booting module or Mini-ITX board + debug card).
3. Plug in the USB boot medium with FreeDOS or UEFI shell containing the BIOS flash tool cgutlcmd and the BIOS binary file. Both files should be in the same directory.
4. Start the system and boot into the operating system on the USB stick.
5. Navigate to the folder where cgutlcmd and the BIOS binary are located.

Note

When using the UEFI shell in order to navigate to the files, you need to select the right file system first. To do this type "FSx:", where x stands for the number of the file system the UEFI shell gave to the USB stick.

6. Unlock the flash part by entering following command:

   ```
   cgutlcmd bflash /eu
   ```

   If the flash part needs to be unlocked, the system will perform a power cycle in order to unlock it. This is necessary to do a full update in the next step. 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).

7. Navigate to the folder where cgutlcmd and the BIOS binary are located and enter the following command:

   ```
   cgutlcmd bflash BIOSNAME.bin /ef /d
   ```

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

Note

The parameter "/ef" will force a full flash update (UEFI firmware + extended area). Usually, it is sufficient to only use "/e" because the congatec system utility auto detects if a full update is necessary and skips it when not, thereby saving much time. However, it is safer to force the full update when an external update is done. When the BIOS does not have an extended area, the tool will ignore this parameter.

The parameter "/d" allows you to switch to another flash part to program the external SPI flash device.

Refer to AN01_BIOS_Update for more information about the different parameters.

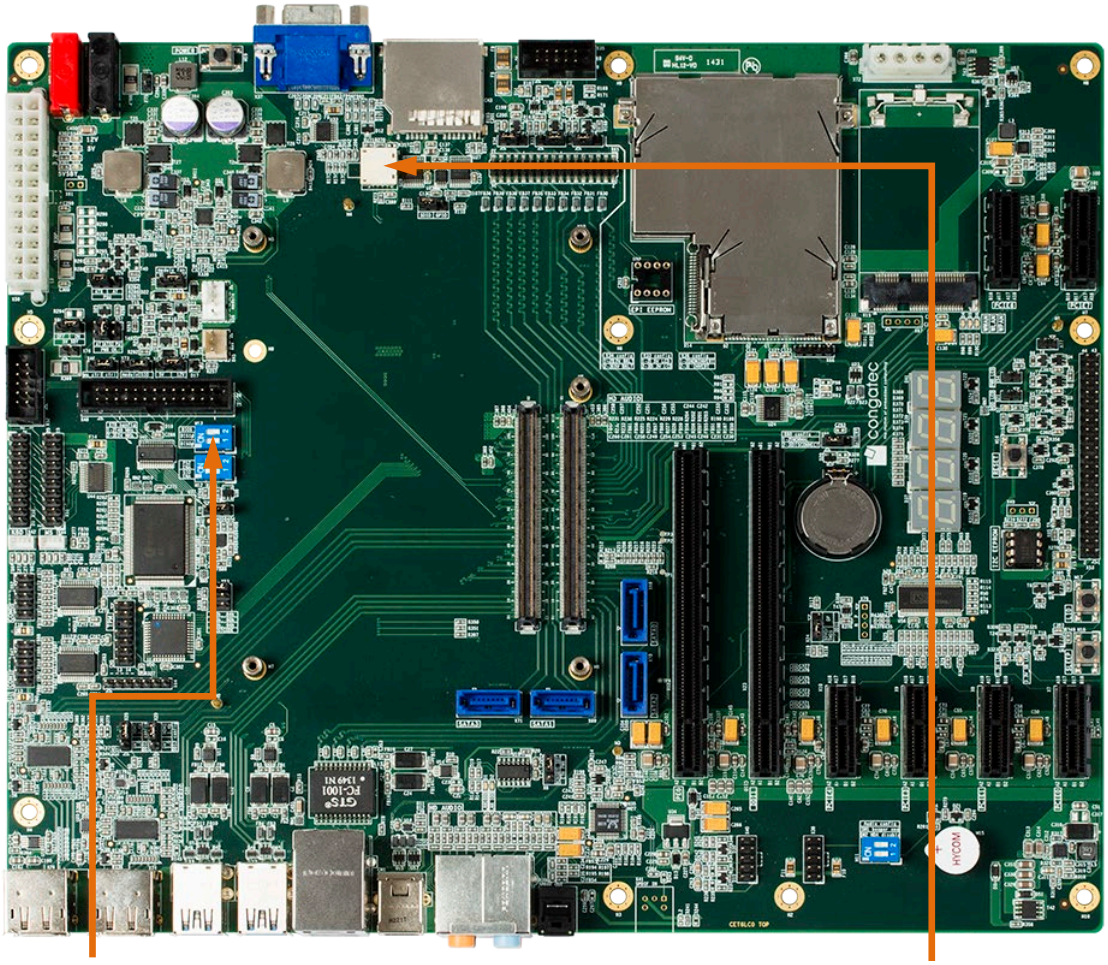
8. After the prompt tells you that you may switch to another flash part, switch to the onboard BIOS with the DIP switch.
9. Confirm by pressing any key to start the update process. Once completed, the message “BIOS successfully updated” will be displayed.
10. The system restarts. Your BIOS has been successfully updated and the product should be able to boot again.

