Arrakis Mk3 Series

Version:
v1.1.0

Date:
17.11.2025

Contents

1 Copyright

2 Regulatory Compliances

2.1 Complies with the following EU directives

Radio Equipment Directive (2014/53/EU) only applies to devices containing radio module EM05-G.

No	Short Name
2014/35/EU	Low Voltage Directive (LVD)
2014/53/EU	Radio Equipment Directive (RED)
2014/30/EU	Electromagnetic Compatibility (EMC)
2011/65/EU	Restriction of the use of certain hazardous substances in electrical and electronic equipment Directive (RoHS2)
2015/863/EU	Amendment to Annex II in Directive 2011/65/EU regards the list of restricted substances (RoHS3)

2.2 References of standards applied

Standard	Reference	Issue
EN 18031-1	Common security requirements for radio equipment - Part 1: Internet connected radio equipment	2024
EN 55032	Electromagnetic compatibility of multimedia equipment - Emission Requirements	2015+A11:2020+A1:2020
EN 55035	Electromagnetic compatibility of multimedia equipment - Immunity requirements	2017+A11:2020
EN IEC 61000-3-2	Electromagnetic compatibility (EMC) - Part 3-2: Limits - Limits for harmonic current emissions	2019
EN 61000-3-3	Electromagnetic compatibility (EMC) - Part 3-3: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems	2013+A1:2019
EN 61000-4-2	Electromagnetic compatibility (EMC). Testing and measurement techniques. Electrostatic discharge immunity test	2009
EN 61000-4-3	Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity test	2006+A1:2008+A2:2010
EN 61000-4-4	Electromagnetic compatibility (EMC) - Part 4-4 : Testing and measurement techniques - Electrical fast transient/burst immunity test	2012
EN 61000-4-5	Electromagnetic compatibility (EMC) - Part 4-5: Testing and measurement techniques - Surge immunity test	2014+A1:2017
EN 61000-4-6	Electromagnetic compatibility (EMC) - Part 4-6: Testing and measurement techniques - Immunity to conducted disturbances, induced by radio-frequency fields	2014+AC:2015
EN 61000-4-8	Electromagnetic compatibility (EMC) - Part 4-8: Testing and measurement techniques - Power frequency magnetic field immunity test	2010
EN IEC 61000-4-11	Electromagnetic compatibility (EMC) - Part 4-11: Testing and measurement techniques - Voltage dips, short interruptions and voltage variations immunity tests	2004+A1:2017
EN 50121-4	Railway applications - Electromagnetic compatibility - Part 4: Emission and immunity of the signalling and telecommunications apparatus	2016+A:2019
EN 61000-6-4	Electromagnetic compatibility (EMC) - Part 6-4: Generic standards - Emission standard for industrial environments	2007+A1:2011
EN 301 489-1 (module)	ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements; Harmonised Standard for ElectroMagnetic Compatibility	V2.2.3
EN 301 489-52 (module)	ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 52: Specific conditions for Cellular Communication User Equipment (UE) radio and ancillary equipment; Harmonised Standard for ElectroMagnetic Compatibility	V1.2.1
Draft EN 301 489-19 (module)	ElectroMagnetic Compatibility (EMC) standard for radio equipment and services - Part 19: Specific conditions for Receive Only Mobile Earth Stations (ROMES) operating in the 1,5 GHz band providing data communications and GNSS receivers operating in the RNSS band (ROGNSS) providing positioning, navigation and timing data	V2.2.0

2.3 FCC PART 15 VERIFICATION STATEMENT

WARNING

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Notice: The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

May contain transmitter module:

- N7NMC7455
- RYK-WPET236ACNBT

2.4 ICES-003 ISSUE 7 VERIFICATION STATEMENT

CAN ICES3(A)/NMB3(A)

This device complies with CAN ICES-003 Issue 7 Class A. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Cet appareil est conforme à la norme CAN ICES-003 Issue 7 Class A. Le fonctionnement est soumis auxdeux conditions suivantes : (1) cet appareil ne doit pas causer d'interférences nuisibles et (2) cet appareil doit accepter toute interférence reçue, y compris les interférences pouvant opération indésirable.

May contain transmitter module:

- 2417C-MC7455
- 6158A-PET236ACNBT

3 Intended Use and IT Security Instructions

This section provides crucial safety and security information and recommendations to help you configure your Welotec Industrial Computer (IPC) for optimal security in your deployment.

3.1 Intended Use

This section specifies the intended use and essential operating conditions for your Welotec Industrial Computer (hereinafter referred to as “IPC”).

The IPC is designed for use as a dedicated control, monitoring, and data acquisition unit within the enclosed control cabinet of a machine. Its primary function is to execute specific machine-control software, process operational data, provide human-machine interface (HMI) functionalities, and/or facilitate communication within the industrial automation environment. The IPC is exclusively intended for continuous operation within a controlled industrial setting.

The intended use of the IPC is strictly defined by the following conditions and requirements:

3.1.1 Physical Security and Installation Environment

- Enclosure: The IPC must be permanently installed within a secure, locked control cabinet (e.g., meeting IP54 or higher protection class) that provides adequate protection against dust, moisture, mechanical impact and unauthorized access.
- Controlled Access: Access to the control cabinet and its wiring must be restricted to authorized personnel only. Physical security measures (e.g., key locks, access control systems) are mandatory.
- Environmental Conditions:
  - Temperature: The IPC must operate within the specified ambient temperature and humidity range as outlined in the technical specifications. Adequate ventilation or active cooling within the cabinet must ensure these limits are not exceeded. This includes accounting for the unit’s own thermal dissipation and that of all other components in the cabinet.
  - Vibration and Shock: The IPC must be mounted securely within the cabinet to minimize exposure to excessive vibrations and mechanical shock, adhering to the manufacturer’s specifications.
  - Cleanliness: The inside of the cabinet must be kept free of dust, debris, and contaminants that could impair cooling or lead to electrical shorts.

3.1.2 EMC compliant electrical Installation and Power Supply

This product is designed to meet EMC standards when installed according to the following instructions. Failure to adhere to these instructions may result in the equipment failing to meet compliance standards and can cause interference with other devices. The installer is responsible for ensuring the EMC conformity of the final system.

- Power Supply: The IPC must be connected to a dedicated stable and filtered power supply within the specified voltage range. To ensure operational reliability and meet EMC requirements, the power source must provide adequate filtering against surges, transients, electrical fast transients (EFTs), and conducted RF noise common in industrial environments. An Uninterruptible Power Supply (UPS) is highly recommended to protect further against power fluctuations and outages.

- Wiring: All wiring connecting to the IPC must comply with applicable industrial wiring standards, be properly insulated, strain-relieved, and protected against mechanical damage.
- Grounding: The unit must be properly grounded according to the installation manual, typically via a low-impedance connection to the control cabinet's central grounding point.

3.1.3 Functional Safety

This unit is not certified as a standalone component for functional safety applications (e.g., SIL, PL).

Intended Use: The unit is intended for standard control and monitoring. It must not be used as the sole or primary controller for safety-critical functions (e.g., emergency stops, safety interlocks, light curtains, burner controls).

System Integration: Safety-related control logic must be executed by dedicated, certified safety controllers (e.g., Safety PLC, safety relays). This unit may be used to supervise or monitor a safety system (e.g., for HMI visualization or data logging) via a non-safety-rated communication channel, but it must not be part of the safety-critical control loop. The failure of this unit must not lead to a loss of the primary safety function.

3.1.4 Qualified and Trained Personnel

- Installation, Configuration, and Maintenance: All installation, configuration, maintenance, troubleshooting, and repair activities on the IPC and its connections within the control cabinet must be performed exclusively by qualified, trained, and authorized technical personnel. This personnel must possess proven expertise in electrical systems, IT hardware, and cybersecurity best practices.
- Security Awareness: All personnel interacting with the IPC or the network it is connected to must receive regular training on IT security awareness including password policies and reporting suspicious activities.

3.1.5 Software and Configuration

- Operating System: Only the pre-installed or manufacturer-approved operating system (OS) version may be used. The OS must be regularly updated with security patches provided by the manufacturer or OS vendor, after thorough testing in a non-production environment.
- Secure Configuration: The IPC's operating system, firmware, and installed applications must be configured according to secure hardening guidelines, including disabling unused services, ports, and protocols, and enforcing strong password policies.
- Secure Boot: Where supported Secure Boot must be enabled to prevent the loading of unsigned or malicious bootloaders.

Please refer to the section "Cyber Security" for further details.

3.1.6 Network Segmentation and "Defense in Depth" IT Security Principles

- Network Segmentation: The unit and its control network must be isolated from all other networks (e.g., corporate, guest, public internet) using industrial firewalls and network segmentation. Direct connection to the internet is considered misuse unless done via a secure, managed gateway.
- Defense in Depth: A multi-layered security approach ("Defense in Depth") must be implemented for the entire machine. This includes:
  - Network Security: Industrial Firewalls (e.g., Next-Generation Firewalls) at network boundaries, strict firewall rules (whitelist approach – only allow explicitly required traffic), VLANs for segmentation.
  - System Security: Operating system hardening (minimum services, disabled unnecessary ports), regular security updates, robust antivirus/anti-malware solutions specifically designed for industrial environments, and strong password policies.

  - Application Security: Secure configuration of all industrial applications, disabling default credentials, and ensuring application-level security features are enabled.
  - Data Integrity: Measures to ensure data integrity and availability (e.g., backups, redundant systems where appropriate).
  - Physical Security: see above

- Access Control: Remote access to the IPC (if required) must be strictly controlled, using secure connections, multi-factor authentication, and granular user permissions. Unnecessary remote access functionalities must be disabled.
- Logging and Monitoring: The IPC and connected network devices should implement logging of security-relevant events. Centralized monitoring and alerting systems are recommended for timely detection of anomalies.

3.2 Non-Intended Use

Any use of the IPC that deviates from the conditions described including but not limited to:

- Operation outside the specified environmental limits.
- Operation without a secure, enclosed control cabinet.
- Operation in hazardous locations (e.g., explosive atmospheres) for which the unit is not explicitly certified.
- Installation or maintenance by unqualified personnel.
- Connection to an unfiltered, unstable, or non-grounded power source.
- Direct connection to unsecured corporate networks or the internet without adequate protective measures.
- Installation of unauthorized software or operating systems.
- Bypassing or disabling of security features (e.g., firewall, antivirus, Secure Boot).
- Failure to implement a cyber security management plan (patching, hardening, access control).

is considered non-intended use and may result in:

- Damage to the IPC or the machine.
- Compromised data security and integrity.
- Serious personal injury or death.
- Failure to comply with regulatory requirements.

3.3 Exposed Interfaces and Services

The following interfaces are exposed:

Interface	Comment
LAN 1 and 2	
COM 1 and 2	
USB 1 … 4	
HDMI	
DP	
DI / GND	Digital Input
DO / GND	Digital Output
SW / GND	Power Switch

Available services highly depend on Operating System type and version.

3.4 Cyber Security

The flexibility to run common operating systems like Windows and Linux places the full responsibility of cyber security implementation on the system integrator and end-user. The unit is a component that must be integrated into a comprehensive, defense-in-depth security architecture.

The intended use requires the integrator/user to implement, at a minimum, the following:

3.4.1 Use Secure Boot

Secure Boot is a crucial security feature that helps protect your system from malware and unauthorized operating systems during the boot process. It's a component of the Unified Extensible Firmware Interface (UEFI) that ensures only trustworthy software, signed with a digital certificate, loads when your system starts. Without Secure Boot, malicious programs or unsigned operating systems could load unnoticed before the actual operating system, compromising your system's integrity and security.

We highly recommend enabling Secure Boot - please refer to "BIOS" section for further details

3.4.2 Enable Storage Encryption

Storage encryption is a critical security measure that protects your sensitive data by rendering it unreadable to unauthorized parties, even if they gain physical access to your storage device. In today's interconnected world, where devices can be lost, stolen, or compromised, ensuring the confidentiality of your information is paramount.

Windows (using BitLocker with TPM)

Windows' built-in BitLocker encryption leverages the TPM to securely store the encryption key, making the process largely automatic and secure.

