SIEMENS

SIMATIC

Industrial PC Firmware/BIOS Description SIMATIC IPC427E, IPC477E

Operating Instructions

07/2020

A5E50262994-AA

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E50262994-AA
Ⓟ 08/2020 Subject to change

Important information

Basic knowledge requirements

This firmware / BIOS description is intended for the following qualified personnel:

- Programmers and testers who commission the device themselves and connect it to an automation system.
- Service and maintenance technicians who install enhancements or conduct fault analysis.

A solid background in personal computers is required to understand this manual. General knowledge in the field automation control engineering is recommended.

Scope of validity

This firmware/BIOS description applies to the following SIMATIC IPCs:

- SIMATIC IPC427E
- SIMATIC IPC477E

History

The following versions of this firmware/BIOS description have been published previously:

Edition	Comment
07/2020	First Edition

Firmware/BIOS

The firmware (BIOS) is located in a FLASH block on the motherboard.

The firmware selection menu can be opened after the device has been started. You can then configure the firmware settings of your device.

Change firmware settings

The firmware settings are preset for working with the included software. You should only change the default firmware settings if technical changes to your device require other settings.

NOTICE
Malfunctions can occur with running software CPU If a PC firmware/BIOS update is being performed while a SIMATIC software controller, such as a SIMATIC WinAC, is running, the software CPU can malfunction, resulting in communication interruptions or failures, among other things. Other actions that put a heavy load on the PC hardware, for example, running hardware tests such as benchmarks, can result in malfunctions of the software CPU. Do not run a firmware/BIOS update or other actions that would put a heavy load on the hardware during operation of a software CPU. Switch the software CPU to "STOP" before you run a firmware/BIOS update or perform other critical actions.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit (http://www.siemens.com/industrialsecurity).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under (http://www.siemens.com/industrialsecurity).

Disclaimer for third-party software updates

This product includes third-party software. Siemens AG only provides a warranty for updates/patches of the third-party software, if these have been distributed as part of a Siemens software update service contract or officially released by Siemens AG. Otherwise, updates/patches are undertaken at your own risk. You can find more information about our Software Update Service offer on the Internet at Software Update Service (http://www.automation.siemens.com/mcms/automation-software/en/software-update-service).

Table of contents

Using the firmware selection menu 1

1.1 Open firmware selection menu

Procedure

1. Switch on the device or restart the device.

   Note

   The following message appears briefly after the device is switched on:

   `Press ESC for boot options`

2. Immediately after switching on the device, press the <Esc> button and hold it down.

Result

The "Main Page" opens with the Firmware selection menu options (Page 8).

1.2 Firmware selection menu options

The number of available options in the firmware selection menu depends on your device version.

The following options are available:

Option	Function
Continue	Exit firmware selection menu Continue the boot procedure.
Boot Manager	Specify the boot media from which to start, for example: • Drive • USB stick
Device Management	Start device manager for UEFI boot media.
Boot From File	Boot from an *.EFI file.
Secure Boot	Configure device startup in "Secure Boot Modus".
SCU	Start firmware configuration menu.
BIOS Update	Perform BIOS update. You can find more detailed information under "Update firmware (Page 36)".

Configure firmware

2

2.1 Starting the Setup Utility

You configure important firmware settings of your device using the firmware configuration menu "Setup Utility".

Procedure

1. Open the firmware selection menu (Page 8).
2. Select the "SCU" option on the "Main Page" with the keyboard arrow keys.
3. Confirm your selection with the <Return> button.

2.2 Keyboard inputs in Setup Utility

Button	Function
<F1>	Call help function.
<F5> or <F6>	Change firmware settings. The <F5> key is used to take the previous setting possibility or value. The <F6> key is used to take the next setting possibility or value.
<F9>	Load Optimal Defaults: The firmware settings are reset to the safe default values. The delivery state is restored. **NOTICE**: All current firmware settings are overwritten.
<F10>	Exit Saving Changes: All changes are saved. The device is restarted with the changed firmware settings.
<Return>	A submenu previously selected with the arrow keys opens. The value of a firmware setting previously selected with the arrow keys can be changed.
[←] [→]	Navigate to a tab.
[↑] [↓]	Navigate to a submenu or a firmware setting. Confirm your selection with the <Return> button.
<Esc>	A submenu or tab or the Setup Utility is exited. If the Setup Utility is closed after the confirmation prompt, changes to the firmware settings are discarded.

2.3 "Main" tab

2.3.1 "Main tab" level

Calling "Main" tab

Select: "Setup Utility (Page 9)" > "Main".

Device information

You can find important device information at the top of the "Main" tab.