Note

On some products, including the conga-xA5 (intel® Apollo Lake) product line, the SoC writes back information to the SPI flash during the first boot. This write-back will prevent other boards from booting with the same flash. Therefore, we recommend to prepare a new SPI flash for every board that needs to be recovered.

6 External BIOS Flash Location

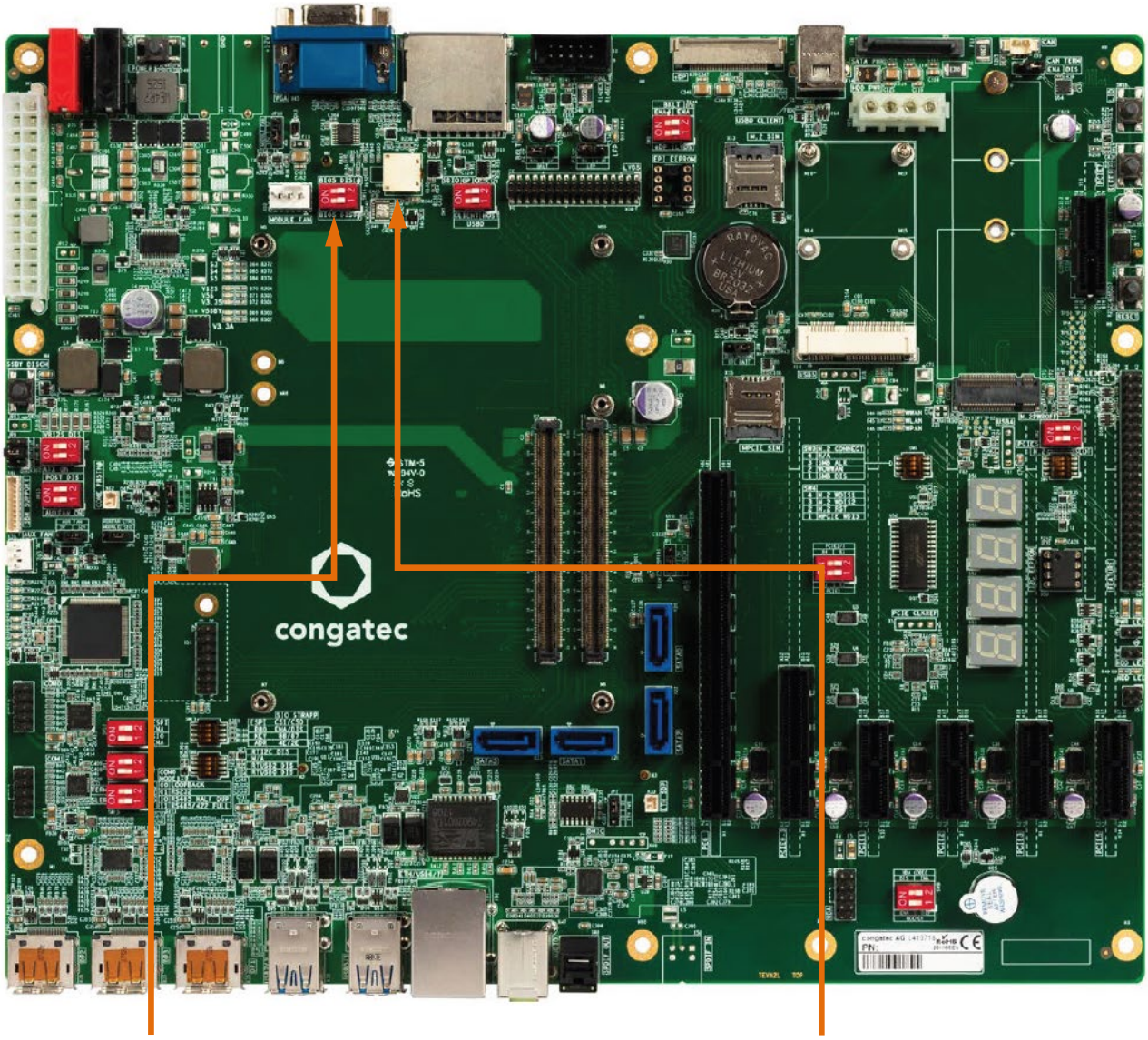
6.1 conga-TEVAL



External SPI flash socket SOIC8

DIP Switch M13		Configuration
SW1(DIS0#)	SW2(DIS1#)	
OFF	OFF	Boot from on-module BIOS
OFF	ON	Boot from external BIOS