- Check TPM Status: Ensure that the TPM chip is enabled in the UEFI/BIOS settings
- Open BitLocker Drive Encryption: Search for "BitLocker" in the Windows search bar and select "Manage BitLocker."
- Turn on BitLocker: Select the drive you wish to encrypt (typically your C: drive) and click "Turn on BitLocker."

- Follow the Wizard: Windows will guide you through the process. Since a TPM is present, it will typically automatically use the TPM to store the encryption key. You will be prompted to save a recovery key (e.g., to a Microsoft account, a USB drive, or print it) – this is crucial in case you ever need to access your data if the TPM is reset or unavailable.
- Start Encryption: The encryption process will begin in the background. You can continue using your computer during this time.

Linux (using LUKS with TPM consideration):

Linux uses LUKS (Linux Unified Key Setup) for full disk encryption. Integrating it with a TPM for automatic unlocking at boot can be more involved than BitLocker but offers similar benefits. This typically involves tools like clevis or systemd-cryptenroll.

- Install Necessary Tools: You'll need cryptsetup for LUKS and potentially tpm2-tools and clevis (or similar TPM integration tools) if you want to bind your LUKS key to the TPM for automatic decryption.
- Encrypt the Drive (during OS Installation or manually):
  - During Installation: Most Linux distributions (e.g., Ubuntu, Fedora) offer an option to "Encrypt the disk" during the installation process. This is the simplest way to set up LUKS.
  - Manually (Post-Installation): If encrypting an existing drive or a secondary drive, you would use cryptsetup luksFormat /dev/sdXy to format the partition for LUKS, followed by cryptsetup luksOpen /dev/sdXy my_encrypted_drive and then creating a filesystem on the opened device.
- Bind LUKS Key to TPM (Optional, for automatic unlock):
  - This is the step that utilizes the TPM. Tools like clevis can be used to "bind" a LUKS passphrase (or a key slot) to the TPM. This allows the system to automatically unlock the encrypted volume at boot if the TPM verifies the system's integrity.
  - The exact commands vary, but it generally involves generating a new LUKS key slot and then using a TPM-binding tool to store the key in the TPM and configure the system to use it for unlocking.
- Update Boot Configuration: Ensure your bootloader (e.g., GRUB) is configured correctly to handle the encrypted root partition and, if used, to leverage the TPM for unlocking.

For both operating systems, it's essential to:

- Backup your recovery keys/passphrases: Without them, your data can be permanently lost if there's a hardware failure or you forget your primary password.
- Understand the implications: While encryption provides strong security, proper handling of keys and adherence to security best practices are still crucial.

3.4.3 Use Strong Passwords

Strong passwords are the first line of defense against unauthorized access. If you want to use password based access it is recommended to:

- Change the factory default password on first login
- Use passwords with a minimum length of 12 characters or more
- Use a combination of uppercase and lowercase letters, numbers, and special characters (e.g., !@#$%^&*)
- Do not use easily guessable patterns, such as sequences (e.g., "123456", "abcdef"), repeated characters (e.g., "aaaaaa"), or dictionary words

3.4.4 System Hardening:

The operating system (Windows or Linux) must be hardened. This includes:

- Disabling all unused services, applications, and network ports.
- Enforcing strong, unique passwords for all accounts.
- Implementing a least-privilege access model for users and applications.
- Configuring OS-level firewalls (e.g., ufw, Windows Defender Firewall).

3.4.5 Patch Management

A robust process must be in place for testing and deploying security patches for the operating system and all installed third-party applications. This process must be compatible with the operational constraints of the industrial environment.

3.4.6 Endpoint Protection

Where appropriate for the application, industrial-compatible endpoint protection (e.g., anti-malware, application whitelisting, host-based intrusion detection) must be installed, maintained, and kept up-to-date.

3.4.7 Physical Security

Use of the locked control cabinet (see Section 3) to prevent unauthorized physical access and tampering (e.g., via USB ports) is a critical part of the security model.

3.5 Vulnerability Handling

Welotec has implemented a Coordinated Vulnerability Disclosure Policy - please visit the following site for further details: https://welotec.com/pages/coordinated-vulnerability-disclosure-policy

4 Safety Instructions

Please read these instructions carefully and retain them for future reference.

1. Disconnect this equipment from the power outlet before cleaning. Do not use liquid or sprayed detergent for cleaning. Use a moist cloth or sheet.
2. Keep this equipment away from humidity.
3. Ensure the power cord is positioned to prevent tripping hazards and do not place anything on top of it.
4. Pay attention to all cautions and warnings on the equipment.
5. If the equipment is not used for an extended period, disconnect it from the main power to avoid damage from transient over-voltage.
6. **Prolonged usage with less than 9V may damage the PSU or destroy the mainboard.**
7. Never pour any liquid into openings as this could cause fire or electrical shock.
8. Have the equipment checked by service personnel if:
    - The power cord or plug is damaged.
    - Liquid has penetrated the equipment.
    - The equipment has been exposed to moisture in a condensation environment.
    - The equipment does not function properly, or you cannot get it to work by following the user manual.
    - The equipment has been dropped and damaged.
9. Do not leave this equipment in an unconditioned environment, with storage temperatures below -20 degrees or above 60 degrees Celsius for extended periods, as this may damage the equipment.
10. Unplug the power cord when performing any service or adding optional kits.
11. Lithium Battery Caution:
    - Risk of explosion if the battery is replaced incorrectly. Replace only with the original or an equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.
    - Do not remove the cover, and ensure no user-serviceable components are inside. Take the unit to a service center for service and repair.

5 Product Specifications

5.1 Technical Details

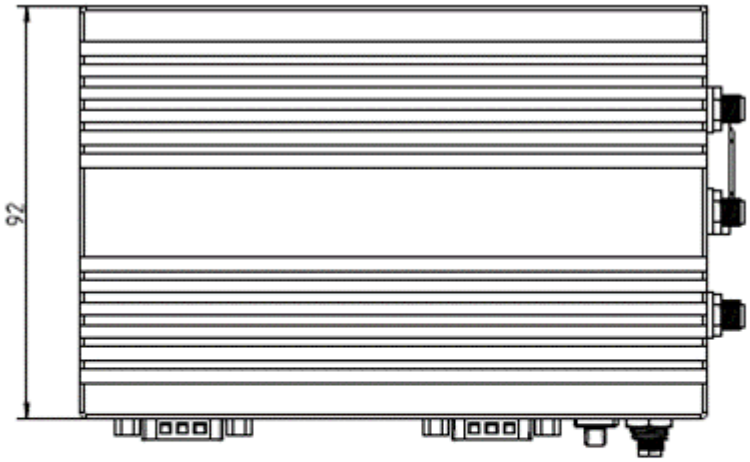
Feature	Specification	Details
Processor	CPU	Intel Atom® Quadcore E3950, 1.6/2.0 GHz (Standard)
Memory	RAM	up to 8GB DDR3L SoDIMM
Storage Options	mSATA	1 mSATA 2.0 Slot
Security	TPM	TPM 2.0 with TrEE 1.1
I/O Ports	HDMI	1 HDMI port
	DisplayPort	1 DisplayPort
	Gigabit Ethernet	2x RJ45 ports
	USB 3.0	4 ports
	Serial Ports	2x RS232/RS485, optional expansion for 2 additional
	Digital I/O	1 DI, 12-24V 1 DO, 12-24V, max. 2 A, output voltage defined by DC input
Connectivity	Ethernet	Dual Intel i210IT LAN chip (Gigabit)
	WLAN (optional)	Optional, via mPCIe
	WWAN (optional)	Optional 4G/5G via USB
Expansion	SIM Slots	2 push-push type SIM slots (available with 4G/5G modules)
Additional	Audio and Other	Line in/out, Digital I/O, CAN (optional)
	Watchdog Timer	Programmable from 1 to 255 seconds
Environmental	Operating Temperature	-20° to 70° C
	Storage Temperature	-20° to 80° C
	Humidity	5% to 95% non-condensing
Power	Supply	9 - 36 V DC (+/-10% tolerance), 4-pin terminal block and DC jack
	Adapter	Optional 60W, 24V/5A external, CR1220 CMOS battery
Mounting	Options	DIN-Rail mounting kits available
Operating System	Compatibility	Windows 10, Ubuntu Linux, others upon request
Physical Build	Material/Color	Steel / Aluminum
	Ingress Protection	IP20
	Dimensions	64 x 140 x 92 mm
	Weight	800 g

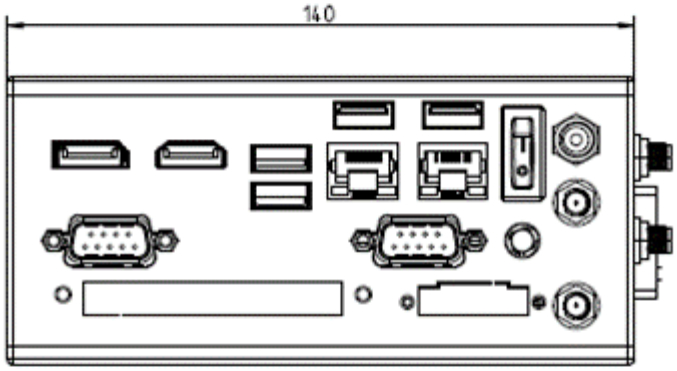
6 System Information

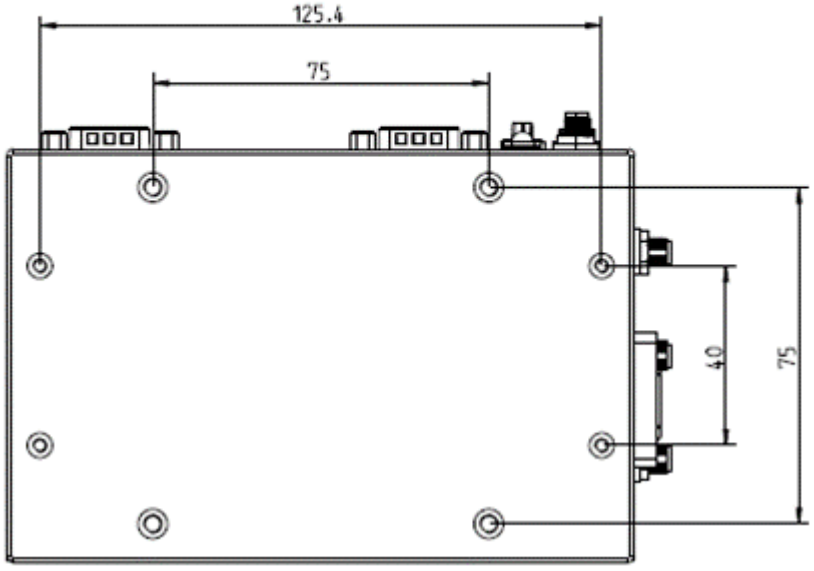
Being a powerful, yet small fanless system, the Arrakis Pico Mk4 may reach very high surface temperatures in excess of 60°C/140°F with risk of injury. Users should ensure sufficient protection against touching.

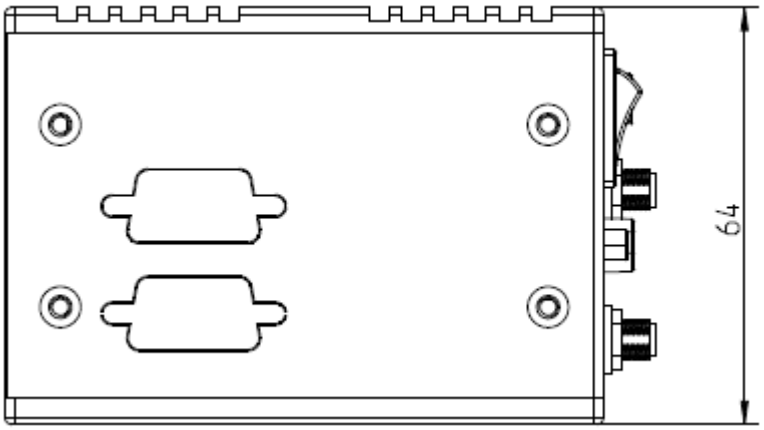
To allow for sufficient heat removal we recommend: 30mm distance on either side of the Arrakis Pico Mk4 when mounted on a DIN-Rail 100mm headroom above the Arrakis Pico Mk4 when mounted horizontally. The heatsink should be on top.