Device information	Explanation
SIMATIC	Device version.
BIOS Version	Current firmware version.
BIOS Number	Article number of the current firmware version.
CPU Type	CPU type.
Cache RAM	L2 cache size total.
Total Memory	Total memory size.
CPU Speed	CPU speed.
CPU Stepping	CPU version.
Number Of Processors	Number of processor cores. Number of threads.
Microcode Rev	Microcode version.
PCH Rev / SKU	Platform Controller Hub (PCH) version.
VBIOS Ver	Version of the video BIOS.
Intel ME Version / SKU	Version of the Intel® Management Engine (ME).
CPB Ver	Version of the Siemens Command Parameter Block (CPB).
SIO Ver	Version of the Super IO firmware.
NVRAM Ver	Version of the NVRAM.

Calling "System Time" and "System Date"

Date and time settings.

Select: "Setup Utility (Page 9)" > "Main" > "System Time" and "System Date".

Firmware setting	Explanation
System Time	Set current device time in the format [Hour:Minute:Second].
System Date	Set current device date in the format [Month/Day/Year].

Key functions for setting the numeric time and date values

Button	Function
<Return>	Switch between the setting options within a firmware setting, e.g. from hour to minute.
[+] [-]	Increase or decrease desired value.
[0] - [9]	Enter desired value.

2.4 "Advanced" tab

2.4.1 "Boot Configuration"

Basic display and input options during the boot procedure

Calling "Boot Configuration"

Select: "Setup Utility (Page 9)" > "Advanced" > "Boot Configuration".

Firmware setting	Value	Setting in delivery state IPC427E IPC477E	Meaning
Numlock	Off		Numerical keypad is switched off after starting the device.
	On	x	Numerical keypad is switched on off after starting the device.
POST Errors	Never halt on errors		Boot procedure is continued when errors occur.
	Halt on all errors		Boot procedure is interrupted when errors occur.
	All without keyboard	x	Boot procedure is interrupted when errors occur, except keyboard errors.
	All without kb/ smart		The boot procedure is canceled when errors occur, except for keyboard errors and S.M.A.R.T. errors (self-monitoring, analysis and reporting technology) which can occur with the storage media.

2.4.2 "Peripheral Configuration"

Configuration of the interfaces.

Calling "Peripheral Configuration"

Select: "Setup Utility (Page 9)" > "Advanced" > "Peripheral Configuration".

Firmware setting	Value	Setting in delivery state IPC427E IPC477E	Meaning
Internal COM 1 (only if COM 1 available in the hardware)	Enabled	x	Configuration of COM1 is enabled
	Disabled		Configuration of COM1 is disabled
• **Base I/O Address** (only if COM 1 available in the hardware)	2E8		Configure start address of COM1
	2F8		
	3E8		
	3F8	x	
• **Interrupt** (only if COM 1 available in the hardware)	IRQ3		Configure interrupt address of COM1
	IRQ4	x	
• **Transceiver Mode** (only if COM 1 available in the hardware)	Transceiver Loopback		Run COM1 in loopback mode
	RS232	x	Run COM1 as RS232 interface
	RS485 Half Duplex		Run COM1 as RS485 interface (with half duplex)
	RS485/422 Full Duplex		Run COM1 as RS485/422 interface (with full duplex)
Internal COM 2 (only if COM 2 available in the hardware)	Disabled	x	Configuration of COM2 is enabled
	Enabled		Configuration of COM2 is disabled
• **Base I/O Address** (only if COM 2 available in the hardware)	2E8		Configure start address of COM2
	2F8	x	
	3E8		
	3F8		
• **Interrupt** (only if COM 2 available in the hardware)	IRQ3	x	Configure interrupt address of COM2
	IRQ4		
• **Transceiver Mode** (only if COM 2 available in the hardware)	Transceiver Loopback		Run COM2 in loopback mode
	RS232	x	Run COM2 as RS232 interface
	RS485 Half Duplex		Run COM2 as RS485 interface (with half duplex)
	RS485/422 Full Duplex		Run COM2 as RS485/422 interface (with full duplex)
Onboard Ethernet 1 (LAN 1, X1 P1)	Disabled		The onboard Ethernet interface "X1 P1" is disabled.
	Enabled	x	The onboard Ethernet interface "X1 P1" is enabled.

