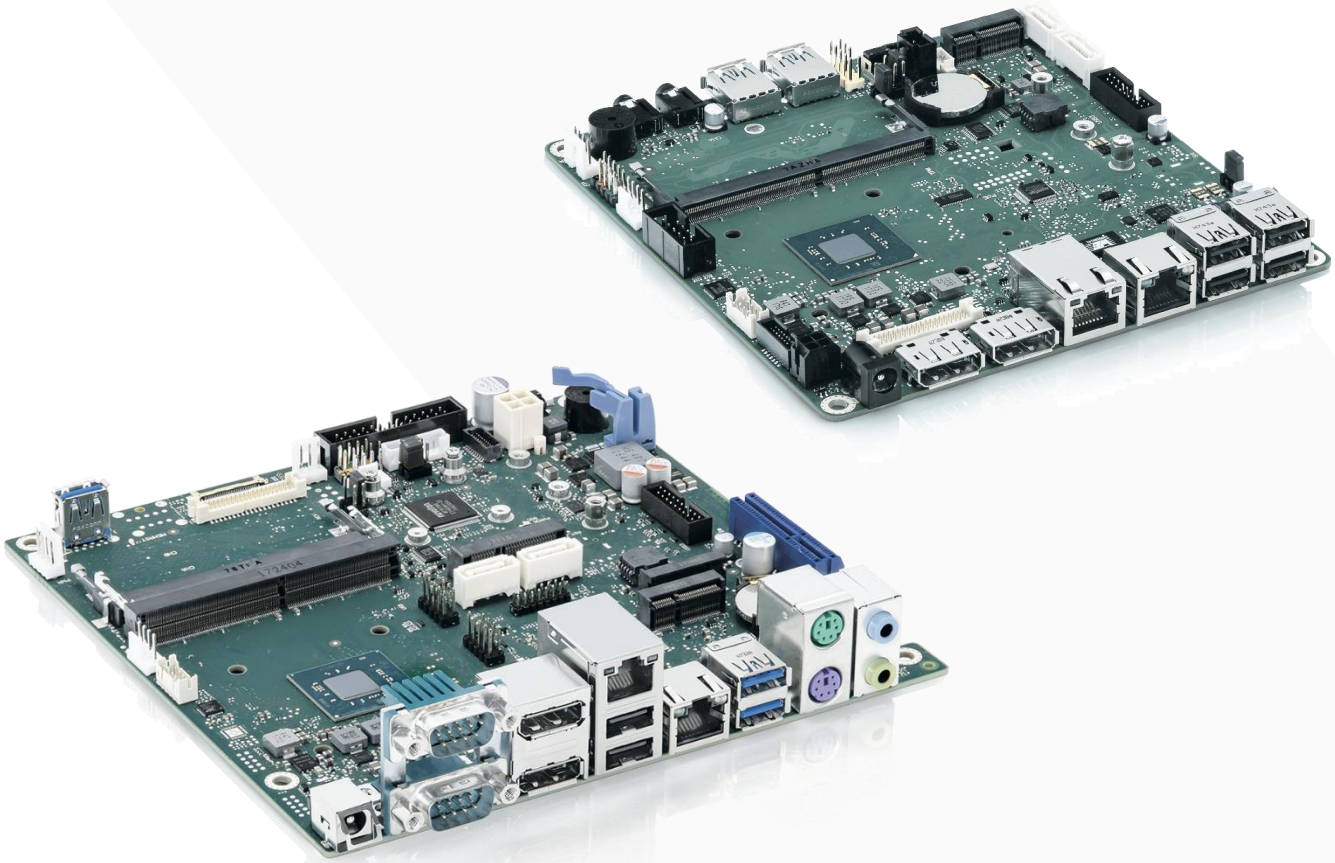
Bios Release Document

GeminiLake SoC mITX and mSTX series



GeminiLake Industrial Series

- D3543-S
- D3544-S

kontron

Content

Revision History:

Date	BIOS Version	Notes
26.09.2023	R1.15.0	Added new BIOS version
28.02.2022	R1.14.0	Added new BIOS version
05.05.2021	R1.13.0	Added new BIOS version
05.08.2020	R1.12.0	Added new BIOS version Changed whole document to Kontron design Reordered some chapters
19.11.2019	R1.11.0	Updated fix description
11.11.2019	R1.11.0	Added new BIOS version
18.06.2019	R1.10.0	Updated Restrictions and Known Issues
14.06.2019	R1.10.0	Added new BIOS version
04.04.2019	R1.8.0	Added new BIOS version
19.11.2018	R1.7.0	Added new BIOS version
23.10.2018	R1.6.0	Added new BIOS version (R1.6.0). Consolidated D3543-S and D3544-S BIOS release documentation.

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:

D3543-S:
ftp://ftp.kontron.com/Products/Motherboards/Industrial/D3543-S_Mini-ITX/BIOS_D3543-S/

D3544-S:
ftp://ftp.kontron.com/Products/Motherboards/Industrial/D3544-S_Mini-STX/BIOS_D3544-S/

1.4 Modify BIOS Setup Settings and Defaults (Tool BIOSSET)

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), Gabisettings (EFI environment)
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 R1.5.0

Since BIOS version R1.6.0 we have consolidated BIOS-Info document for D3543-S and D3544-S.

You can find the revision history for previous released BIOS versions within the “Previous_Versions” subfolder:

- D3543-S: ftp://ftp.kontron.com/Products/Motherboards/Industrial/D3543-S_Mini-ITX/BIOS_D3543-S/Previous_Versions/
- D3544-S: ftp://ftp.kontron.com/Products/Motherboards/Industrial/D3544-S_Mini-STX/BIOS_D3544-S/Previous_Versions/

3. BIOS R1.6.0

Changes vs. previous released BIOS

Important Note: BIOS downgrade to R1.5.0 or earlier is not possible (and therefore blocked) due to Intel security policy!

- Updated to CPU Microcode 0x28. Fix for Intel-SA-00115 (CVE2018-3639, CVE2018-3640)
- Updated: Intel Trusted Execution Engine (CVE-2018-3657, CVE-2018-3658 ,CVE-2018-3659, CVE-2018-3655, CVE-2018-3616)
- Fixed: If both LVDS and DisplayPort are connected, no output on LVDS display.
- Fixed: Faulty boot behavior without monitor connected.
- Feature: Always use internal graphics, if no external graphics card is present. Preserves the user from locking out themselves from the system.
- Feature: Enable SoC serial ports (D3543-S: COM3 + COM4 | D3544-S: COM2)
    - Note: For these COM ports, an additional driver is required: ftp://ftp.kontron.com/Products/Motherboards/Industrial/D3544-S_Mini-STX/Drivers_D3544/ -> "10_optional_SoC-COM-Driver…."
- Feature: Enhance Setup Password Severity Options (Standard, Strong, Stringent)
- Feature: New PCIe setup items: [Slot n Enable/Disable] and [Slot n Link Speed] **[D3543-Sx only]**
- Feature: Added support for "LVDS BacklightApp" (Windows) **[D3543-Sx only]**
    - BacklightApp and API can be downloaded from our FTP server: ftp://ftp.kontron.com/Services/Software_Tools/LVDS_Brightness-Tool/

Known Issues and Limitations:

- No legacy OS support (UEFI only due to Intel restrictions)!
- BIOS Recovery flash not working as expected: BIOS Recovery flash process is running in endless loop until Recovery jumper is removed.
    - Best practice: If you hear a "double beep" at the beginning of the Recovery process, remove the jumper immediately. After the process is done, the mainboard will boot in normal mode.
- BIOS Recovery flash not supported by all USB ports: Prefer USB 3.0 ports for BIOS Recovery flash.
- [PCIe Subsystem Settings] > "PCI Express Slot 1" string is wrong. Correct: "PCI Express Slot mPCIe"

4. BIOS R1.7.0

Changes vs. previous released BIOS

- Updated: System Monitoring Characteristics.
- Fixed: System fails to boot with some memory modules.
- Fixed: Defaults for RS-485 (PCH GPIO) changed.
- Fixed: If COM port full duplex mode selected in BIOS setup, half duplex was configured (and vice versa).
- Fixed: LVDS backlight polarity control does not work.