6.1 System Drawing

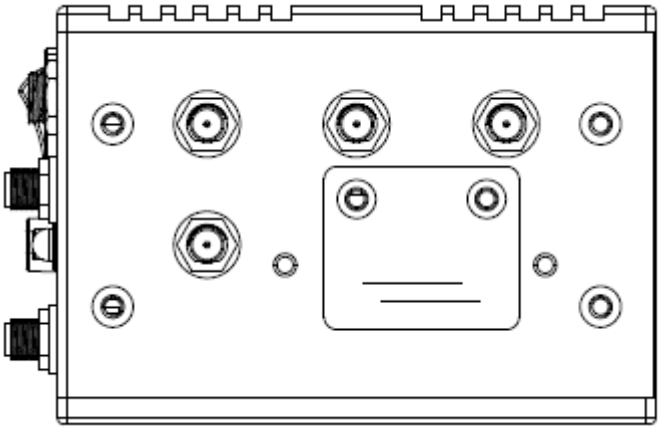




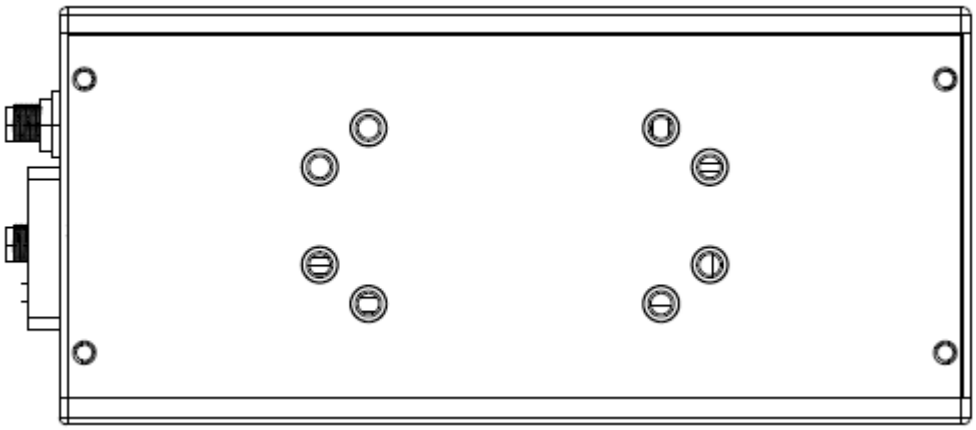




Bottom side



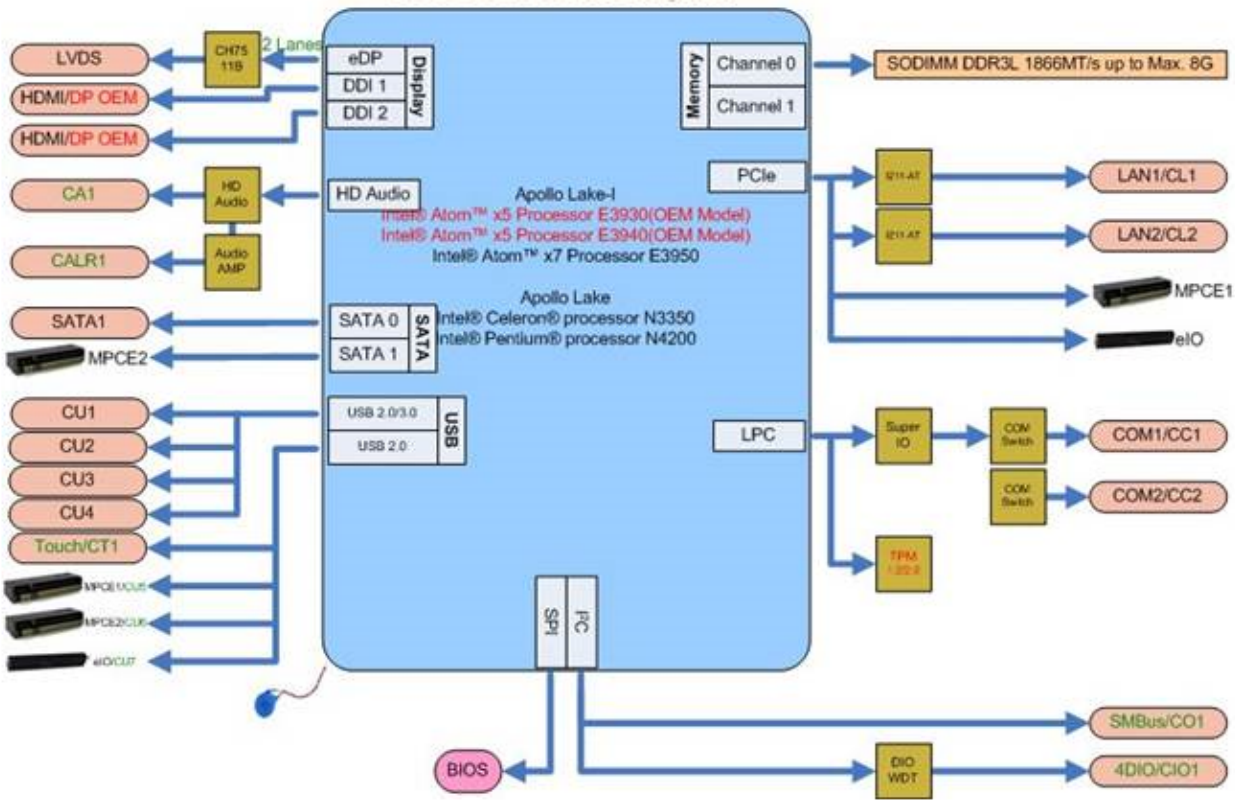
Top side



Rear side

6.2 Mainboard Block Diagram

This block diagram describes the relationship among all interfaces and modules on the mainboard.



7 Power Supply

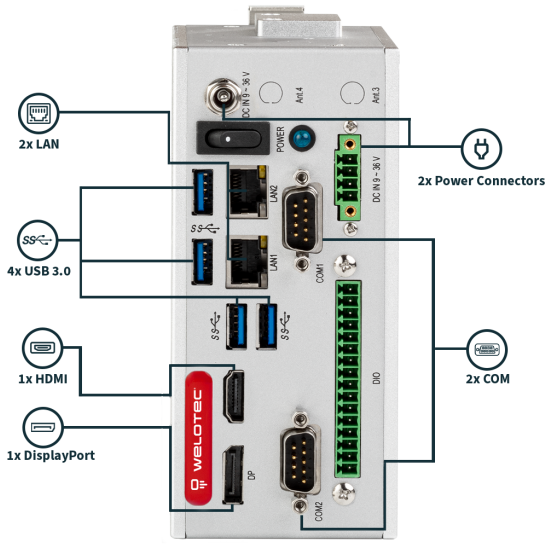
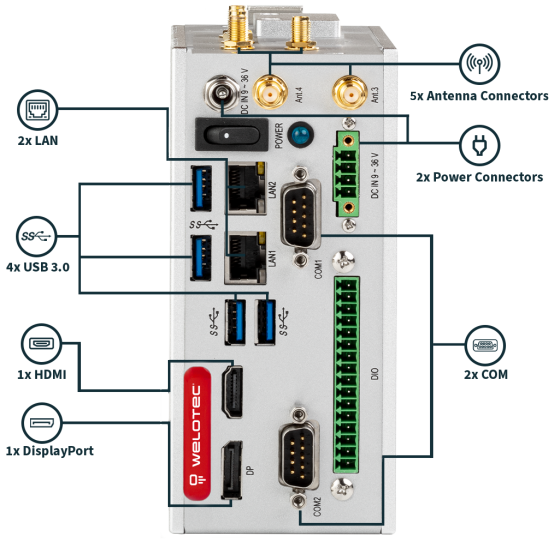
⚠ Please ensure no external voltage is applied to PSW! This could cause damage.

To power the Arrakis Mk3, use either the terminal block or the DC jack with a 9-36V DC input - please consider “EMC compliant electrical Installation” part in chapter “Intended Use and IT Security Instruction”

Pin	Description
Pin 0 - VCC (left)	V+ (9-36V DC)
Pin 1 & 2 - PSW	External power switch
Pin 3 - GND (right)	Ground

8 Interfaces and Connections

8.1 Arrakis Mk3 Series

Arrakis Mk3	Arrakis Mk3 (with optional Modules)
	
	
	

9 Radio Modules (only relevant with optional LTE/WiFi Modules)

The Arrakis Mk3 may contain the following RF Modules:

- Sierra Wireless MC7455
- Telit Cinterion LEPCIC4EU08T080700
- SparkLAN WZ-WPET-236ACN(BT)

LTE:

Sierra Wireless MC7455	Supported Bands
LTE	B1/ B2/ B3/ B4/ B5/ B7/B8/ B12/B13/ B20/ B25/ B26/B29/B30/ B41
WCDMA	B1/ B2/ B3/ B4/ B5/ B8

WiFi

SparkLAN WZ-WPET-236ACN(BT)	
Operating Frequency	IEEE 802.11ac/a/b/g/nISM Band: 2.412GHz~2.484GHz, 5.150GHz~5.850GHz*Subject to local regulations

9.1 Radio Frequencies Sierra Wireless MC7455

9.1.1 4G LTE Europe

Band	Frequency Range Down	Frequency Range Up	Max Transmission Power
Band 1	2110 MHz - 2170 MHz	1920 MHz - 1980 MHz	199 mW
Band 2	1930 MHz - 1990 MHz	1850 MHz - 1910 MHz	199 mW
Band 3	1805 MHz - 1880 MHz	1710 MHz - 1785 MHz	199 mW
Band 4	2110 MHz - 2155 MHz	1710 MHz - 1755 MHz	199 mW
Band 5	869 MHz - 894 MHz	824 MHz - 849 MHz	199 mW
Band 7	2620 MHz - 2690 MHz	2500 MHz - 2570 MHz	199 mW
Band 8	925 MHz - 960 MHz	880 MHz - 915 MHz	199 mW
Band 12	729 MHz - 746 MHz	699 MHz - 716 MHz	199 mW
Band 13	746 MHz - 756 MHz	777 MHz - 787 MHz	199 mW
Band 20	791 MHz - 821 MHz	832 MHz - 862 MHz	199 mW
Band 25	1930 MHz - 1995 MHz	1850 MHz - 1915 MHz	199 mW
Band 26	859 MHz - 894 MHz	814 MHz - 849 MHz	199 mW
Band 28	758 MHz - 803 MHz	703 MHz - 748 MHz	199 mW
Band 29	717 MHz - 728 MHz	n/a	199 mW
Band 30	2350 MHz - 2360 MHz	2305 MHz - 2315 MHz	199 mW
Band 41	2496 MHz - 2690 MHz	2496 MHz - 2690 MHz	199 mW

9.1.2 3G WCDMA

Band	Frequency Range Down	Frequency Range Up	Max Transmission Power
Band 1	2110 MHz – 2170 MHz	1920 MHz – 1980 MHz	251 mW
Band 2	1930 MHz – 1990 MHz	1850 MHz – 1910 MHz	251 mW
Band 3	1805 MHz – 1880 MHz	1710 MHz – 1785 MHz	251 mW
Band 4	2110 MHz – 2155 MHz	1710 MHz – 1755 MHz	251 mW
Band 5	869 MHz – 894 MHz	824 MHz – 849 MHz	251 mW
Band 8	925 MHz – 960 MHz	880 MHz – 915 MHz	251 mW

9.1.3 3G UMTS

Band	Frequency Range Down	Frequency Range Up	Max Transmission Power
Band 1	2110 MHz – 2170 MHz	1920 MHz – 1980 MHz	251 mW
Band 2	1930 MHz – 1990 MHz	1850 MHz – 1910 MHz	251 mW
Band 3	1805 MHz – 1880 MHz	1710 MHz – 1785 MHz	251 mW
Band 4	2110 MHz – 2155 MHz	1710 MHz – 1755 MHz	251 mW
Band 5	869 MHz – 894 MHz	824 MHz – 849 MHz	251 mW
Band 8	925 MHz – 960 MHz	880 MHz – 915 MHz	251 mW