Firmware setting	Value	Setting in delivery state IPC427E IPC477E	Meaning
Onboard Ethernet 1 Adresse	Shows the MAC address of Ethernet 1 (LAN 1, X1 P1)		
Onboard Ethernet 2 (LAN 2, X2 P1)	Disabled		The onboard Ethernet interface "X2 P1" is disabled.
	Enabled	x	The onboard Ethernet interface "X2 P1" is enabled.
Onboard Ethernet 2 Adresse	Shows the MAC address of Ethernet 2 (LAN 2, X2 P1)		
Onboard Ethernet 3 (LAN 3, X3 P1)	Disabled		The onboard Ethernet interface "X3 P1" is disabled.
	Enabled	x	The onboard Ethernet interface "X3 P1" is enabled.
Onboard Ethernet 3 Adresse	Shows the MAC address of Ethernet 3 (LAN 3, X3 P1)		
USB Port 1 (X61)	Enabled	x	USB port 1 (X61) is enabled.
USB Port 2 (X65)	Disabled		USB port 2 (X60) is disabled.
	Enabled	x	USB port 2 (X60) is enabled.
USB Port 3 (X63)	Disabled		USB port 3 (X63) is disabled.
	Enabled	x	USB port 3 (X63) is enabled.
USB Port 4 (X62)	Disabled		USB port 4 (X62) is disabled.
	Enabled	x	USB port 4 (X62) is enabled.
USB Port 10 (Internal Port)	Disabled		USB port 10 (Internal Port) is disabled.
	Enabled	x	USB port 10 (Internal Port) is enabled.

2.4.3 "SATA Configuration"

Calling "SATA Configuration"

Select: "Setup Utility (Page 9)" > "Advanced" > "SATA Configuration".

Here you will find information about (depending on the device type, only a subset of these SATA ports may be visible):

- Serial ATA Port 0
- Serial ATA Port 2
- Serial ATA Port 3

2.4.4 "System Agent (SA) Configuration"

2.4.4.1 "Graphics Configuration"

Calling "Graphics Configuration"

Select: "Setup Utility (Page 9)" > "Advanced" > "System Agent (SA) Configuration" > "Graphics Configuration".

Firmware setting	Value	Setting in delivery state IPC427E IPC477E	Meaning
Primary Display	Auto	x	During the boot procedure, the system automatically detects whether the device has a graphics card. Messages during the boot procedure are then issued via the graphics card. If no graphics card is available, messages are generated during the boot process via the integrated onboard graphics interface (Internal Graphics Device = IGFX).
	IGFX		Messages are output exclusively via the integrated onboard graphics interface (Internal Graphics Device = IGFX) during the boot process.
	PCI		During the boot procedure, the system automatically detects whether the device has a PCIe graphics card. Messages during the boot procedure are then issued via the PEG graphics card. If no PCIe graphics card is available, messages are generated during the boot process via the integrated onboard graphics interface (Internal Graphics Device = IGFX).
Primary IGFX Boot Display	VBIOS Default	x	Information about the integrated onboard graphics interface (Internal Graphics Device = IGFX) is provided by the "Display Port" like the value defined for VBIOS.
	Internal Display		Information about the integrated onboard graphics interface (Internal Graphics Device = IGFX) is provided by the internal display. (only available on IPC477E)
	DPP (0x71)		Information about the integrated onboard graphics interface (Internal Graphics Device = IGFX) is provided by the "Display Port" DPP (0x71).
	DPP (0x70)		Information about the integrated onboard graphics interface (Internal Graphics Device = IGFX) is provided by the "Display Port" DPP (0x70).

2.4.4.2 "PCIe Port Configuration"

The following information applies to the following PCIe slots (depending on the device type and device configuration, only a subset of these PCIe slots may be visible):

- PCIe-Slot 0:1:1 (x4 Slot)

Calling "PCIe Port Configuration"

Select: "Setup Utility (Page 9)" > "Advanced" > "System Agent (SA) Configuration" > "PCIe Port Configuration".

Firmware setting	Value	Setting in delivery state IPC427E IPC477E	Meaning
Max Link Speed for PCIe slot #	Auto	x	For **PCIe slot #** , the maximum speed is set automatically or set to Gen1, Gen2 or Gen3.
	Gen1		
	Gen2		
	Gen3		

2.4.4.3 Level: "System Agent (SA) Configuration"

Calling "System Agent (SA) Configuration"

Select: "Setup Utility (Page 9)" > "Advanced" > "System Agent (SA) Configuration".

Firmware setting	Value	Setting in delivery state IPC427E IPC477E	Meaning
VT-d	Disabled		Hardware support for shared use of input/output devices across multiple virtual machines (VT-d; Intel® Virtualization Technology for Directed I/O) is disabled.
	Enabled	x	Hardware support for shared use of input/output devices across multiple virtual machines (VT-d; Intel® Virtualization Technology for Directed I/O) is enabled.

2.4.5 "Active Management Technology Support"

Calling "Active Management Technology Support"

Select: "Setup Usability (Page 9)" > "Advanced" > "Active Management Technology Support".

Firmware setting	Value	Setting in delivery state	Meaning
		IPC427E IPC477E	
Intel AMT Configuration Screens	Disabled	x	Active Management Technology BIOS Extension is enabled.
	Enabled		Active Management Technology BIOS Extension is disabled.
Un-Configure ME	Disabled	x	The settings for "Intel AMT Configuration Screens" must be retained.
	Enabled		The settings for "Intel AMT Configuration Screens" must be reconfigured.
USB Configure	Disabled	x	The USB configuration (USB Provisioning) from Intel® Active Management Technology (iAMT) is disabled.
	Enabled		The USB configuration (USB Provisioning) from Intel® Active Management Technology (iAMT) is enabled.