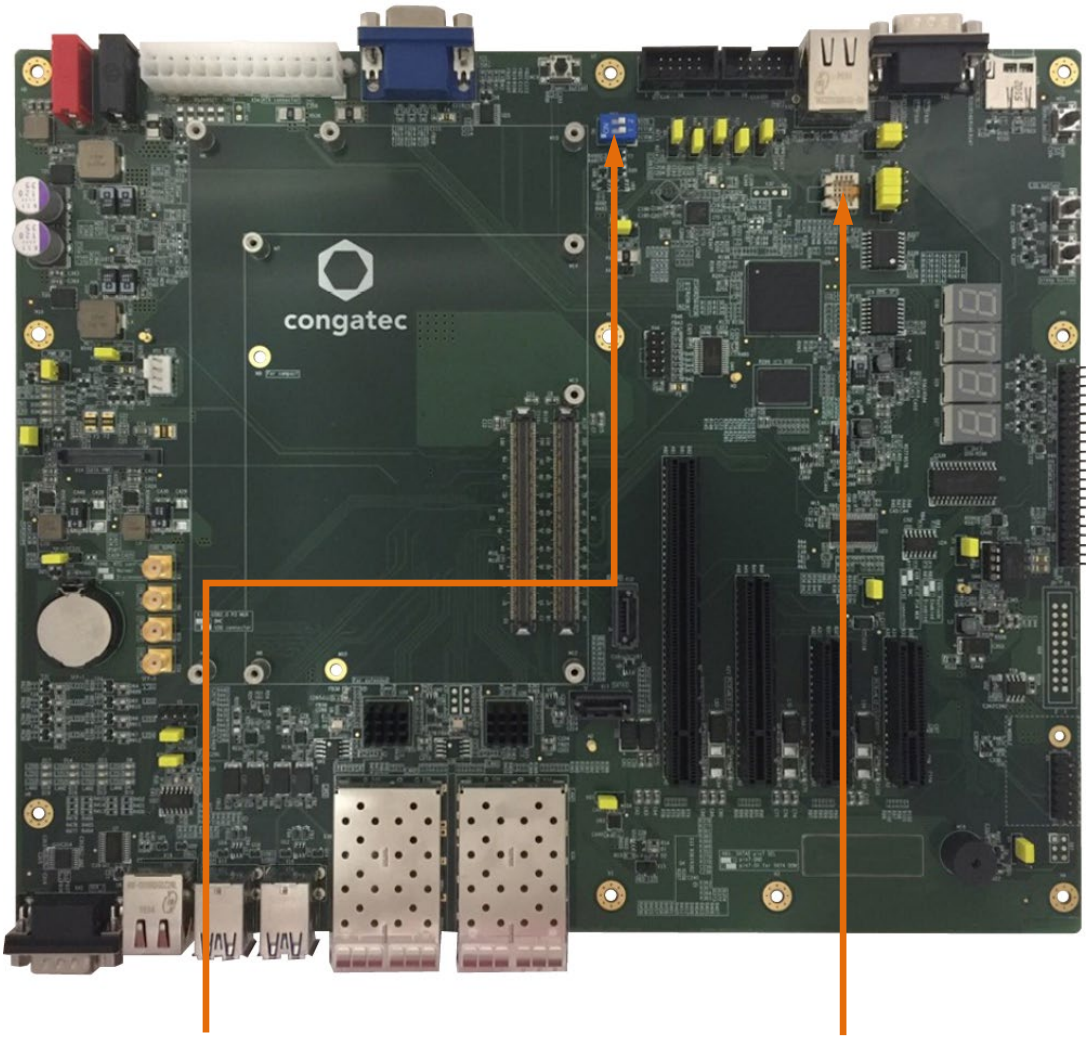
6.2 conga-TEVAL/COMe 3.0



External SPI flash socket SOIC8

DIP Switch SW14		Configuration
SW1(DIS0#)	SW2(DIS1#)	
OFF	OFF	Boot from on-module BIOS
OFF	ON	Boot from external BIOS

