CoffeeLake Industrial

BIOS Release Document

Designed by Fujitsu

- D3633-S
- D3634-S
- D3641-S
- D3646-S

POSSIBILITIES START HERE kontron S&T Group

Content

Revision History:

Date	BIOS Version	Notes
18.02.2020	R1.8.0	Updated Release Notes with CVE information
17.02.2020	R1.8.0	Updated chapter 1.4
12.02.2020	R1.8.0	Added new BIOS version Changed whole document to Kontron design Reordered some chapters
17.07.2019	R1.7.0	Updated Known Restrictions (PEG slot mode)
27.06.2019	R1.7.0	Added new BIOS version
06.05.2019	R1.6.0	Added new BIOS version
30.11.2018	R1.3.0	Updated Known Restrictions and Limitations
26.11.2018	R1.3.0	Initial mass production release for D3634. Updated Known Restrictions and Limitations
12.11.2018	R1.3.0	Added new BIOS version (D3633, D3641, D3646)
18.09.2018	R1.2.0	Initial mass production release (D3633, D3641, D3646)

1. General Notes

- AMI Aptio V5.0.0.13

1.1 Released OS Versions

- MS Windows 10 (64bit)

1.2 BIOS Update Options

EFI Flash Update

Use ZIP-files for EFI-based BIOS Update

Copy content of the BIOS ZIP to any FAT32 formatted USB drive/stick. The files should be visible in following directories:

- EfiFlash.efi -> /EFI/FUJITSU
- Flash update files (e.g. .UPD) in root directory of USB stick.

Boot the system and choose “FUJITSU Update Utility” in F12 boot menu.

Please see the BIOS-Flash-Tools documentation for more information:
ftp://ftp.kontron.com/Services/Software_Tools/BIOS-Flash-Tools/

Windows Flash Update

Use Dxxx-xyz.DFI.$xe for Windows-based BIOS update
→ Rename file to *.exe after download and run exe-file from MS Windows

Auto BIOS Update

With Auto BIOS Update it is possible to check a Fujitsu server automatically to see if there is a new BIOS version for the system. For the update, no operating system or external storage medium is required. This feature must be enabled in BIOS Setup first.
For details on the Auto BIOS Update function please see the BIOS manual.

BIOS Recovery

Please see the BIOS-Flash-Tools documentation for more information:
ftp://ftp.kontron.com/Services/Software_Tools/BIOS-Flash-Tools/

Additional information

If you have any problems after a BIOS flash please try if “Load Optimized Default Values” (F3) in BIOS setup solves the problem.

1.3 FTP BIOS Folder

The released BIOS version is available here:

D363x-S:
ftp://ftp.kontron.com/Products/Motherboards/Industrial/D363x-S_Mini-ITX/BIOS_D363x/

D364x-S:
ftp://ftp.kontron.com/Products/Motherboards/Industrial/D364x-S/BIOS_D364x-S/

1.4 Modify BIOS Setup Settings and Defaults (Tool EditCMOS / BIOSSET) [updated]

BIOS settings can be modified by the Windows and Linux tool BIOSSET (Modify BIOS Setup Settings and Defaults). See BIOSSET tool help (parameter –h) for further details.

The tool is also described in our Manufacturing-Tools HowTo document:
ftp://ftp.kontron.com/Services/Software_Tools/Common-Mainboard-Tools/

1.5 What's about DOS support and where are the DOS tools?

Due to Intel's and Microsoft's decision, there is no "Legacy" OS support (CSM mode) implemented anymore. So only usage of UEFI operating systems is possible. We will provide the necessary tools and documentation for Windows and Linux.

Editcmos (DOS) -> Biosset (Windows and Linux)
EfiFlash.exe (DOS) -> Efiflash.efi (EFI environment) or Dskflash/Deskflash (Windows/Linux)
SMCO, LVDS tool, OEMIdent are also available for Windows and Linux.

ftp://ftp.kontron.com/Services/Software_Tools/Common-Mainboard-Tools/

1.6 Note: Customer Service Release BIOS

Besides the released BIOS versions there may be additional BIOS versions
(Customer Service Release BIOS = CSR BIOS) that solve specific customer problems.
Please note: These versions are available via OEM FTP only and they are not pre-installed ex factory.

2. BIOS R1.2.0

First released mass production BIOS for D3633-S, D3641-S and D3646-S

- Includes updated CPU microcode. Fix for Intel-SA-00115 (CVE2018-3639, CVE2018-3640)
  - 0x96 for CoffeeLake-S U-0
- Includes updated Intel ME version 12.0.6.1120
  - Fix for CVE-2018-3655, CVE-2018-3657, CVE-2018-3658, CVE-2018-3659, CVE -2018-3616

Known Issues and Limitations:

- No legacy OS support (UEFI only due to Intel restrictions)!