2.4.6 "Memory Configuration"

Calling "Memory Configuration"

Select: "Setup Utility (Page 9)" > "Advanced" > "Memory Configuration".

Firmware setting	Value	Setting in delivery state	Meaning
		IPC427E IPC477E	
Max TOLUD	Dynamic		The maximum value of TOLUD (Top Of Low Usable DRAM) is set. With the "Dynamic" setting, TOLUD is automatically adjusted based on the longest MMIO length of the installed graphics controller.
	1 GB		
	1.25 GB		
	1.5 GB		
	1.75 GB		
	2 GB		
	2.25 GB		
	2.5 GB		
	2.75 GB		
	3 GB	x	

2.4.7 Level: "Advanced" tab

Calling "Advanced"

Select: "Setup Utility (Page 9)" > "Advanced".

Firmware setting	Value	Setting in delivery state IPC427E IPC477E	Meaning
HPET - HPET Support	Disabled		The high-precision event timer for multimedia HPET (High Precision Event Timer) is disabled.
	Enabled	x	The high-precision event timer for multimedia HPET (High Precision Event Timer) is enabled.

2.5 "Security" tab

2.5.1 Level: "Security" tab

Calling "Security" tab

Select: "Setup Utility (Page 9)" > "Security".

Firmware setting	Value	Setting in delivery state IPC427E IPC477E	Meaning
TPM Availability (only if TPM is present in the hardware)	Available	x	The TPM (Trusted Platform Module) is visible in the operating system.
	Hidden		The TPM (Trusted Platform Module) is not visible in the operating system.
TPM Operation (only if TPM is present in the hardware)	No Operation	x	The status of the TPM (Trusted Platform Module) is not changed.
	Enable		The status of the TPM (Trusted Platform Module) is changed dependent on the selected action.
Clear TPM	Deletes the initialization of the TPM block.		
Password Management Interface	Enabled	x	The interface for password configuration is enabled. The password settings can be configured via the software. You need the current password to make changes.
	Disabled		The interface for password configuration is disabled. The password settings can only be configured via the firmware settings.

Firmware setting	Value	Setting in delivery state IPC427E IPC477E	Meaning
Set Supervisor Password			Here you can set a general password for full access to the firmware settings. A password prompt then appears before the firmware is opened. After correct entry of the general password, it can be changed by entering a new one. If no password is entered and only the <Return> key is pressed, the configured general password is deleted, thereby disabling the password prompt again. **NOTICE**: If you lose the general password that you defined during firmware setup, the device must be reset by the manufacturer. • Make a note of the general password and keep it in a safe place. • Protect the general password from unauthorized access.
• **Power on Password** (only if a "Supervisor Password" was set up)	Enabled		A password prompt is displayed for every boot procedure. The general password or a user password must be entered.
	Disabled	x	A password prompt appears only when the setup utility is opened. The general password or a user password must be entered.
• **User Access Level** (only if a "Supervisor Password" was set up)	View Only		Only read access to Setup utility is permitted. Firmware settings cannot be changed.
	Limited		Restricted write access to Setup utility is permitted. Only certain firmware settings can be changed.
	Full	x	Unrestricted write access to the Setup utility is permitted. All firmware settings except the general password (Supervisor Password) can be changed.
• **User Boot Manager Access** (only if a "Supervisor Password" was set up)	Disabled		A user password is sufficient to start the Boot Manager.
	Enabled	x	

Firmware setting	Value	Setting in delivery state IPC427E IPC477E	Meaning
Set User Password			Here you can set a user password for limited access to the firmware settings. After correct entry of the user password, it can be changed by entering a new one. If no password is entered and only the <Return> key is pressed, the configured user password is deleted.
• **Clear User Password** (only if a "User Password" was set up)			Here you can delete the user password.

2.6 "Power" tab

2.6.1 "CPU Configuration"

Calling "CPU Configuration"

Select: "Setup Utility (Page 9)" > "Power" > "CPU Configuration".

CPU Type	CPU type.
ID	CPU ID
CPU Speed	CPU speed.
L1 Data Cache	L1 data cache size (size per processor core x number of processor cores).
L1 Instruktion Cache	L1 instruction cache size (size per processor core x number of processor cores).
L2 Cache	L2 cache size (size per processor core x number of processor cores).
L3 Cache	L3 cache size.
L4 Cache eDRAM	L4 cache eDRAM size.
VMX	Indicates whether Intel (VMX) Virtualization Technology is supported by the processor.
SMX/TXT	Indicates whether SMX/TXT is supported by the processor.