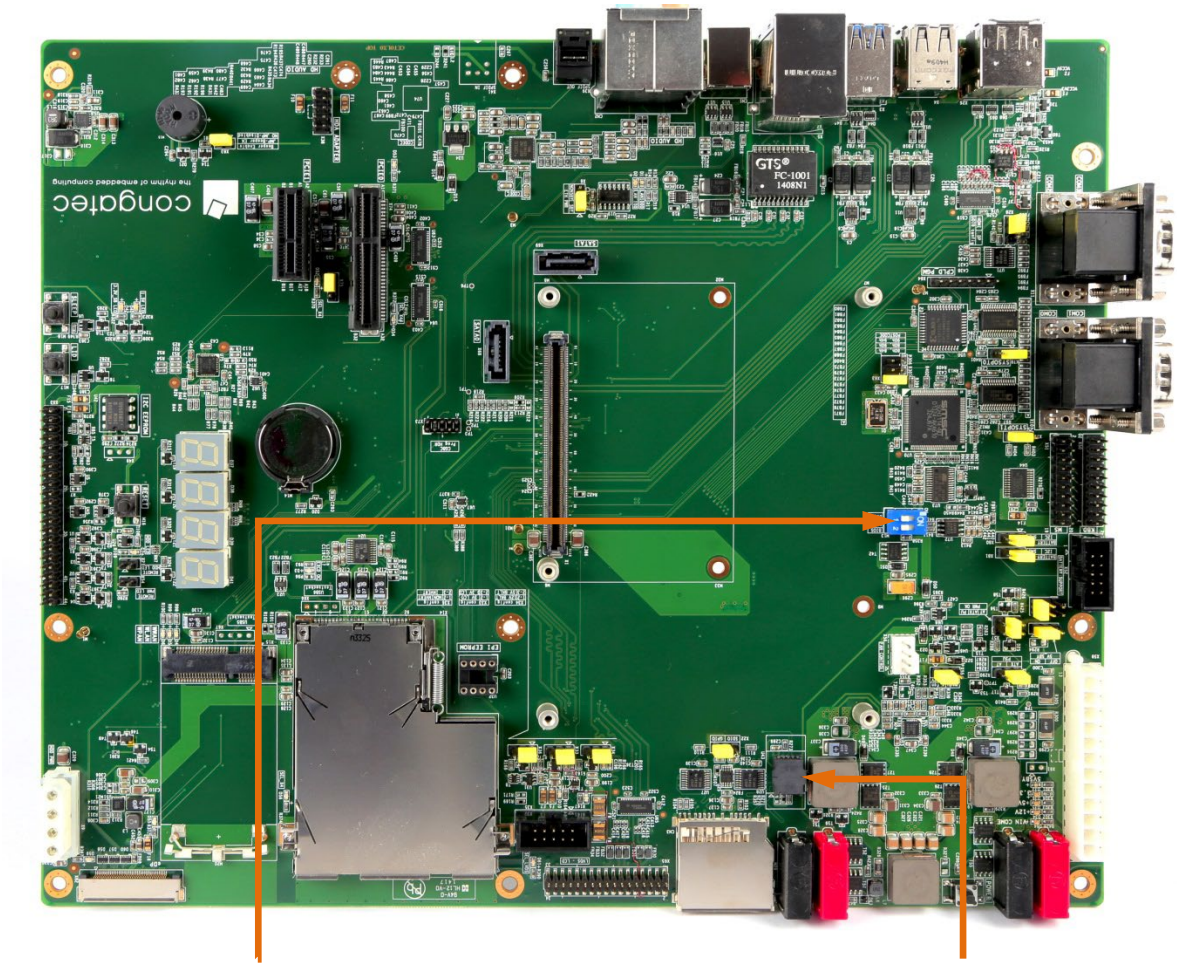
6.3 conga-X7EVAL



External SPI flash socket SOIC8

DIP Switch M13		Configuration
SW1(DIS0#)	SW2(DIS1#)	
OFF	OFF	Boot from on-module BIOS
OFF	ON	Boot from external BIOS