3. BIOS R1.3.0

First released mass production BIOS for D3634-S

Changes vs. previous released BIOS

- Updated CPU Microcode (0x9A) for CoffeeLake-S U-0
- Updated to Management Engine Firmware version 12.0.10.1127 (Fix for CVE-2018-3655)
- Feature: Implemented setup option for SERR# and PERR#. (Advanced > PCI Subsystem Configuration)
- Feature: Implemented setup option for eDP brightness. (Advanced > Embedded Display Port Configuration)
- Fixed: Some m.2 PCIe devices were not detected.
- Fixed: LVDS backlight enable polarity corrected.
- Fixed: Power Button=Disabled was not working. (Boot)
- Fixed: Default for C-States corrected to “disabled”.
- Fixed: Default for POST Beep corrected to “disabled”.
- Fixed: Corrected typo of PCI Slot number. (Advanced > PCI Subsystem Configuration)
- Fixed: Plugged memory module for "DIMM CHA1" not shown. (Main > System Information)

Known Issues and Limitations:

- No legacy OS support (UEFI only due to Intel restrictions)!
- Energy saving settings are not disabled completely (NativePCIe and NativeASPM are enabled)
- BIOS defaults not loaded if jumper is set to Recovery position without connecting a recovering image on USB stick.
- POST beep only works on internal buzzer, not from the internal frontpanel speaker.
- “System Power Limit” > “Custom System Power Limit” not working properly.
- D363x-S only: When updated from R1.2.0 the m.2 Slot is disabled by the setup option “WLAN + Bluetooth” (Advanced > Onboard Devices Configuration). If you want to use any m.2 device please change the option to “enabled” manually or just execute “Restore Defaults” (F3) (Save & Exit)

4. BIOS R1.6.0

Changes vs. previous released BIOS

- Integrated Fixes for PSIRT-TA-201810-007, PSIRT-TA-201810-004, PSIRT-TA-201901-002, CVE-2018-12201, CVE-2018-12202, CVE-2018-12203, CVE-2018-12204, CVE-2018-12205
- Updated CPU Microcode for CoffeeLake-S U-0
- Updated Intel Reference Code with support for 9th gen CPUs.
- Updated Power Management Integration for CFL Refresh (9th gen) CPU support.
- Updated to Management Engine Firmware version 12.0.30.1408
- Updated BMC Teutates Firmware (V058)
- Updated: Erase Disk Module
- Feature: Implemented new setup options:
- Advanced > CPU Configuration > “Intel® Speed Shift Technology”
- Advanced > Onboard Devices > “Mini PCIe WLAN”
- Power > “CPU TDP Limit” (see Technotes for details)
- [D364x-S only] Advanced > “Runtime Error Logging”
- Feature: Improved BIOS firmware update time (takes effect on upcoming updates).
- Feature: Disabled additional energy saving settings (NativePCIe and NativeASPM).
- Feature: Reduced boot time after AC recover with PCIe bifurcation mode (PEG slot mode).
- Fixed: USB Port Security “Enable used ports” is not working properly after S5 / Standby.
- Fixed: Loading BIOS default values via Recovery Jumper (without connected recovery image) not working.
- Fixed: POST beep only works on internal buzzer, not from the internal front panel speaker.
- Fixed: Only one MAC address in “System Information” shown,
- [D3634-S only] Fixed: Removed “PEG slot mode” setting. Not supported!
- [D363x-S only] Power > System Power Limit** > “Custom System Power Limit” not working properly.

**Setup Item will only appear if 12V PSU mode is active on mITX mainboard.

Known Issues and Limitations:

- No legacy OS support (UEFI only due to Intel restrictions)!
- D363x-S only: When updated from R1.2.0 the m.2 Slot is disabled by the setup option “WLAN + Bluetooth” (Advanced > Onboard Devices Configuration). If you want to use any m.2 device please change the option to “enabled” manually or just execute “Restore Defaults” (F3) (Save & Exit)
- Default value for “Intel ® Speed Shift Technology” (Hardware P-State control) had been changed to “Disabled”. This will only take effect, if you load “Optimized Defaults” after BIOS update.
- [D3641-S and D3646-S only] “PEG slot mode” setting in BIOS removed mistakenly. Will be re-added in next BIOS version!
- Some Linux distributions still use 32bit installer/bootloader, and therefore booting will cause hang or errors. In that case, please disable Advanced>PCI Subsystem Settings>”Above 4G Decoding”. A general description of this setting can be found in BIOS manual on OEM FTP site.
- BIOS downgrade to a version prior R1.6.0 is blocked due to security reasons and the support of 9th gen Intel CPUs!