Firmware setting	**Value**	**Setting in delivery state**	**Meaning**
		IPC427E **IPC477E**	
SW Guard Extensions (SGX)	Disabled		The use of Software Guard Extensions (SG) is disabled.
	Enabled		The use of Software Guard Extensions (SG) is enabled.
	Software Controlled	x	The use of Software Guard Extensions (SG) is controlled by the software.
Select Owner EPOCH input type	No Change in Owner EPOCHs	x	The EPOCH values are not changed.
	Change to New Random Owner EPOCHs		The EPOCH values are changed to randomly generated values. After creating new EPOCH values using "Change to New Random Owner EPOCHs", the selection is reset to "No Change in Owner EPOCH" to ensure that the EPOCH values remain the same in all Sx states.
Intel (VMX) Virtualization Technology	Disabled		The virtualization functionality of Intel® is locked.
	Enabled	x	The virtualization functionality of Intel® is released. VMM systems (virtual machine monitor) can use the processor support for virtualization purposes (virtual machine extensions VMX) and additional performance features of the Vanderpool Technology hardware (VT).

Firmware setting	Value	Setting in delivery state IPC427E IPC477E	Meaning
Active Processor Cores	All	x	All cores of the processor are active and used.
	1		Number of processor cores used provided they do not exceed the actual number of cores. The remaining processor cores are inactive and are hidden from the operating system. This can resolve certain problems with software.
	2		
	3		
Hyper-Threading	Disabled		Hyper-Threading technology is disabled.
	Enabled	x	Hyper-Threading technology is enabled.
AES	Disabled		The secure encryption method AES (Advanced Encryption Standard) is not supported by hardware.
	Enabled	x	The secure encryption method AES (Advanced Encryption Standard) is supported by hardware. Encryption and decryption are accelerated.

2.6.2 "Power & Performance"

2.6.2.1 "CPU - Power Management Control"

Calling "CPU - Power Management Control"

Select: "Setup Utility (Page 9)" > "Power" > "Power & Performance" > "CPU - Power Management Control".

Firmware setting	Value	Setting in delivery state IPC427E IPC477E	Meaning
CPU Power Level	Performance Optimized		Setting the high performance for CPU and Graphics at the same time. The maximum CPU power consumption is 25 W.
	Standard	x	The CPU clock is dynamically limited with maximum 3D graphics performance. The maximum CPU power consumption is 17 W.
	Temperature Optimized		Setting for lowest power consumption. The CPU clock is limited at a higher load. The maximum power consumption of the CPU is 12 W.
	Determinism Optimized		Same as standard, but additionally optimized for deterministic operation with constant CPU frequency.
Intel(R) SpeedStep(tm)	Disabled		The use of more than two frequency ranges is disabled.
	Enabled	x [1)]	The use of more than two frequency ranges is enabled.
Intel(R) Speed Shift Technology	Disabled		Intel® Speed Shift Technology is disabled.
	Enabled	x [1)]	Intel® Speed Shift Technology is enabled.
Turbo Mode (only if the processor type used supports turbo mode) (only if "Intel (R) SpeedStep (tm)" = Enabled or "Intel (R) Speed Shift Technology" = Enabled)	Disabled	x [1)]	Turbo mode is disabled.
	Enabled		Turbo mode is enabled. When the operating system requires more power, the processor can use Intel® Turbo Boost Technology to increase the clock speed. To use turbo mode effectively, the performance modes of the "Intel(R) SpeedStep(tm)"/"Intel (R) Speed Shift Technology" processor and the power saving modes of the "C states" processor must be enabled.
C states	Disabled		The energy-saving modes of the "C states" processor are disabled.
	Enabled	x [1)]	The energy-saving modes of the "C states" processor are enabled.

1) Depending on the device type, the device configuration and other firmware settings, if applicable, the setting on delivery may deviate from the specified value.

2.6.3 Level: "Power" tab

Device behavior after a power failure and after a "wake event".

Calling "Power" tab

Select: "Setup Utility (Page 9)" > "Power".