Known Issues and Limitations:

- BIOS downgrade to R1.5.0 or earlier is not possible (and therefore blocked) due to Intel security policy!
- No legacy OS support (UEFI only due to Intel restrictions)!
- BIOS Recovery flash not working as expected: BIOS Recovery flash process is running in endless loop until Recovery jumper is removed.
    - Best practice: If you hear a “double beep” at the beginning of the Recovery process, remove the jumper immediately. After the process is done, the mainboard will boot in normal mode.
- BIOS Recovery flash not supported by all USB ports: Prefer USB 3.0 ports for BIOS Recovery flash.
- [PCIe Subsystem Settings] > “PCI Express Slot 1” string is wrong. Correct: “PCI Express Slot mPCIe”

5. BIOS R1.8.0

Changes vs. previous released BIOS

- Fixed: Under some circumstances, power button potentially was disabled completely.
- Fixed: eLux boot time was very long.

Known Issues and Limitations:

- BIOS downgrade to R1.5.0 or earlier is not possible (and therefore blocked) due to Intel security policy!
- No legacy OS support (UEFI only due to Intel restrictions)!
- BIOS Recovery flash not working as expected: BIOS Recovery flash process is running in endless loop until Recovery jumper is removed.
    - Best practice: If you hear a “double beep” at the beginning of the Recovery process, remove the jumper immediately. After the process is done, the mainboard will boot in normal mode.
- BIOS Recovery flash not supported by all USB ports: Prefer USB 3.0 ports for BIOS Recovery flash.
- [PCIe Subsystem Settings] > “PCI Express Slot 1” string is wrong. Correct: “PCI Express Slot mPCIe”
- [added] RS422 Half-Duplex mode currently not supported. Only receiving is working, no RS422 transmit on COM1.
- [added] Selection/booting a UEFI shell on USB stick in POST boot menu (F12) is not possible, if the Fujitsu Update Utility is detected from BIOS in /EFI/FUJITSU/Efiflash.efi.

6. BIOS R1.10.0

Changes vs. previous released BIOS

- Integrated Fixes for PSIRT-TA-201810-004, CVE-2018-12188 CVE-2018-12189 CVE-2018-12190 CVE-2018-12191 CVE-2018-12192 CVE-2018-12199 CVE-2018-12198 CVE-2018-12200 CVE-2018-12187 CVE-2018-12196 CVE-2018-12185, CVE-2018-12201, CVE-2018-12202, CVE-2018-12203, CVE-2018-12204, CVE-2018-12205
- Updated to CPU Microcode 0x2C
- Updated system monitoring characteristics
- Feature: Implemented "eDP to DP Support" (requires graphics driver ≥ V25.20.100.6582!).
- Feature: Location definition of internal USB pin header connectors now possible.
- Feature: Erase Disk is now enabled by default.
- Fixed: RS422 Half-Duplex mode is now working.
- Fixed: Removed doubled entry "Serial Port Enabled/Disabled" in BIOS setup.
- Fixed: Removed value “IO=3F8;IRQ=4” for COM1.
- Fixed: Trusted Computing menu displayed only when TPM license set.
- Fixed: Sporadic blue screen in Windows 10 RS5 IOT occurred.