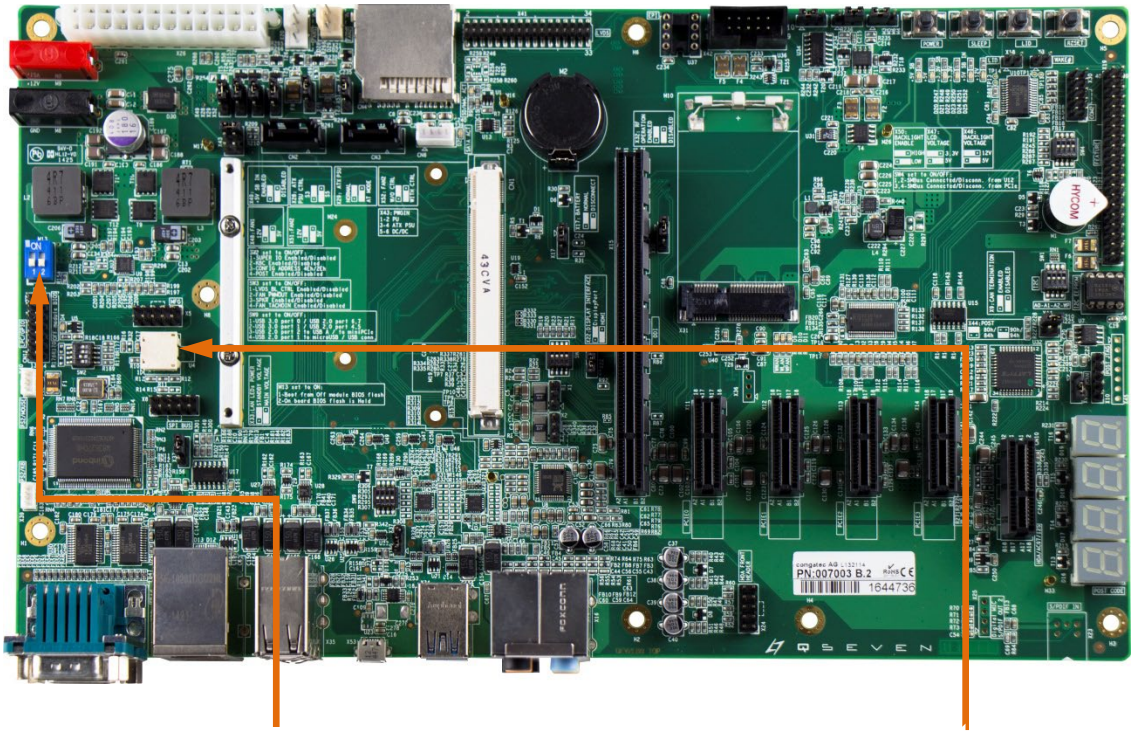
6.4 conga-MEVAL



External SPI flash socket SOIC8

DIP Switch M13		Configuration
SW1(DIS0#)	SW2(DIS1#)	
OFF	OFF	Boot from on-module BIOS
OFF	ON	Boot from external BIOS