Firmware setting	Value	Setting in delivery state IPC427E IPC477E	Meaning
Wake on LAN 1 (X1 P1)	Disabled		The LAN controller of the onboard Ethernet interface "X1 P1" cannot switch on the device.
	Enabled	x	The LAN controller of the onboard Ethernet interface "X1 P1" can switch on the device.
Wake on LAN 2 (X2 P1)	Disabled		The LAN controller of the onboard Ethernet interface "X2 P1" cannot switch on the device.
	Enabled	x	The LAN controller of the onboard Ethernet interface "X2 P1" can switch on the device.
Wake on LAN 3 (X3 P1)	Disabled		The LAN controller of the onboard Ethernet interface "X3 P1" cannot switch on the device.
	Enabled	x	The LAN controller of the onboard Ethernet interface "X3 P1" can switch on the device.
PROFINET always On	Disabled	x	The onboard PROFINET interface of CP1616 is not supplied with power in the operating states S4 and S5.
	Enabled		The onboard PROFINET interface of CP1616 is supplied with power in the operating states S4 and S5.
USB Ports 1/2 (X61/X60)	Disabled		The respective USB ports are not supplied with voltage in sleep mode.
	Enabled	x	The respective USB ports are supplied with voltage in sleep mode.
USB Ports 3/4 (X63/X62)	Disabled	x	The respective USB ports are not supplied with voltage in sleep mode.
	Enabled		The respective USB ports are supplied with voltage in sleep mode.
USB Ports 5/6(MCP/OTC)	Disabled	x	The respective USB ports are not supplied with voltage in sleep mode. (only available on IPC477E)
	Enabled		The respective USB ports are supplied with voltage in sleep mode. (only available on IPC477E)
USB Ports 9 (Front USB)	Disabled	x	The respective USB port is not supplied with voltage in sleep mode. (only available on IPC477E)
	Enabled		The respective USB port is supplied with voltage in sleep mode. (only available on IPC477E)
USB Port 10 (internal)	Disabled	x	The respective USB port is not supplied with voltage in sleep mode.
	Enabled		The respective USB port is supplied with voltage in sleep mode.
Touch Controller Mode • Only with: IPC477E	Ignored	x	Touch controller is disabled.
	Singletouch		Touch controller is operated in single-touch mode.
	Multitouch		Touch controller is operated in multi-touch mode.

2.7 "Boot" tab

2.7.1 Level: "Boot" tab

Boot behavior of the device, bootable device components (boot media) and boot sequence.

Calling "Boot" tab

Select: "Setup Utility (Page 9)" > "Boot".

Firmware setting	Value	Setting in delivery state	Meaning
		IPC427E IPC477E	
Boot Type	Dual Boot Type	x	Booting from legacy and UEFI devices is supported.
	Legacy Boot Type		Only booting from legacy devices is supported.
	UEFI Boot Type		Only booting from UEFI devices is supported.
Quick Boot	Enabled	x	Quick start of the device is enabled. During the boot procedure, various hardware function tests are skipped. This shortens the boot procedure.
	Disabled		Quick start of the device is disabled.
Quiet Boot	Enabled	x	The boot logo is displayed during the self-test.
	Disabled		Start information appears in text mode during the self-test.

Firmware setting	Value	Setting in delivery state IPC427E IPC477E	Meaning	
PXE BOOT / Network Stack	Disabled	x	The UEFI Network Stack for network access under UEFI is not available. For example, UEFI installation via PXE (Preboot Executable Environment) is not possible.	
	Enabled		The UEFI Network Stack for network access under UEFI is available.	
• **PXE Boot capability** (only if "Network Stack" = Enabled)	Disabled	x	Booting via PXE (Preboot Executable Environment) is disabled. Only UEFI Network Stack is supported.	PXE = Preboot Executable Environment Controls the booting of a boot image that can be loaded over the network.
	UEFI:IPv4		Only UEFI boot media that support Internet protocol version 4 are considered as PXE boot media.	
	UEFI:IPv6		Only UEFI boot media that support Internet protocol version 6 are considered as PXE boot media.	
	UEFI:IPv4/IPv6		Only UEFI boot media that support Internet protocol version 4 or version 6 are considered as PXE boot media.	
	Legacy		PXE boot legacy for legacy boot media	
Add Boot Options	First		Newly detected boot media are placed at the top of the boot sequence.	
	Auto	x	Newly detected boot media are placed automatically in the boot sequence, e.g. depending on the device path for UEFI boot media.	
	Last		Newly detected boot media are placed at the bottom of the boot sequence.	
USB Boot	Enabled		Booting from USB devices is permitted.	
	Disabled	x	Booting from USB devices is not permitted.	
EFI Device First	Disabled		Legacy devices are started before UEFI devices in the boot sequence	
	Enabled	x	UEFI devices are started before legacy devices in the boot sequence	
SATA Boot	Enabled	x	Booting from SATA devices is permitted.	
	Disabled		Booting from SATA devices is not permitted.	
Timeout	0..10	0	Delay time (in seconds) during booting so that the user has time to press the hotkey to open the firmware selection menu.	

2.7.2 "EFI"

List of boot media.

Calling "EFI"

Select: "Setup Utility (Page 9)" > "Boot" > "EFI".

- If "Add Boot Options" = "Auto", the boot media is grayed out and cannot be changed.
- If "Add Boot Options" = "First" or "Last", the following can be changed:
  - Sequence of the boot media: <F6>, <F5> or <+>, <-> keys
  - List of valid boot media: <Return> button

2.7.3 "Legacy"

List of boot media.