5. BIOS R1.7.0

Changes vs. previous released BIOS

- Integrated Fixes for CVE-2018-12179, CVE-2018-12180, CVE-2018-12181, CVE-2019-0098, CVE-2019-0099, CVE-2019-0153, CVE-2019-0170, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130
- Updated CPU Microcode (0xB4) for CoffeeLake-S U-0 and (0xB8) for CoffeeLake-S R-0
- Updated to Management Engine Firmware version 12.0.35.1427
- Updated BMC Teutates Firmware (V059)
- Feature: BIOS option "CPU TDP Limit" is now available by default.
- Only for mainboards shipped with R1.7.0 or later!
- If BIOS was flashed from version <R1.7.0 setting can only be activated by system integrator tool “OEMIdent”
- Fixed: “PEG slot mode” setting integrated for the feature capable mainboards (D3633-S, D3641-S, D3646-S).
- Fixed: Linux boot was not possible under some circumstances.

Known Issues and Limitations:

- PEG slot mode is not working an all capable mainboards!
- No legacy OS support (UEFI only due to Intel restrictions)!
- D363x-S only: When updated from R1.2.0 the m.2 Slot is disabled by the setup option “WLAN + Bluetooth” (Advanced > Onboard Devices Configuration). If you want to use any m.2 device please change the option to “enabled” manually or just execute “Restore Defaults” (F3) (Save & Exit)
- Default value for “Intel ® Speed Shift Technology” (Hardware P-State control) had been changed to “Disabled”. This will only take effect, if you load “Optimized Defaults” after BIOS update.
- BIOS downgrade to a version prior R1.6.0 is blocked due to security reasons and the support of 9th gen Intel CPUs!

6. BIOS R1.8.0

Changes vs. previous released BIOS

- Intel IPU 2019 Q2 Security Update - Integrated Fixes for CVE-2019-14598, CVE-2019-0123 CVE-2019-0117, CVE-2019-0131, CVE-2019-0165, CVE-2019-0166, CVE-2019-0168, CVE-2019-0169, CVE-2019-11086, CVE-2019-11087, CVE-2019-11088, CVE-2019-11090, CVE-2019-11097, CVE-2019-11100, CVE-2019-11101, CVE-2019-11102, CVE-2019-11103, CVE-2019-11104, CVE-2019-11105, CVE-2019-11106, CVE-2019-11107, CVE-2019-11108, CVE-2019-11110, CVE-2019-11131, CVE-2019-11132, CVE-2019-11147, CVE-2019-11157, CVE-2019-0124 CVE-2019-0151 CVE-2019-0184, CVE-2019-11157
- Updated CPU Microcode for CoffeeLake-S U-0 (0xCA) and for CoffeeLake-S R-0 (0xCA)
- Updated to Management Engine Firmware version 12.0.49.1534
- Updated Intel i210 UEFI LAN driver – Improves POST boot time for i210/i350 based systems.
- Updated Intel Raid & RST UEFI driver – Fixes boot issues in RAID1, if one drive was removed.
- Fixed: “PEG slot mode” was not working at all capable mainboards.
- Fixed: Some miniPCIe devices on mPCIe slot were not working correctly.
- Feature: Reduced SMI to improve real time capability.
- Fixed: Windows Boot Manager was missing under some circumstances.
- Fixed: Changed BIOS Setup default value of “System Power Limit” (Power) was lost after CMOS battery was removed.
- Fixed: Drive size of disks with native 4k sectors was not shown correctly in BIOS setup.
- Fixed: MCE is sporadically shown for different banks during Linux boot.
- File transfer via serial port 1 improved.
- Fixed: Signals at serial port 1 were toggling during Windows boot.
- [D363x-S only] Fixed: Serial mPCIe adapter not fully working.
- [D364x-S only] Fixed: Implemented missing Setup Item IDs for serial ports.

Known Issues and Limitations:

- No legacy OS support (UEFI only due to Intel restrictions)!
- D363x-S only: When updated from R1.2.0 the m.2 Slot is disabled by the setup option “WLAN + Bluetooth” (Advanced > Onboard Devices Configuration). If you want to use any m.2 device please change the option to “enabled” manually or just execute “Restore Defaults” (F3) (Save & Exit)
- Default value for “Intel ® Speed Shift Technology” (Hardware P-State control) had been changed to “Disabled”. This will only take effect, if you load “Optimized Defaults” after BIOS update.
- BIOS downgrade to a version prior R1.6.0 is blocked due to security reasons and the support of 9th gen Intel CPUs!

Global Headquarters

Kontron S&T AG

Lise-Meitner-Str. 3-5
86156 Augsburg, Germany
Tel.: +49 821 4086 0
Fax: +49 821 4086 111
info@kontron.com
www.kontron.com