6.5 conga-QEVAL/Qseven 2.0

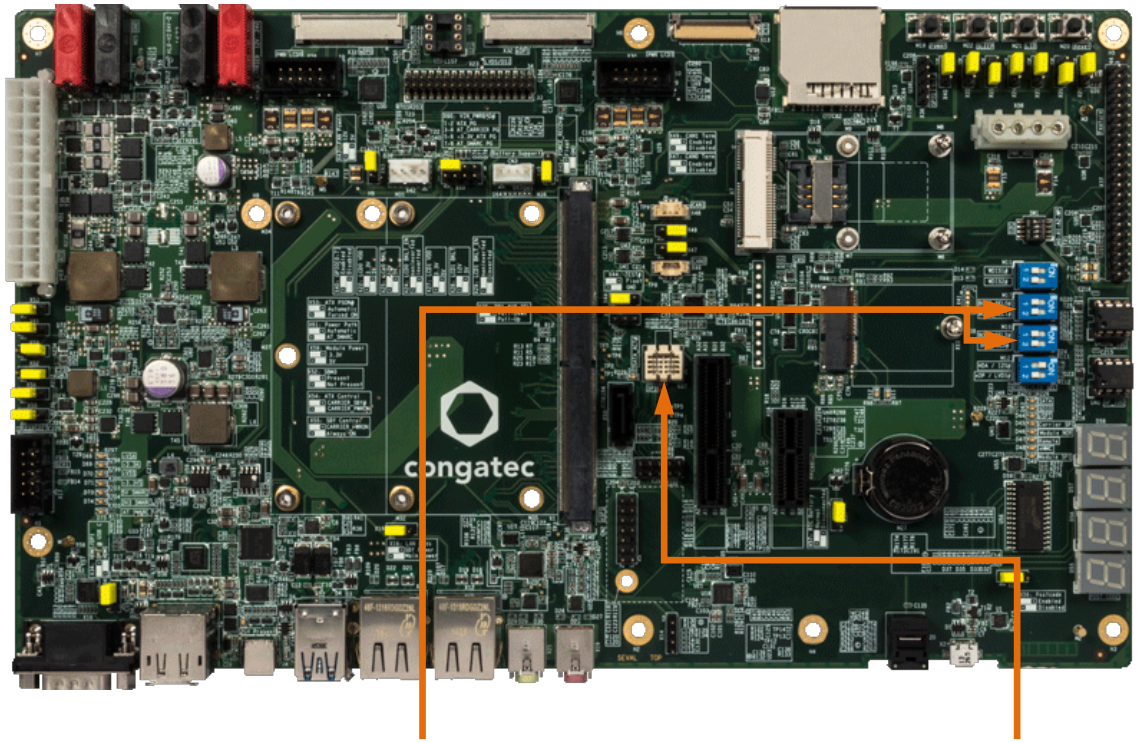


External SPI flash socket SOIC8

DIP Switch M13		Configuration
SW1	SW2	
OFF	OFF	Boot from on-module BIOS
ON	OFF	Boot from external BIOS

When the DIP switch is set to external the LED D4 is lit.

6.6 conga-SEVAL



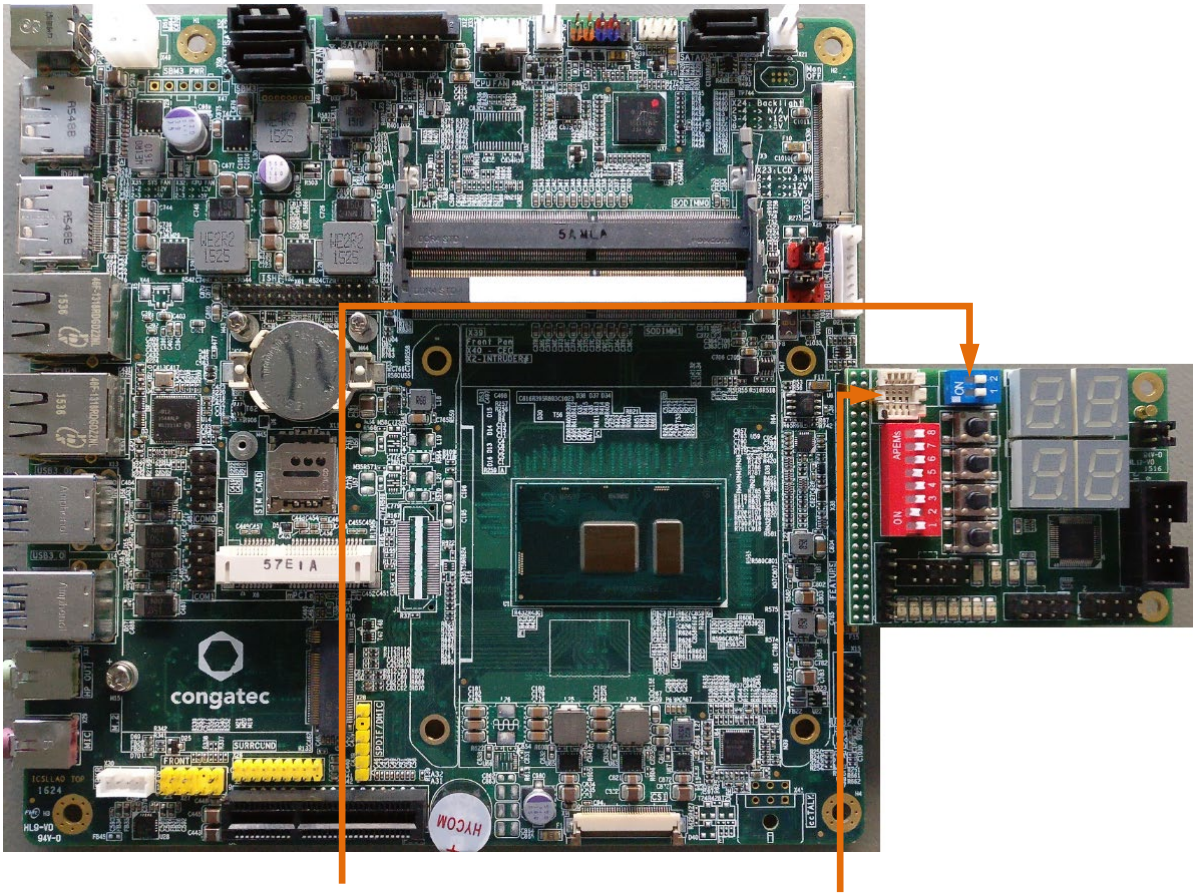
DIP Switch M17		DIP Switch M18	Configuration
SW1 (BOOT_SEL0#)	SW2 (BOOT_SEL1#)	SW1 (BOOT_SEL2#)	
OFF	OFF	OFF	Boot from on-module BIOS
OFF	OFF	ON	Boot from external BIOS

When the DIP switch is set to external, the LED D4 is lit.