Calling "Legacy"

Select: "Setup Utility" > "Boot" > "Legacy"

- If "Add Boot Options" = "Auto", the boot media is grayed out and cannot be changed.
- If "Add Boot Options" = "First" or "Last", the following can be changed:
  - Sequence of the boot media: <F6>, <F5> or <+>, <-> keys
  - List of valid boot media: <Return> button

Firmware setting	Value	Setting in delivery state IPC427E IPC477E	Meaning
Normal Boot Menu	Normal	x	Normal order of the boot options
	Advance		Advanced order of the boot options

2.7.4 "Boot Type Order"

Specification of the boot sequence according to device type.

The following can be changed:

- Sequence of the boot media: Keys <F6>, <F5>

2.7.5 "Hard Disk Drive"

Specification of the boot sequence of the hard disks.

The following can be changed:

- Boot sequence of the hard disks: Keys <F6>, <F5>

2.8 "Exit" tab

2.8.1 Level: "Exit" tab

Exit the Setup utility. You have the following options for saving or discarding the changes you made:

Calling "Exit"

Choose: "Setup Utility (Page 9)" > "Exit".

Firmware setting	Meaning
Exit Saving Changes	All changes are saved. The device is restarted with the changed firmware settings.
Save Change Without Exit	All changes are saved. Setup utility remains open.
Exit Discarding Changes	Setup Utility is closed. All changes are discarded.
Load Optimal Defaults	The firmware settings are reset to the safe default values. The delivery state is restored. **NOTICE**: All current firmware settings are overwritten.
Load Custom Defaults	The user-specific profile with the user-specific firmware settings is loaded. **Requirement:** The firmware settings were previously saved as user-specific profile with "Save Custom Defaults". **NOTICE**: All current firmware settings are overwritten when loading the user-specific profile with "Load Custom Defaults".
Save Custom Defaults	The current firmware settings are saved as a user-specific profile (see also "Load Custom Defaults").
Discard Changes	All changes to the firmware settings are discarded.
Save setup settings to file	The current firmware settings are written to a file.
Load setup settings from file	Firmware settings are loaded from a file.

Configuring Intel® Management Engine BIOS Extension (MEBx) 3

3.1 Logging onto MEBx (assigning password)

Procedure

1. Open the firmware selection menu (Page 8).
2. Select the "Intel(R) Management Engine BIOS Extension" option on the "Main Page" with the arrow keys.
3. Confirm your selection with the <Return> key.
4. In the "MAIN MENU" of the MEBx, select the "MEBx Login" option.
5. Enter the following "**Intel(R) ME Password**" when logging on the first time:

   admin
6. Afterwards, change the password immediately.

   The new password must contain the following characters:

   – A total of at least eight characters
   – An upper case letter
   – A lower case letter
   – A number
   – A special character . ! @ # $ % ^ & *

   Note

   The underscore and blank space are valid password characters but do not increase password complexity.

3.2 Options of the MEBx

Use "Intel® Management Engine BIOS Extension" (MEBx) to configure important firmware settings of your device to use Intel® AMT functions and the Intel® Management Engine (ME). The following options are available for Intel® AMT-enabled devices:

- Intel(R) ME General Settings
- Intel(R) AMT
- Intel(R) AMT Configuration
- MEBx Exit

Requirement for the use of "Intel® Management Engine BIOS Extension" (MEBx)

- The firmware setting "AMT BIOS Features" is assigned the value "Enabled". You can find information on this under AUTOHOTSPOT.

Note

The MEBx setting options depend on whether or not your device supports Intel® AMT.

Intel(R) ME General Settings

MEBx setting	Meaning
Change ME Passwort	Here, you can change the current password for logging onto MEBx. You can find information on this under "Logging onto MEBx (assigning password) (Page 31)".
FW Update	Firmware updates of the "Intel® Management Engine" (ME) can be installed, not installed or only installed after entering the password.

Intel(R) AMT

MEBx setting	Meaning
Intel(R) AMT	When Intel® Active Management Technology (iAMT) is disabled, all network settings are reset to the settings in the delivery state.

Intel(R) AMT Configuration

MEBx setting	Meaning
Manageability Feature Selection	Intel® AMT functions are enabled or disabled. In the delivery state, "Manageability Feature Selection" = Disabled.
SOL/Storage Redirection/KVM (only if "Manageability Feature Selection" = Enabled)	Enabling and disabling of the Intel® AMT functions: • Username and Password • SOL • Storage Redirection • KVM Feature Selection
User Consent (only if "Manageability Feature Selection" = Enabled)	User Consent settings. Forces the following additional security behavior: When a user attempts to establish a KVM connection remotely, a six-digit number is displayed on the AMT PC. The remote user must enter this number on the help desk PC before the KVM connection can be opened.
Password Policy (only if "Manageability Feature Selection" = Enabled)	Password policy that specifies the conditions under which the password is permitted to be changed remotely. The following options can be selected: • Default Password Only • During Setup And Configuration • Anytime
Network Setup (only if "Manageability Feature Selection" = Enabled)	The following network settings can be configured: Intel(R) ME Network Name Settings • Host Name • Domain Name • Shared/Dedicated FQDN • Dynamic DNS Update TCP/IP Settings > Wired LAN IPV4 Configuration • DHCP mode
Activate Network Access (only if "Manageability Feature Selection" = Enabled)	Enables the network interface. This MEBx setting is only available when the network is not enabled.
Unconfigure Network Access (only if "Manageability Feature Selection" = Enabled)	Disables the network interface and resets the network settings to their default values.
Remote Setup And Configuration (only if "Manageability Feature Selection" = Enabled)	Displays the current provisioning settings.
Power Control (only if "Manageability Feature Selection" = Enabled)	Specifies the power states (S0, S3, S4, S5) of the computer in which MEBx is enabled.