9.2 Radio Frequencies Telit

Band	Frequency Range Down	Frequency Range Up	Max Transmission Power
Band 1	2110 MHz - 2170 MHz	1920 MHz - 1980 MHz	199 mW
Band 3	1805 MHz - 1880 MHz	1710 MHz - 1785 MHz	199 mW
Band 7	2620 MHz - 2690 MHz	2500 MHz - 2570 MHz	199 mW
Band 8	925 MHz - 960 MHz	880 MHz - 915 MHz	199 mW
Band 20	791 MHz - 821 MHz	832 MHz - 862 MHz	199 mW
Band 28A	758 MHz - 803 MHz	703 MHz - 748 MHz	199 mW

9.3 Radio Frequencies SparkLAN

9.3.1 WiFi Output Power & Sensitivity

IEEE Standard	Data Rate	Tx ± 2dBm	Rx Sensitivity
802.11b	11Mbps	18dBm	-85dBm
802.11g	54Mbps	14.5dBm	-71dBm
802.11n / 2.4GHz (HT20)	MCS7	14dBm (1TX)17dBm (2TX)	-67dBm
802.11n / 2.4GHz (HT40)	MCS7	13.5dBm (1TX)16.5dBm (2TX)	-65dBm
802.11a	54Mbps	14dBm	-75dBm
802.11n / 5GHz (HT20)	MCS7	13dBm (1TX)16dBm (2TX)	-71dBm
802.11n / 5GHz (HT40)	MCS7	13dBm (1TX)16dBm (2TX)	-67dBm
802.11ac (VHT80)	MCS9	11dBm (1TX)14dBm (2TX)	-57dBm
Bluetooth	3Mbps	0 Output Power 4 dBm	

Notes

- **Down:** Refers to the downlink frequency range.
- **Up:** Refers to the uplink frequency range.
- **Max Transmission Power:** Maximum power at which the device transmits.

10 BIOS

10.1 Introduction

The BIOS (Basic Input/Output System) serves as the fundamental bridge connecting the motherboard and operating system in your computer. It resides in the Flash Memory on the motherboard. When you start up the computer, the BIOS is the first to take control, initiating a series of checks known as the POST (Power-On Self Test) to ensure all hardware components are functioning properly. It identifies and configures hardware settings and prepares the system to hand over control to the operating system. The BIOS is crucial for system stability and optimal performance.

Within the BIOS setup menu, you'll find a range of options to configure. Below, we outline the function keys used to navigate and modify settings within the BIOS:

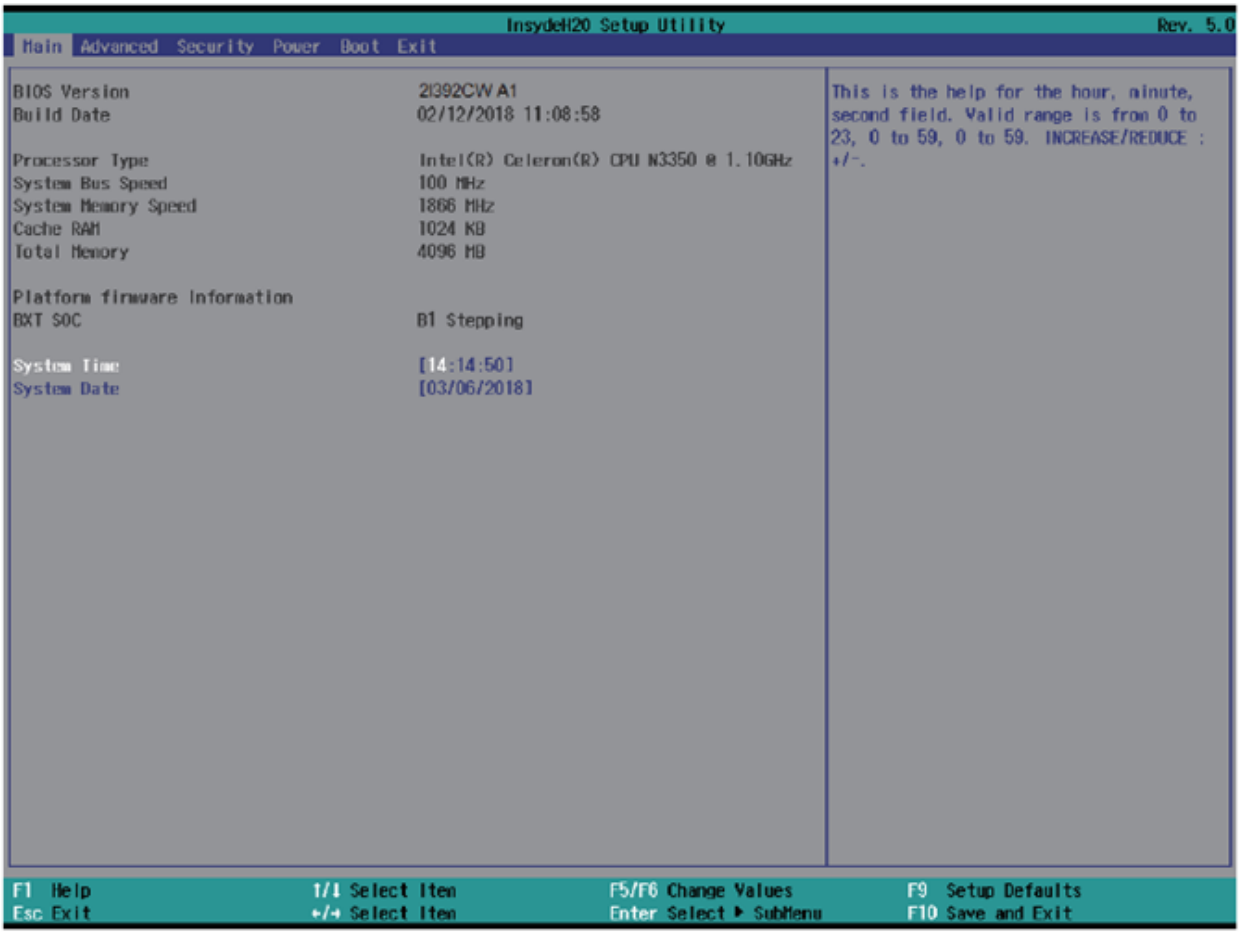
- **Esc:** Exit the BIOS setup.
- **Arrow keys (↑↓←→):** Navigate through options.
- **F10:** Save changes and exit.
- **Page Up/Page Down or +/-:** Adjust settings for selected options.

10.2 Accessing BIOS

To enter the BIOS setup:

1. Power on your computer and immediately press the `Del` key.
2. If you miss the initial prompt, restart your system by turning it off and on, or by pressing `Ctrl`, `Alt`, and `Delete` simultaneously to perform a soft reboot.

10.3 BIOS Menu Overview



The BIOS main menu offers a range of configurable settings crucial for tailoring your system's operation. Here's how you can navigate through these options efficiently:

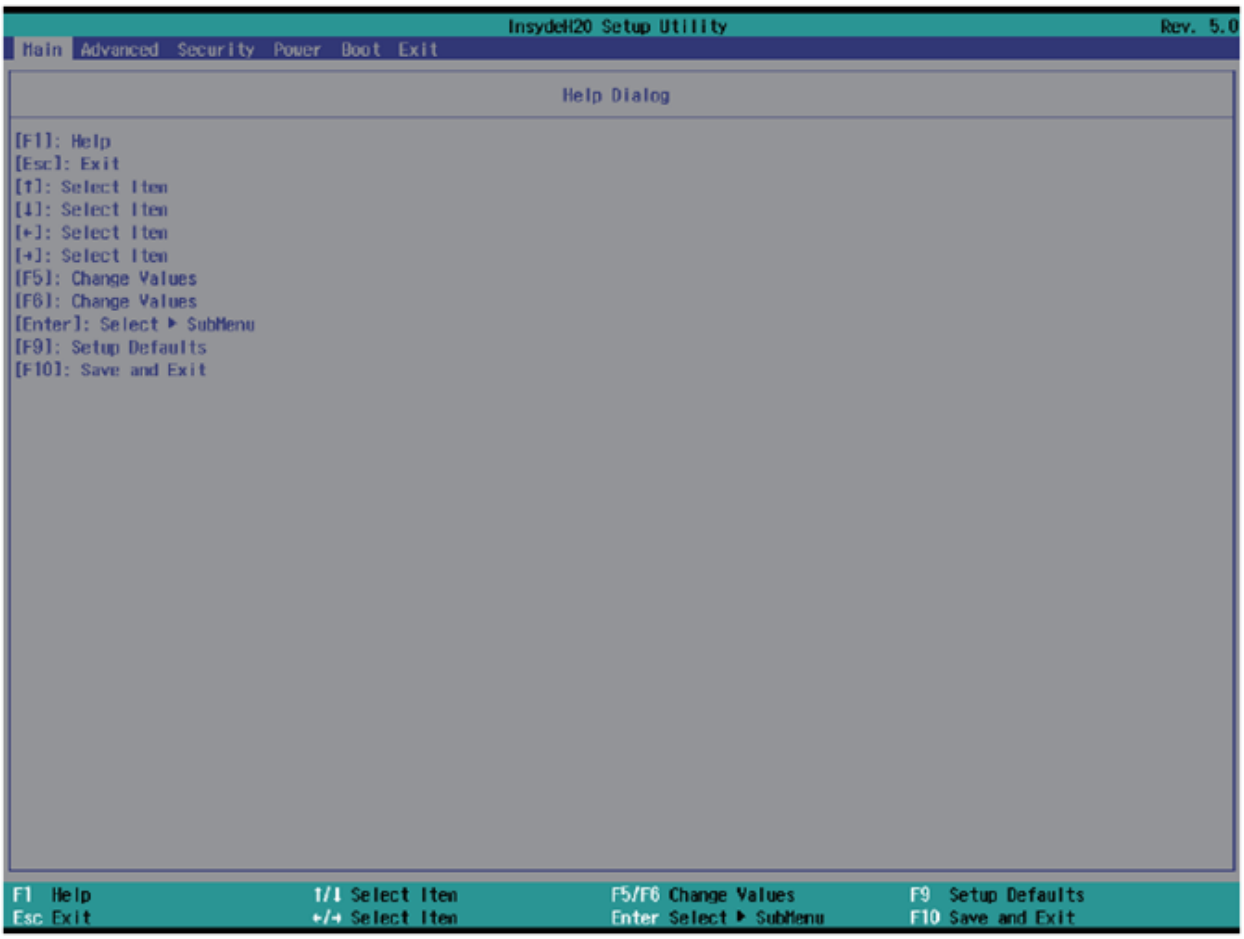
- **Navigating Screens:** Use the left (←) and right (→) arrow keys to switch between different settings screens.
- **Selecting Options:** Use the up (↑) and down (↓) arrow keys to highlight the specific option you want to adjust or confirm in the main menu.
- **Modifying Values:** Press `Enter` to select an option for modification. Use the plus (+) and minus (−) keys to adjust the values for the selected option.
- **Shortcut Keys:**
  - **`F1`:** Displays general help.
  - **`F2`:** Reverts to the previous value.
  - **`F3`:** Loads optimized default settings.
  - **`F4`:** Saves changes and resets the system.
  - **`Esc`:** Exits the BIOS Setup.

10.3.1 Menu Tabs:

- **Main:** Adjust basic system settings.
- **Advanced:** Modify advanced system configurations.
- **Security:** Set or change BIOS passwords.
- **Power:** Manage ACPI settings and power management options.
- **Boot:** Configure system boot options.
- **Exit:** Save changes or load default settings before exiting.