Note

Given the limited availability of 1.8V-flash devices with ≥32Mbyte in SOIC8-packages, you might consider using a 1.8V WSON8-package. An appropriate adapter can be used for compatibility with the conga-SEVAL. For guidance on programming the flash device, refer to sections 4.1 and 4.2.

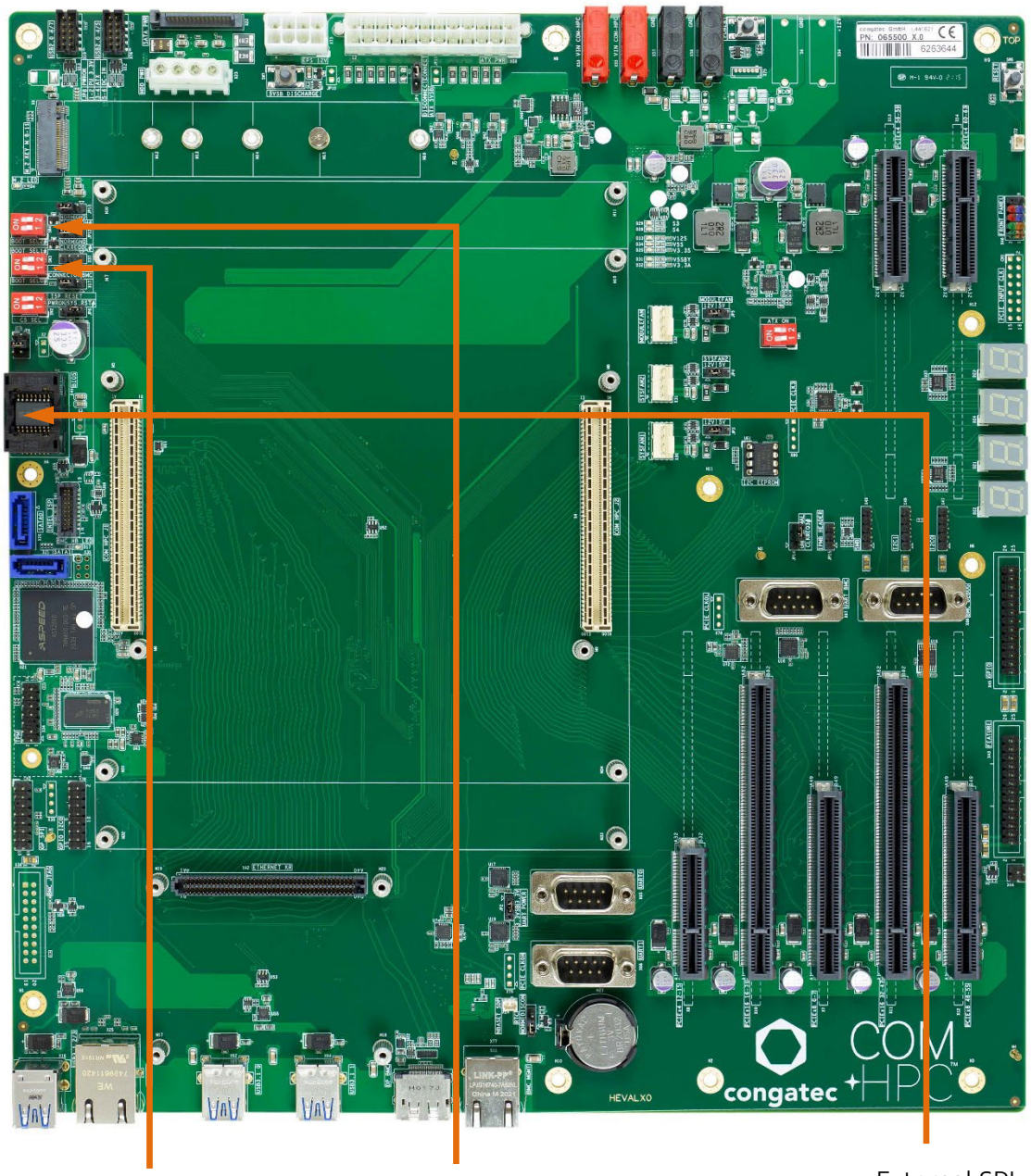
6.7 Mini ITX



External SPI flash socket SOIC8

DIP Switch M13		Configuration
SW1	SW2	
OFF	OFF	Boot from on-board BIOS
ON	OFF	Boot from external BIOS