MEBx Exit

Exiting MEBx. The changes are saved.

Further information

More information about MEBx can be found here: Intel® website (https://www.intel.com).

Configuring Intel® AMT

4

To make use of "Intel® Active Management Technology ", proceed as follows:

- First, enable the Intel® AMT functions in the firmware settings of the Setup Utility.
- Then, configure the Intel® AMT functions with Intel® Management Engine BIOS Extension

Enabling and configuring Intel® AMT functions

1. Open "Setup Utility (Page 9)".
2. Assign the "Enabled" value to the firmware setting "AMT BIOS Features". You can find information on this under "AUTOHOTSPOT".
3. Press the <ESC> key to return to the firmware selection menu.
4. Select the "Intel(R) Management Engine BIOS Extension" option and configure the Intel® AMT functions again. You can find information on this under "Options of the MEBx (Page 32)".

Reset Intel® AMT functions to default settings and disabling iAMT

One effect of resetting to the default settings is that Intel® AMT is disabled.

1. Open "Setup Utility (Page 9)".
2. Enable the firmware setting "Unconfigure ME". You can find information on this under AUTOHOTSPOT.

   If the "Hide Unconfigure ME Confirmation Prompt" option is disabled, a confirmation prompt for performing the "Unconfigure ME" action is displayed at the next startup. If you perform this action, all values of the Intel® Management Engine BIOS Extension (MEBx) including the MEBx password are reset to default values.

Disabling Intel® AMT access to the firmware/BIOS settings

You can prevent access to firmware/BIOS settings with Intel® AMT

This may be necessary, for example, in the following cases:

- When you are no longer using Intel® AMT.
- You want to ensure that Intel® AMT is not used without authorization.

For this, you need to disable iAMT as described in the previous section.

All Intel® AMT functions are thereby reset to default settings.

Update firmware

5

Firmware/BIOS updates are regularly available for your device. You can download these from the Internet.

Backing up firmware settings before updating the firmware

NOTICE
Risk of irretrievable loss of data After a firmware/BIOS update all firmware settings are deleted. This can put the system in an undefined state. The consequence may be damage to the device or system. • Before updating your firmware, back up the current firmware settings by writing them to a file. You can find information on this under "Level: "Exit" tab (Page 30)".

Procedure

1. Open the "SIEMENS Industry Online Support (https://support.industry.siemens.com/cs/ww/en/view/75842768)" page.
2. Navigate to your device in the area "Online Support; Drivers and BIOS Updates for download".
3. Download the current firmware/BIOS version in the download area.

   Registration is required for this.
4. Install the current firmware/BIOS update on your device following the instructions accompanying the download.
5. Change the firmware settings as required for your application. If necessary, use the previously created file with the previous firmware settings for this.
6. Save the firmware settings.

Booting from USB stick

6

Note

The "USB Boot" option has to be set to "Enabled" in the "Boot" tab so that the device can boot from the USB stick.

1. Connect the USB stick to the device.
2. Open the firmware selection menu (Page 8).
3. Select "Boot-Manager."
4. Select the USB medium in the "Boot-Manager" and confirm the entry.

Enable Trusted Platform Module (TPM) 7

Depending on the ordered configuration, you device may have a Trusted Platform Module. The Trusted Platform Module is a chip that enhances your device with security functions. This provides improved protection against device manipulation.

You enable use of the Trusted Platform Module in the firmware settings.

NOTICE
Import restrictions for the Trusted Platform Module Use of the Trusted Platform Module is subject to legal restrictions in some countries and is not permitted in these countries. • Always observe the import restrictions of the country in which the device will be operated.

Procedure

1. Check your order documents to find out whether a Trusted Platform Module is present on your device.
2. Open the "Security" tab. You can find information on this under "Level: "Security" tab (Page 19)".
3. Ensure that the "Available" value is assigned to firmware setting "TPM Availability".
4. Save the changes you made before closing the Setup Utility. You can find information on this under ""Exit" tab (Page 30)".

Index

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W