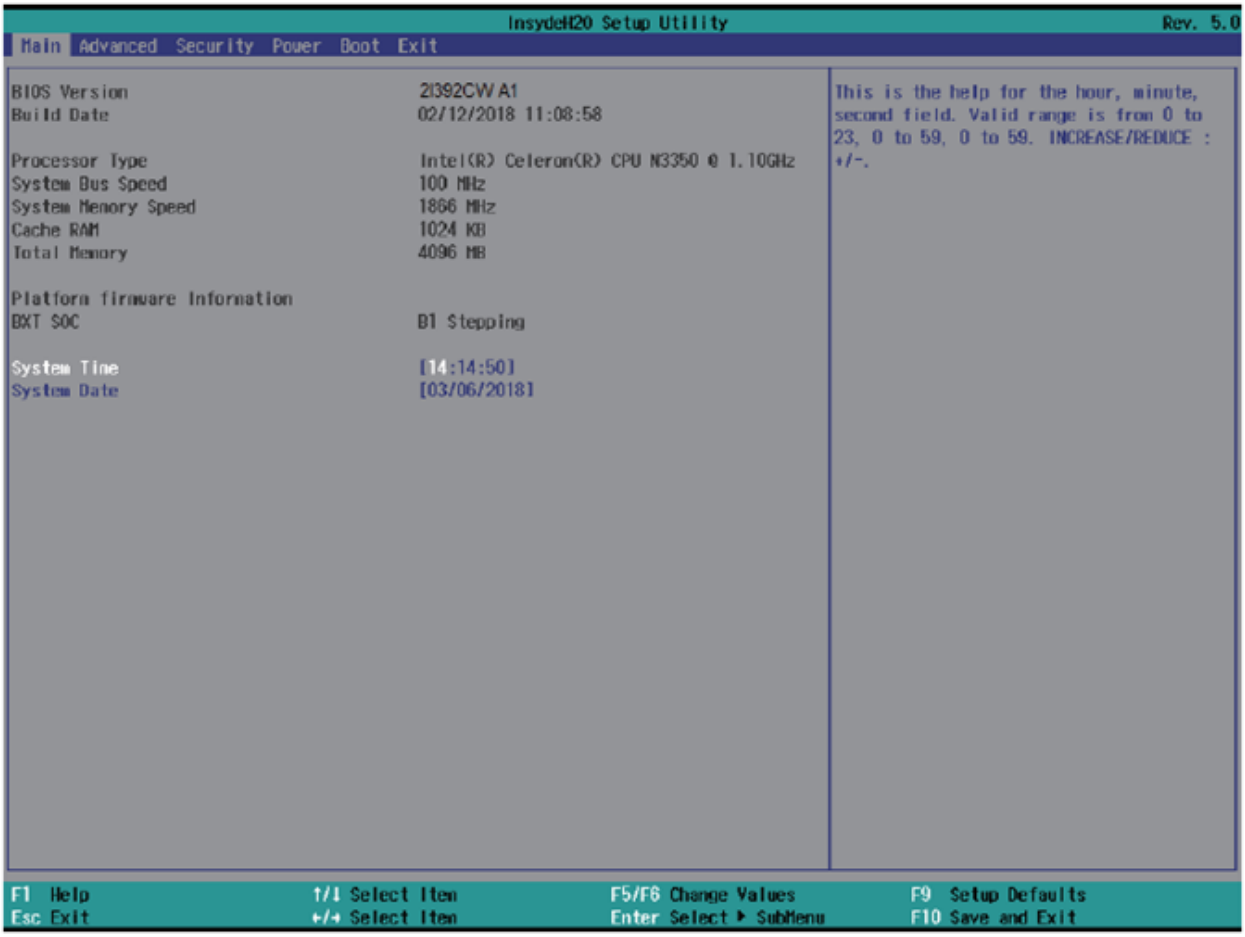
The selected tab is highlighted for easier navigation.

10.4 BIOS Help Feature



Access the BIOS Help window by pressing `F1`. This feature provides a detailed description of the function keys and their uses for the highlighted menu item. Press `Esc` to close the Help window.

10.5 Detailed Menu Options



The main menu screen displays basic system information and allows for easy configuration:

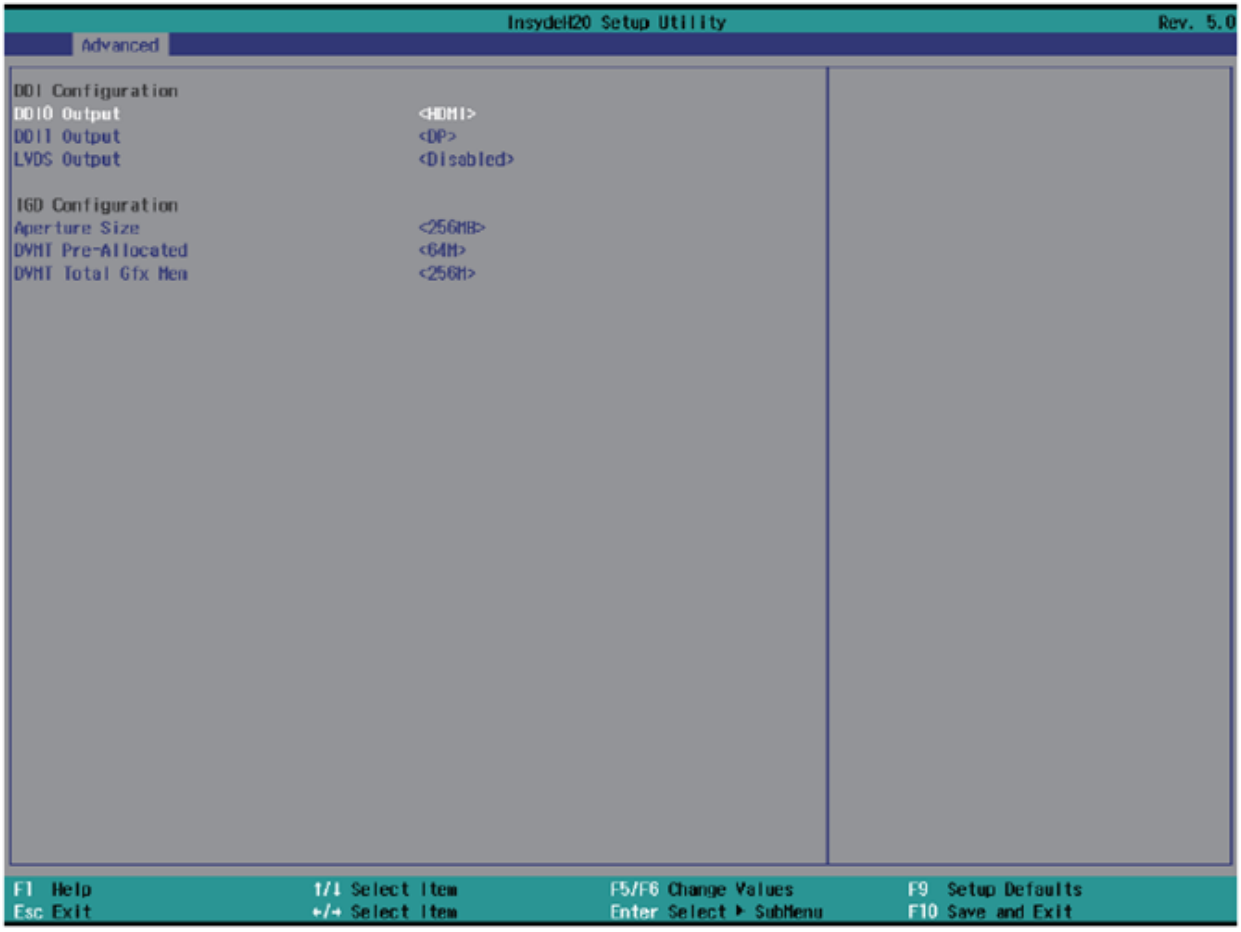
- **System Date:** Adjust the system date by using the `Tab` key to move between elements and the numerical keys to set the values.
- **System Time:** Set the system time in a similar manner, utilizing the `Tab` key for navigation and numerical keys for adjustments.

These settings help ensure that your system functions correctly and maintains accurate logs of system events and tasks.

10.6 Advanced BIOS Settings

Explore the configuration possibilities for your system's performance and functionality. Adjust settings to suit your hardware requirements and preferences.

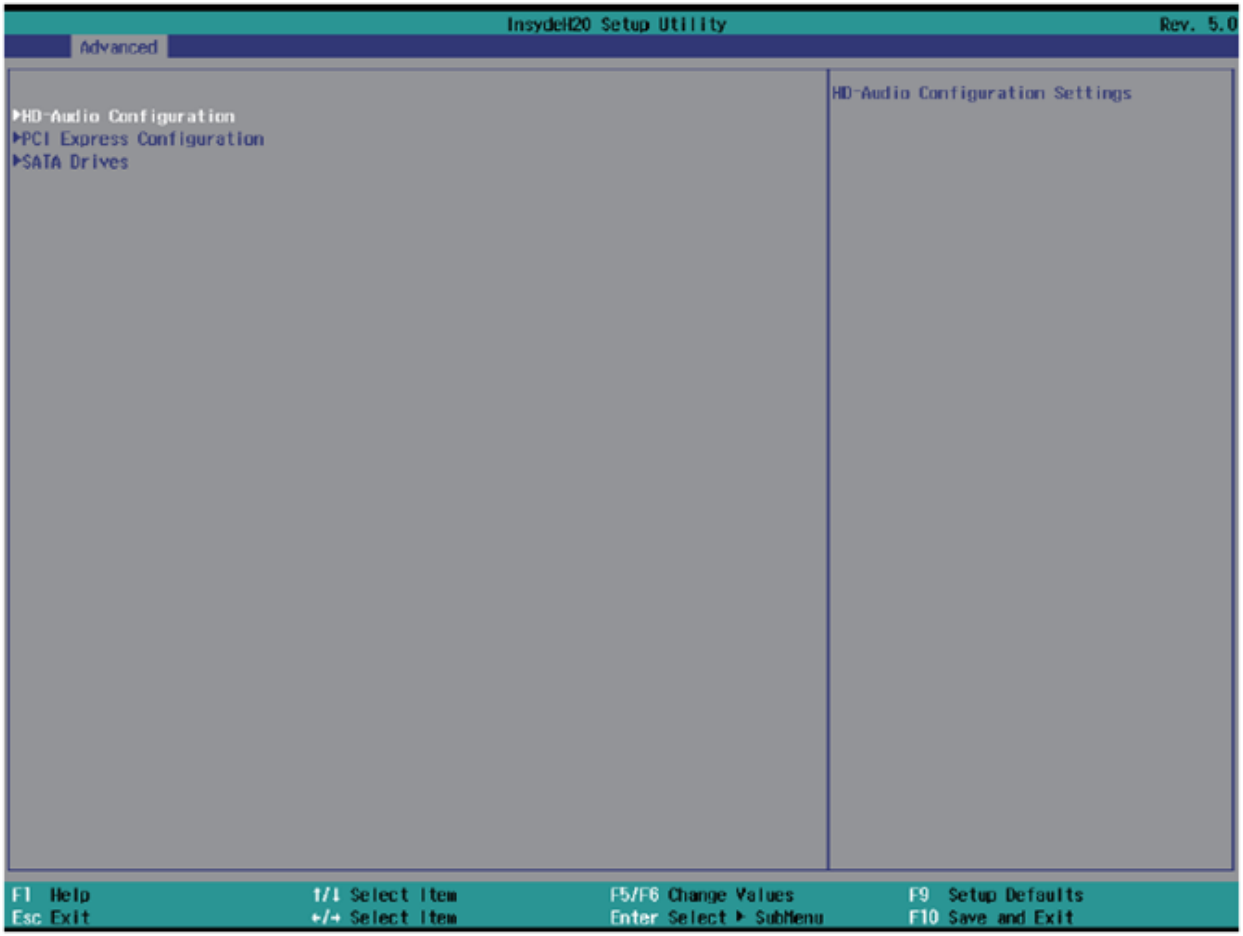
10.6.1 Video Configuration



Fine-tune the graphics performance by configuring the memory allocation:

- **Aperture Size**: Choose between 128MB, 256MB (default), or 512MB to optimize your system's graphics memory usage.
- **IGD - DVMT Pre-Allocated**: Set the fixed allocation for the integrated graphics memory. Available options are 64MB (default), 128MB, 256MB, or 512MB to enhance video performance.
- **IGD - DVMT Total Gfx Mem**: Adjust the total available graphics memory for the system, with choices of 128MB, 256MB (default), or the maximum supported by your hardware.