Known Issues and Limitations:

- BIOS downgrade to R1.5.0 or earlier is not possible (and therefore blocked) due to Intel security policy!
- No legacy OS support (UEFI only due to Intel restrictions)!
- **Before installing BIOS > R1.8.0** for an LVDS-based system, the MS Windows graphics driver has to be updated to driver revision **≥** V25.20.100.6582! Otherwise LVDS output may fail after BIOS update!
- BIOS Recovery flash not working as expected: BIOS Recovery flash process is running in endless loop until Recovery jumper is removed.
    - Best practice: If you hear a “double beep” at the beginning of the Recovery process, remove the jumper immediately. After the process is done, the mainboard will boot in normal mode.
- BIOS Recovery flash not supported by all USB ports: Prefer USB 3.0 ports for BIOS Recovery flash.
- [PCIe Subsystem Settings] > “PCI Express Slot 1” string is wrong. Correct: “PCI Express Slot mPCIe”
- Selection/booting a UEFI shell on USB stick in POST boot menu (F12) is not possible, if the Fujitsu Update Utility is detected from BIOS in /EFI/FUJITSU/Efiflash.efi.

7. BIOS R1.11.0

Changes vs. previous released BIOS

- Updated to CPU Microcode 0x32
- Feature (D3543-Sx only): Added BIOS option for USB3 header (internal / external).
- Feature: Renamed BIOS Setup option "Internal Port n" to "Internal USB Header n".
- Fixed: Windows Boot Manager was missing under some circumstances.
- Fixed: Realtek WLAN RTL8821 responds with all "0xEA" in PCI CFG-Space registers, when plugged in the Mini-Pci slot.
- Fixed (D3543-Sx only): BIOS-integrated Diagnostic Tool was missing.
- Fixed: Implemented missing Setup Item IDs for serial ports.
- Fixed: COM Port 2 configuration in BIOS Setup changed, when COM 1 was changed.

Known Issues and Limitations:

- BIOS downgrade to R1.5.0 or earlier is not possible (and therefore blocked) due to Intel security policy!
- No legacy OS support (UEFI only due to Intel restrictions)!
- **Before installing BIOS > R1.8.0** for an LVDS-based system, the MS Windows graphics driver has to be updated to driver revision **≥** V25.20.100.6582! Otherwise LVDS output may fail after BIOS update!
- BIOS Recovery flash not working as expected: BIOS Recovery flash process is running in endless loop until Recovery jumper is removed.
    - Best practice: If you hear a “double beep” at the beginning of the Recovery process, remove the jumper immediately. After the process is done, the mainboard will boot in normal mode.
- BIOS Recovery flash not supported by all USB ports: Prefer USB 3.0 ports for BIOS Recovery flash.
- [PCIe Subsystem Settings] > “PCI Express Slot 1” string is wrong. Correct: “PCI Express Slot mPCIe”
- Selection/booting a UEFI shell on USB stick in POST boot menu (F12) is not possible, if the Fujitsu Update Utility is detected from BIOS in /EFI/FUJITSU/Efiflash.efi.

8. BIOS R1.12.0

Changes vs. previous released BIOS

- Updated Intel i210 UEFI LAN driver – Improves POST boot time for i210/i350 based systems.
- Info: Replaced Fujitsu logos with Kontron logos.
    - Diagnostic screen logo (Quiet Boot = Disabled) takes immediate effect after BIOS update.
    - Silent boot logo will not be replaced during BIOS updates in field (logo preserve function). It just takes effect on newly produced or RMA processed motherboards. To activate the logo on "old" motherboards, you can use the Logo file from: ftp://ftp.kontron.com/Services/Software_Tools/Miscellaneous/
        - Kontron_QuietBootBIOSLogo.zip

Known Issues and Limitations:

- BIOS downgrade to R1.5.0 or earlier is not possible (and therefore blocked) due to Intel security policy!
- No legacy OS support (UEFI only due to Intel restrictions)!
- **Before installing BIOS > R1.8.0** for an LVDS-based system, the MS Windows graphics driver has to be updated to driver revision ≥ V25.20.100.6582! Otherwise LVDS output may fail after BIOS update!
- BIOS Recovery flash not working as expected: BIOS Recovery flash process is running in endless loop until Recovery jumper is removed.
    - Best practice: If you hear a "double beep" at the beginning of the Recovery process, remove the jumper immediately. After the process is done, the mainboard will boot in normal mode.
- BIOS Recovery flash not supported by all USB ports: Prefer USB 3.0 ports for BIOS Recovery flash.
- [PCIe Subsystem Settings] > "PCI Express Slot 1" string is wrong. Correct: "PCI Express Slot mPCIe"
- Selection/booting a UEFI shell on USB stick in POST boot menu (F12) is not possible, if the Fujitsu Update Utility is detected from BIOS in /EFI/FUJITSU/Efiflash.efi.