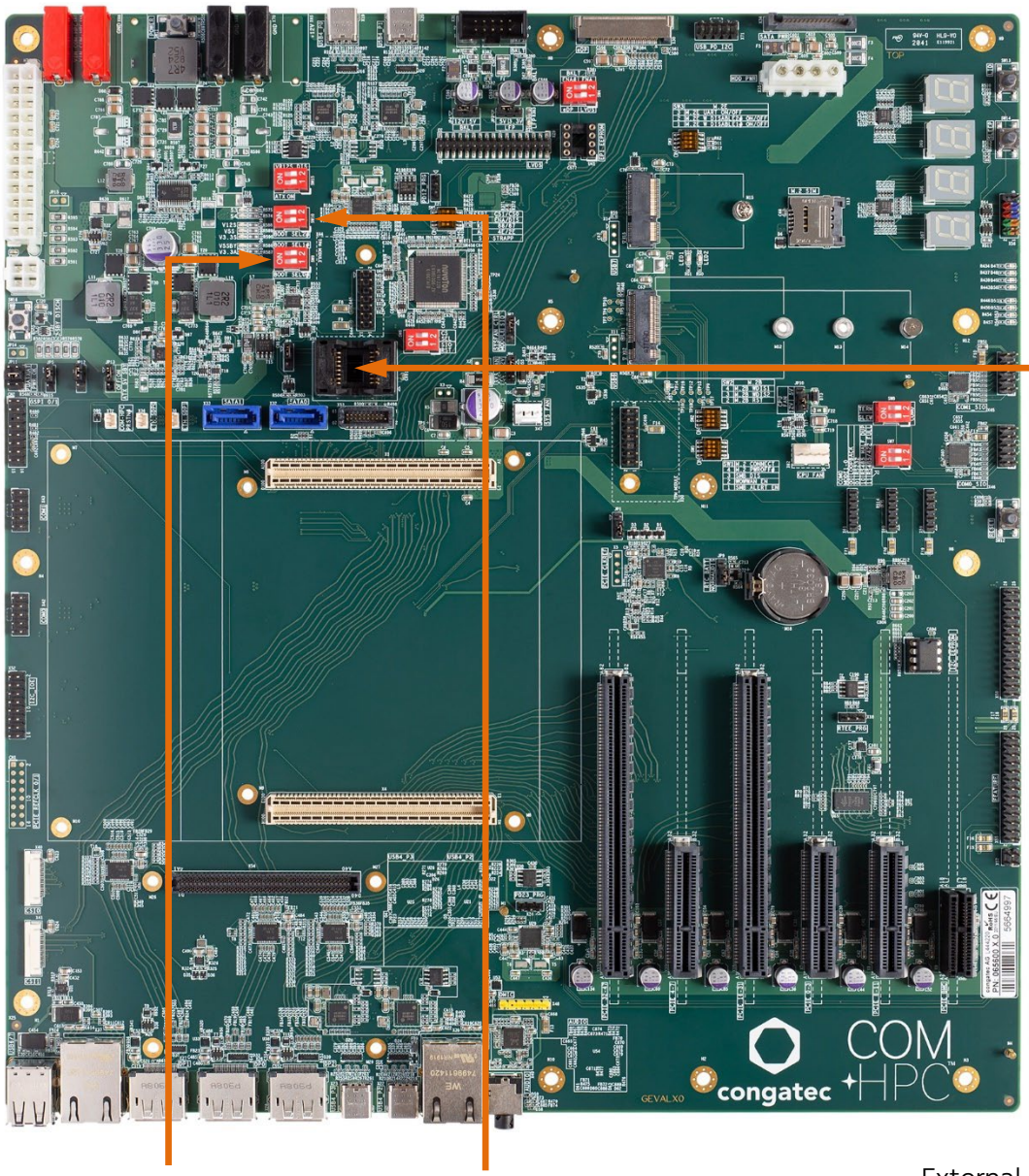
6.8 conga-HPC/EVAL-Server



External SPI flash socket SOIC16

DIP Switch SW3		DIP Switch SW4	Configuration
SW3.1 (BSEL0)	SW3.2 (BSEL1)	SW4.1 (BSEL2)	
OFF	OFF	OFF	Boot from on-module BIOS
ON	OFF	OFF	Boot from external BIOS

6.9 conga-HPC/EVAL-Client



DIP Switch SW9		DIP Switch SW10	Configuration
SW9.1 (BSEL0)	SW9.2 (BSEL1)	SW10.1 (BSEL2)	
OFF	OFF	OFF	Boot from on-module BIOS
ON	OFF	OFF	Boot from external BIOS