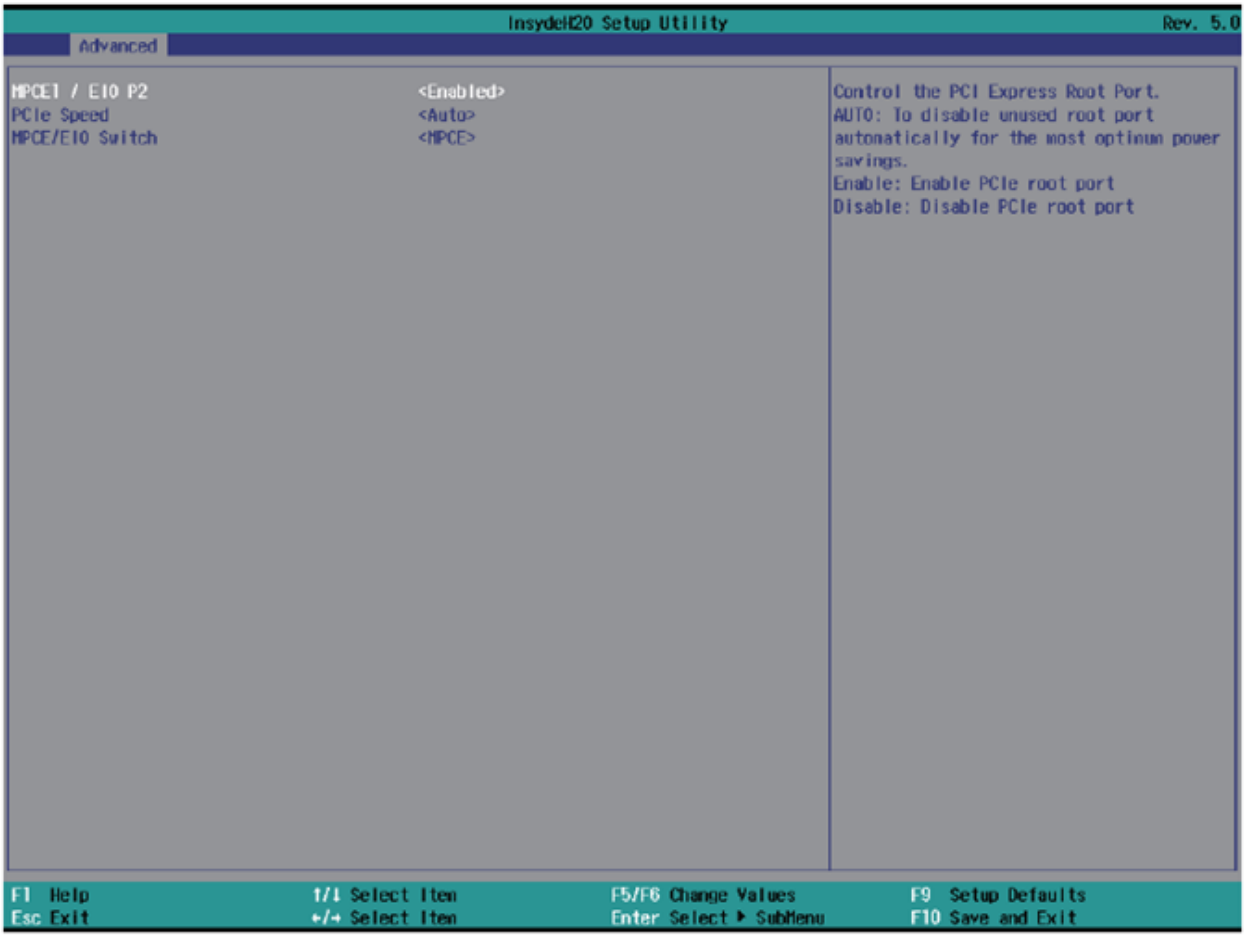
10.6.2 HD-Audio Configuration



Control audio capabilities to suit your media needs:

- **HD-Audio Support**: Toggle the high-definition audio to enhance your multimedia experience. Available settings are Enabled (default) and Disabled, allowing you to optimize audio performance according to your needs.

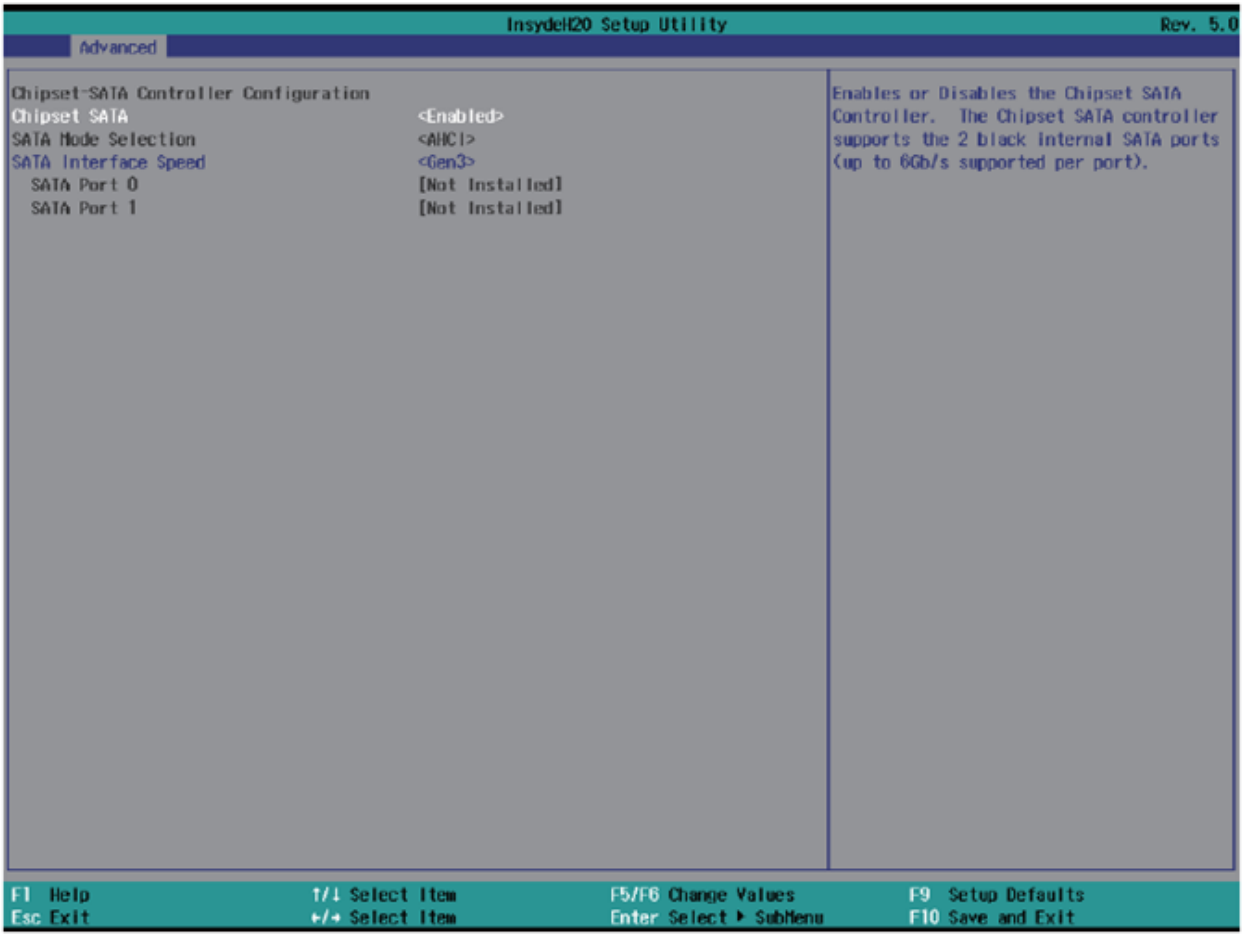
10.6.3 PCI Express Configuration



Configure the PCI Express settings to optimize connectivity and performance for expansion cards:

- **MPCE1 / EIO P2**: Enable or disable the MPCE1 slot with options for Disabled or Enabled (default), adapting to your hardware expansion needs.
- **PCIe speed**: Set the operational speed of the PCIe slots to match component specifications for optimal performance. Options include Auto (default), Gen1, and Gen2.
- **MPCE / EIO Switch**: Direct the PCIe signal either to the MPCE1 (default) or to the EIO, catering to different internal expansion needs for OEM I/O or function boards.

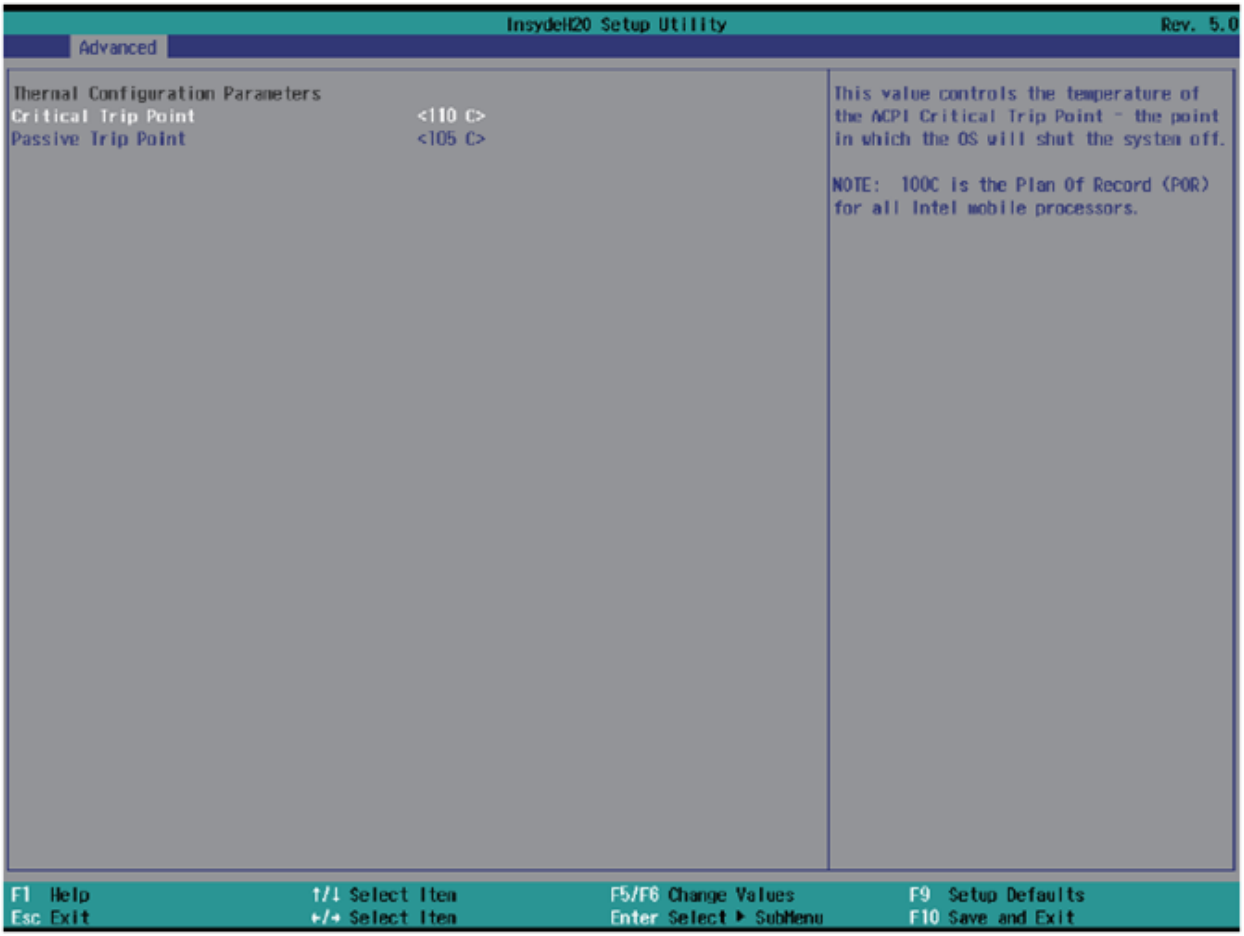
10.6.4 SATA Drives Configuration



Manage SATA settings to control internal storage interfaces and improve drive performance:

- **Chipset SATA**: Toggle the SATA controller to enhance system compatibility and power management with options for Enabled (default) or Disabled.
- **SATA Mode Select**: Note that the Arrakis MK3 operates exclusively in AHCI mode, ensuring modern storage performance and features.
- **SATA Interface Speed**: Choose the operation speed of the SATA ports to match your drive capabilities for improved data transfer rates. Available speeds are Gen1, Gen2, and Gen3 (default).