9. BIOS R1.13.0

Changes vs. previous released BIOS

Important Note: BIOS downgrade to R1.12.0 or earlier is not possible (and therefore blocked) due to Intel security policy!

- Intel IPU2020.1 Security Update – Integrated Fixes for CVE-2020-0531, -0532, -0533, -0534, -0535, -0536, -0537, -0538, -0539, -0540, -0541, -0542, -0545, -0566, -0586, -0594, -0595, -0596, -0597, -8674
- Intel IPU2020.2 Security Update – Integrated Fixes for CVE-2020-8694, -8695, -8705, -8744, -8745, -8746, -8747, -8749, -8750, -8751, -8752, -8753, -8754, -8755, -8761, -12297, -12303, -12304, -12354, -12355, -12356Integrated fixes for INTEL-SA-00347 (CVE-2020-0570, CVE-2020-0571)
- Updated CPU Microcode (0x34)
- Updated to Intel Trusted Execution Engine (4.0.30.1386v2)
- Fixed: Auto BIOS Update failed under some circumstances.
- Fixed: Background of new Kontron silent boot logo (POST, Windows) is not “pure” black.
- Info: BIOS Feature “Auto BIOS Update” not working with the Fujitsu default server address. The server infrastructure at Fujitsu does not contain data for Kontron Extended Lifecycle and Industrial motherboards anymore. Therefore, the address was removed. Kontron will not provide an update server. Custom TFTP server solutions are still possible.

Known Issues and Limitations:

- BIOS downgrade to R1.12.0 or earlier blocked due to Intel security policy!
- No legacy OS support (UEFI only due to Intel restrictions)!
- **Before installing BIOS > R1.8.0** for an LVDS-based system, the MS Windows graphics driver has to be updated to driver revision **≥** V25.20.100.6582! Otherwise, LVDS output may fail after BIOS update!
- BIOS Recovery flash not working as expected: BIOS Recovery flash process is running in endless loop until Recovery jumper is removed.
    - Best practice: If you hear a “double beep” at the beginning of the Recovery process, remove the jumper immediately. After the process is done, the mainboard will boot in normal mode.
- BIOS Recovery flash not supported by all USB ports: Prefer USB 3.0 ports for BIOS Recovery flash.
- [PCIe Subsystem Settings] > “PCI Express Slot 1” string is wrong. Correct: “PCI Express Slot mPCIe”
- Selection/booting a UEFI shell on USB stick in POST boot menu (F12) is not possible, if the Fujitsu Update Utility is detected from BIOS in /EFI/FUJITSU/Efiflash.efi.

10. BIOS R1.14.0

Changes vs. previous released BIOS

Important Note: BIOS downgrade to R1.13.0 or earlier is not possible (and therefore blocked). No need to update to this BIOS version if you have standard boards with LVDS controller available.

- Fixed: Black screen hang during POST on boards with reduced BOM (without LVDS controller) and enabled “LVDS Support” in BIOS setup.
  - This BIOS version will be automatically flashed ex-factory on “no LVDS” D354x-Sx boards.
  - Since enabled LVDS support could leads to a black screen on these D354x-Sx boards (Only replacing the BIOS chip can recover boards from this state) we blocked the downgrade to any previous BIOS version.