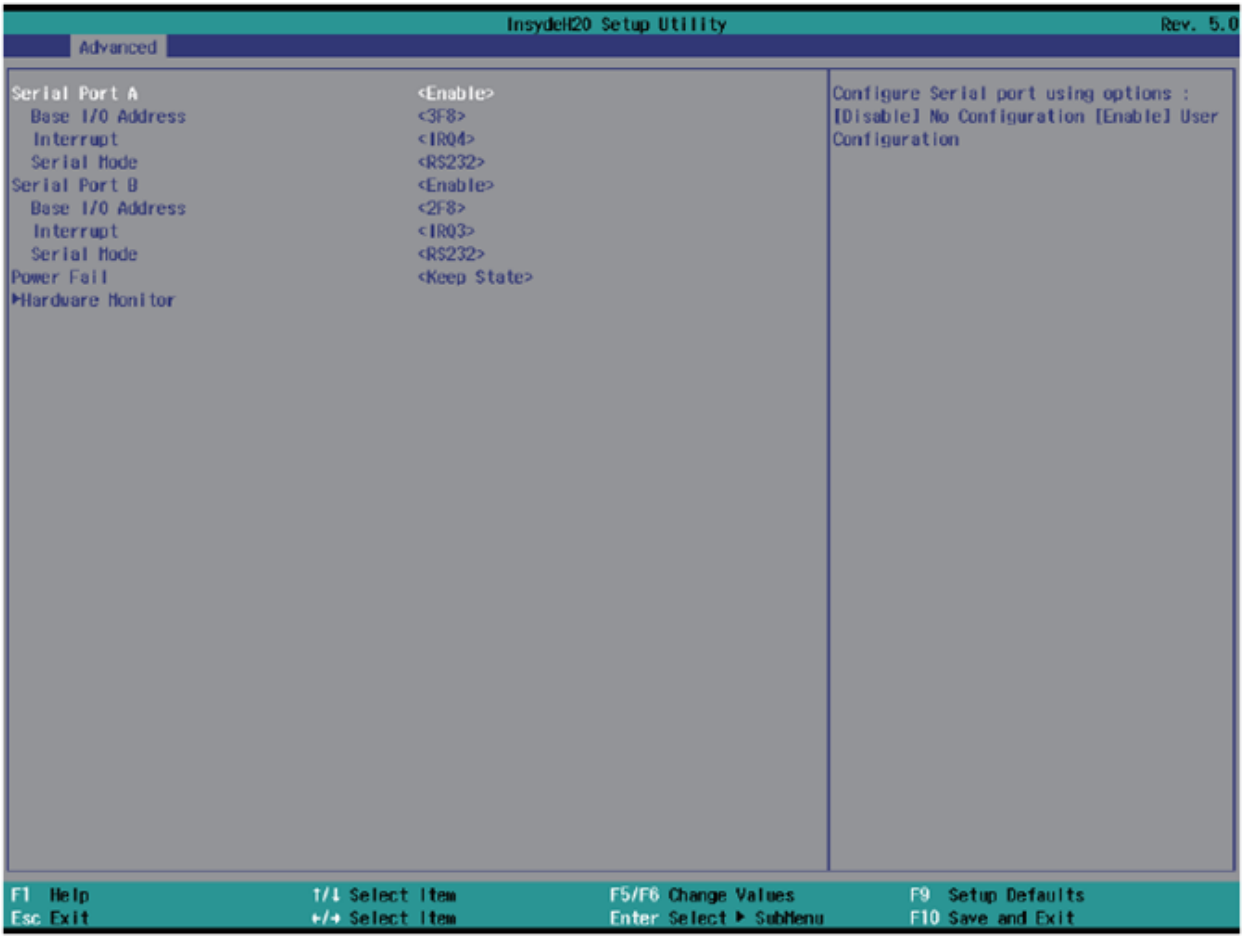
10.6.5 Thermal Configuration



Adjust the system's thermal settings to optimize performance and prevent overheating:

- **Thermal Configuration Parameters**: Manage the system's temperature thresholds that determine at which temperatures the OS will take critical actions.
- **Critical Trip Point**: Set at a default of 110°C, this is the temperature at which the system will shut down to prevent damage.
- **Passive Trip Point**: Set at a default of 105°C, this is the temperature at which the system begins to throttle CPU frequency to reduce heat generation.

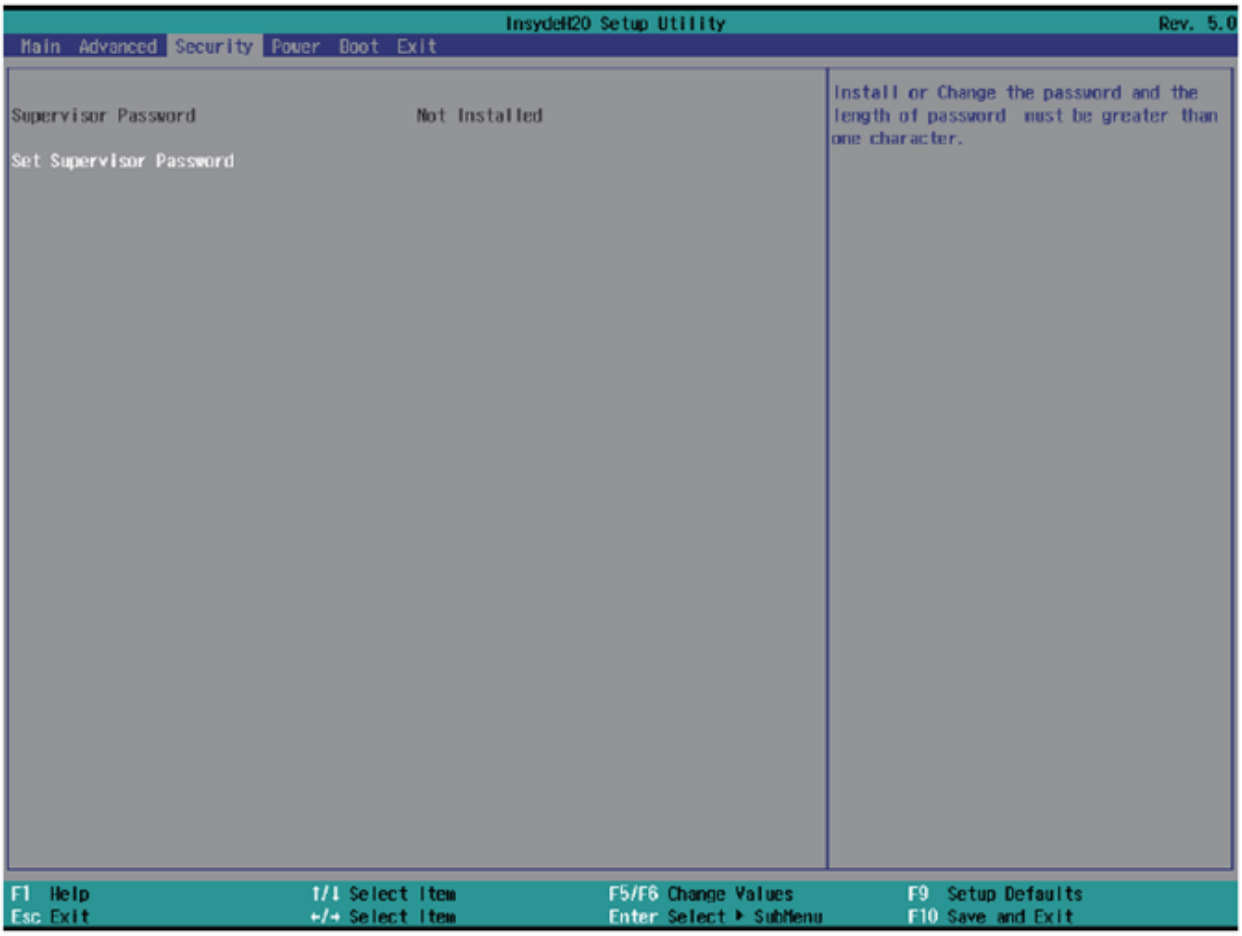
10.6.6 SIO FINETEK 81801U Configuration



Configure serial port settings and power failure responses for system stability and expanded connectivity:

- **Serial Port A/B**: Enable or disable COM ports as required, with both ports enabled by default.
- **Base IO Address / Interrupt**: Customize the I/O addresses and interrupts for each serial port with options such as:
  - `IO=3F8h; IRQ=4` for Port A (default)
  - `IO=2F8h; IRQ=3` for Port B (default)
- **Serial Mode**: Select between RS232 (default) and RS485 modes, the latter includes auto flow control for RS485.
- **Power Failure Settings**:
  - `Keep state` (default): Maintains the system's last state in case of power disruption.
  - `Always on`: System reboots automatically after power restoration.
  - `Always off`: System stays off after power loss.
- **Hardware Monitor**: Monitors and displays crucial system voltage and temperature readings, providing real-time data to safeguard the system's operational health.

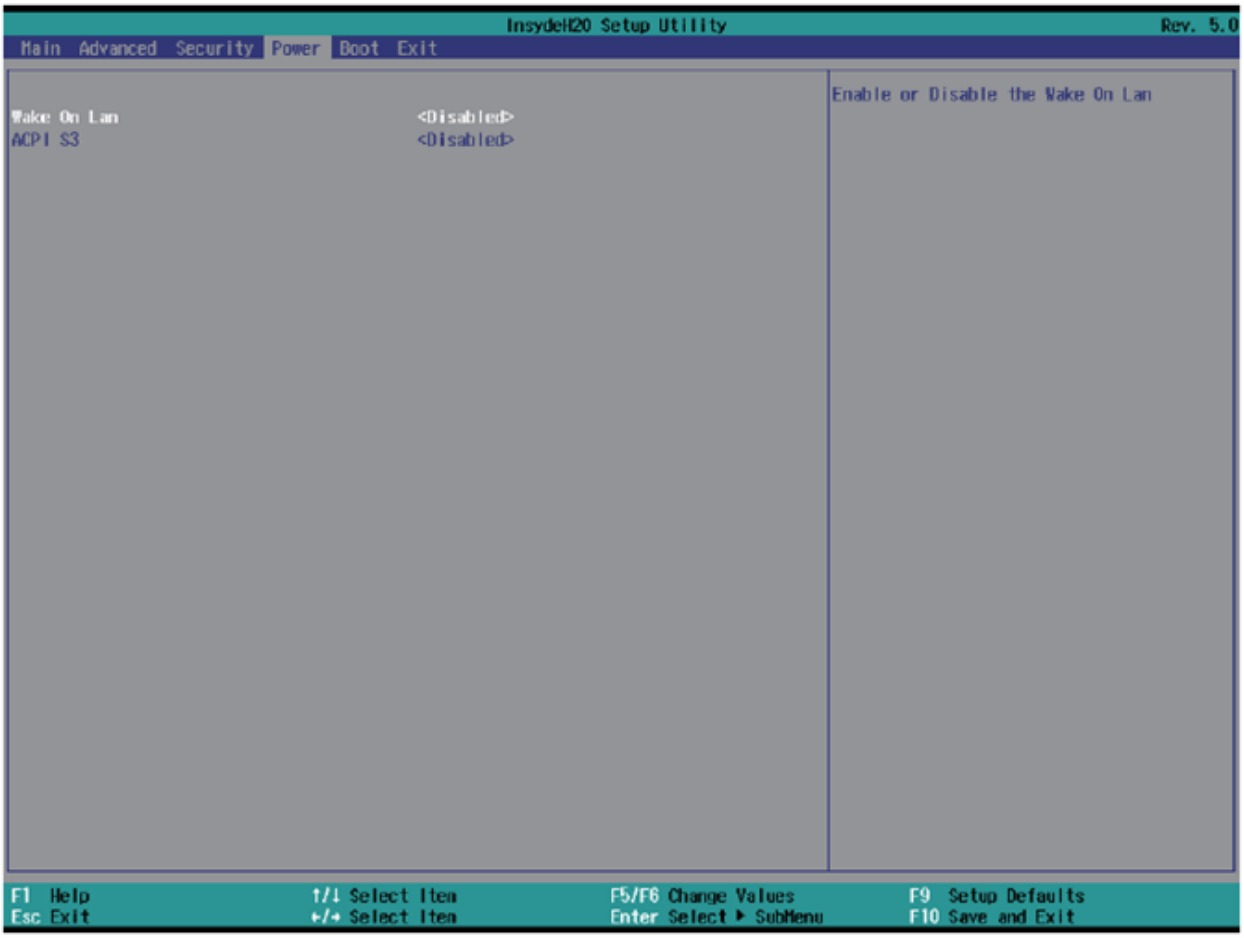
10.7 Security Settings



Set up a Supervisor password to enhance system security:

1. **Select Supervisor Password**: Opens a dialog to create a new password.
2. **Create Password**: Enter a password between 3 and 10 characters long.
3. **Confirm**: Press the `Enter` key to set the password.