Known Issues and Limitations:

- BIOS downgrade to R1.13.0 or earlier blocked due to Intel security policy!
- No legacy OS support (UEFI only due to Intel restrictions)!
- **Before installing BIOS > R1.8.0** for an LVDS-based system, the MS Windows graphics driver has to be updated to driver revision **≥** V25.20.100.6582! Otherwise, LVDS output may fail after BIOS update!
- BIOS Recovery flash not working as expected: BIOS Recovery flash process is running in endless loop until Recovery jumper is removed.
  - Best practice: If you hear a “double beep” at the beginning of the Recovery process, remove the jumper immediately. After the process is done, the mainboard will boot in normal mode.
- BIOS Recovery flash not supported by all USB ports: Prefer USB 3.0 ports for BIOS Recovery flash.
- [PCIe Subsystem Settings] > “PCI Express Slot 1” string is wrong. Correct: “PCI Express Slot mPCIe”
- Selection/booting a UEFI shell on USB stick in POST boot menu (F12) is not possible, if the Fujitsu Update Utility is detected from BIOS in /EFI/FUJITSU/Efiflash.efi.

11. BIOS R1.15.0 [new]

Changes vs. previous released BIOS

- Security: AMI SA50119, 2022.2 Platform Update, CVE-2021-33060, CVE-2022-21233, CVE-2022-26074
- Security: AMI SA50097, 2021.2 Platform Update, CVE-2021-0060, -0091, -0092, -0093, -0099, -0103, -0107, -0111, -0114, -0115, -0116, -0117, -0118, -0119, -0124, -0125, -0127, -0145, -0146, -0147, -0156, -0157, -0158
- Security: Updated CPU Microcode (0x3C)
- Fixed: OemIdent corrupts link to SMBIOS Type 3 within Type 2 structure.
- Fixed: PCI Subsystem help is displayed half in Japanese and half in English.
- Fixed: Possible Memory Exception while BIOS Update in POST
- (Feature: Add additional verb table for Tempo Audio Codec)
    - Info: Tempo Audio controller models of D354x not released.

Known Issues and Limitations:

- BIOS downgrade to R1.13.0 or earlier blocked due to Intel security policy!
- No legacy OS support (UEFI only due to Intel restrictions)!
- Before installing BIOS > R1.8.0 for an LVDS-based system, the MS Windows graphics driver has to be updated to driver revision ≥ V25.20.100.6582! Otherwise, LVDS output may fail after BIOS update!
- BIOS Recovery flash not working as expected: BIOS Recovery flash process is running in endless loop until Recovery jumper is removed.
    - Best practice: If you hear a “double beep” at the beginning of the Recovery process, remove the jumper immediately. After the process is done, the mainboard will boot in normal mode.
- BIOS Recovery flash not supported by all USB ports: Prefer USB 3.0 ports for BIOS Recovery flash.
- [PCIe Subsystem Settings] > “PCI Express Slot 1” string is wrong. Correct: “PCI Express Slot mPCIe”
- Selection/booting a UEFI shell on USB stick in POST boot menu (F12) is not possible, if the Fujitsu Update Utility is detected from BIOS in /EFI/FUJITSU/Efiflash.efi.

About Kontron

Kontron is a global leader in IoT/Embedded Computing Technology (ECT). Kontron offers individual solutions in the areas of Internet of Things (IoT) and Industry 4.0 through a combined portfolio of hardware, software and services. With its standard and customized products based on highly reliable state-of-the-art technologies, Kontron provides secure and innovative applications for a wide variety of industries. As a result, customers benefit from accelerated time-to-market, lower total cost of ownership, extended product lifecycles and the best fully integrated applications.

For more information, please visit: www.kontron.com

Global Headquarters

Kontron Europe GmbH

Gutenbergstraße 2
85737 Ismaning, Germany
Tel.: + 49 821 4086 0
Fax: + 821 4086 111
pcmb-sales@kontron.com

Copyright © 2023 Kontron. All rights reserved. All data is for information purposes only and not guaranteed for legal purposes. Information has been carefully checked and is believed to be accurate; however, no responsibility is assumed for inaccuracies. Kontron and the Kontron logo and all other trademarks or registered trademarks are the property of their respective owners and are recognized. Specifications are subject to change without notice.