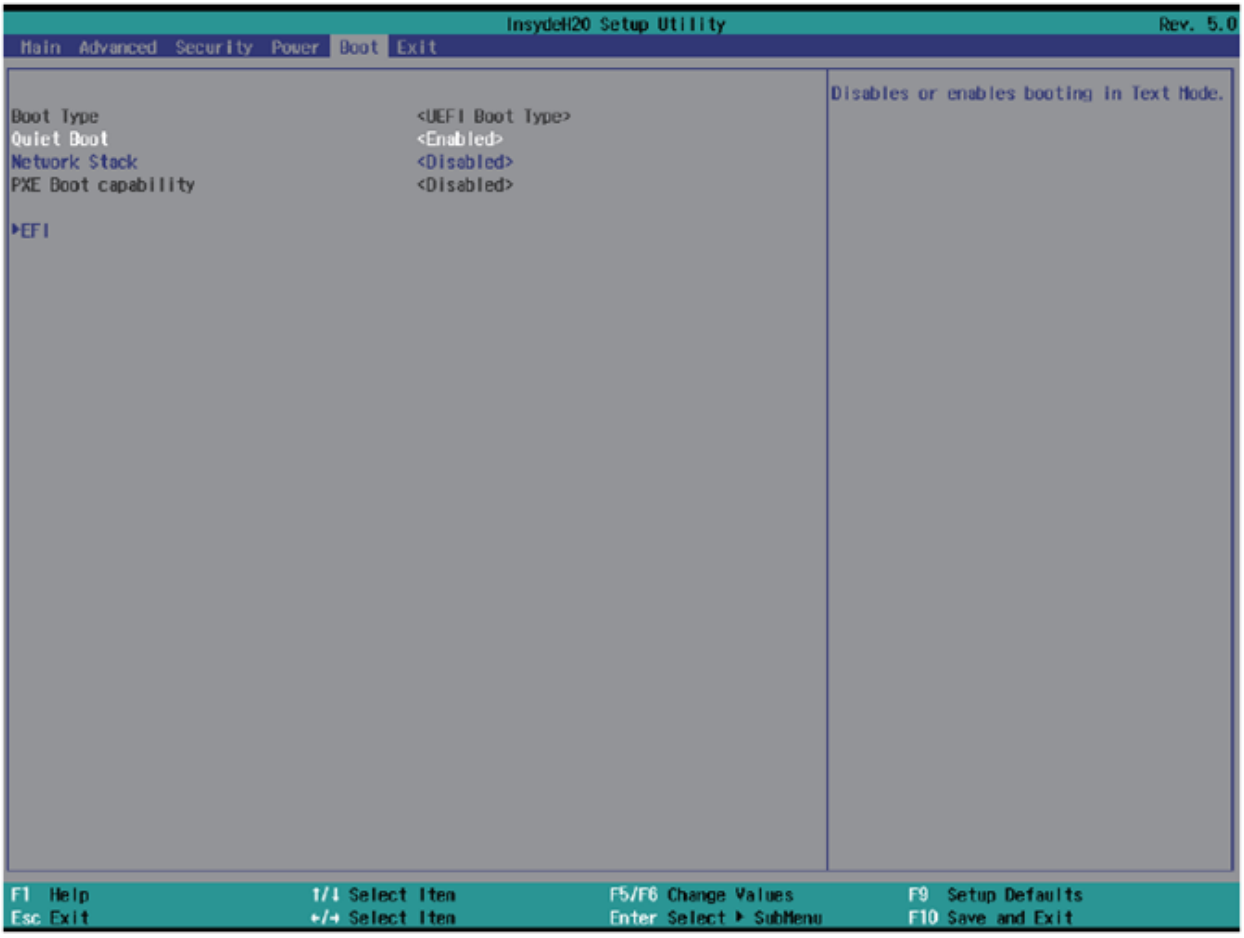
10.8 Power Management



Configure settings to manage power and wake capabilities:

- **Wake on LAN**: Enable the system to wake from sleep states (S3 or S5) via LAN.
  - Options: `S3`, `S5`, `S3 / S5`, `Disabled` (default)
- **ACPI S3 Support**: Decide if the system should support the ACPI S3 sleep state for energy saving.
  - Options: `Enabled`, `Disabled` (default)

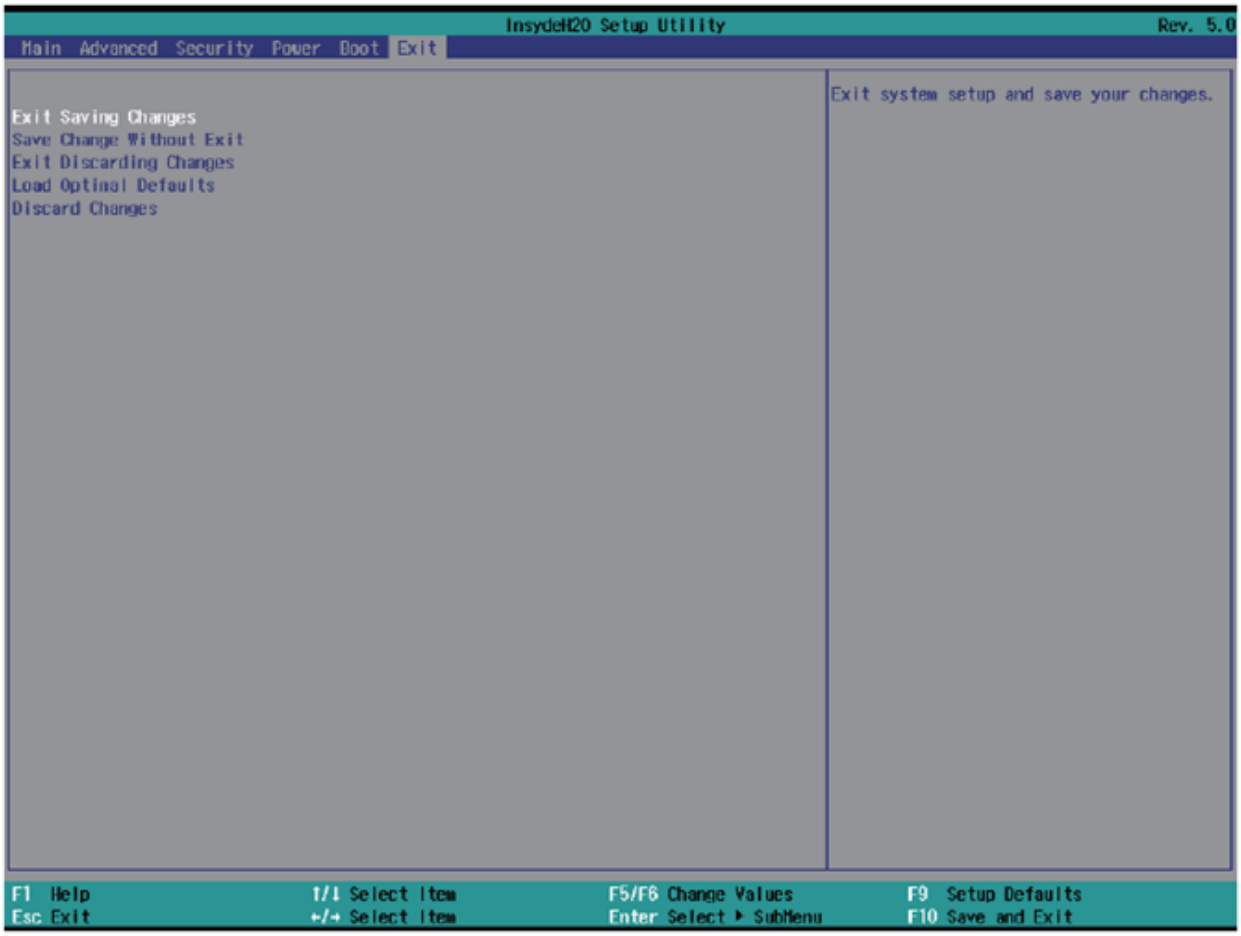
10.9 Boot Configuration



Manage settings that control the system's boot operations:

- **Boot Type**: Specifies that the Arrakis MK3 supports UEFI Boot only.
- **Quiet Boot**: Controls the display of messages during boot.
  - Options: `Enabled` (default), `Disabled`
- **Network Stack**: Enable this if using PXE functionality; otherwise, it should be disabled (default).
- **PXE Boot Capability**: Sets the protocol for PXE operations.
  - Options: `Disabled` (default), `UEFI: IPv4`, `UEFI: IPv6`
- **EFI Device Priority**: Determines which EFI-enabled storage device the system should boot from.

10.10 Exit Options



Manage your BIOS settings changes efficiently with these exit options:

- **Exit Saving Changes**: Saves all modifications and reboots the system, applying the new settings.
- **Save Changes Without Exit**: Saves your changes without rebooting, allowing you to continue adjusting settings.
- **Exit Discarding Changes**: Exits the BIOS without saving, reverting to previously saved settings, and reboots the system.
- **Load Optimal Defaults**: Resets the BIOS to the factory settings, which are optimized for general use.
- **Discard Changes**: Cancels any unsaved changes, reverting to the last saved configurations.

11 Driver Installation

The Arrakis Mk3 typically comes with an Operating System preinstalled for optimal performance.

Should you need to install or reinstall the operating system or other software on the Arrakis MK3 without a preinstalled system, all necessary drivers are readily available for download. Simply scan the QR code provided or visit the link below to access the full range of system drivers:

Download Drivers

To install the drivers, follow the on-screen instructions provided by the driver installation programs. This ensures your system is up-to-date and functioning efficiently.

12 Appendix A: Power Consumption

This appendix outlines the power consumption metrics for the Arrakis MK3 system under various operating conditions. The specific hardware configurations and operating parameters used during testing are listed below. These results should be considered as a reference only, as actual power consumption can vary based on software and hardware options.

Hardware Configuration:

- **CPU:** Intel Atom E3950
- **Memory:** 4GB DDR3L at 1866MHz
- **Operating System:** Windows 10 IoT 2019 LTSC
- **Storage:** 64GB mSATA
- **Benchmarking Tool:** Passmark

Power Consumption Measurements:

Voltage	Power Off	Startup (Max)	Startup (Stable)	Burn-in (Max)	Shutdown
12V	0.14A	0.95A	0.62A	1.10A	0.82A
24V	0.09A	0.50A	0.32A	0.57A	0.42A

Note: Power consumption values depend significantly on the configuration and usage of the system.

13 Appendix B: F75111N DIO & Watchdog Device

The Arrakis MK3, equipped with optional DIO ports, supports enhanced functionality through the use of a watchdog timer. This section provides guidance on how to program and utilize these features effectively.

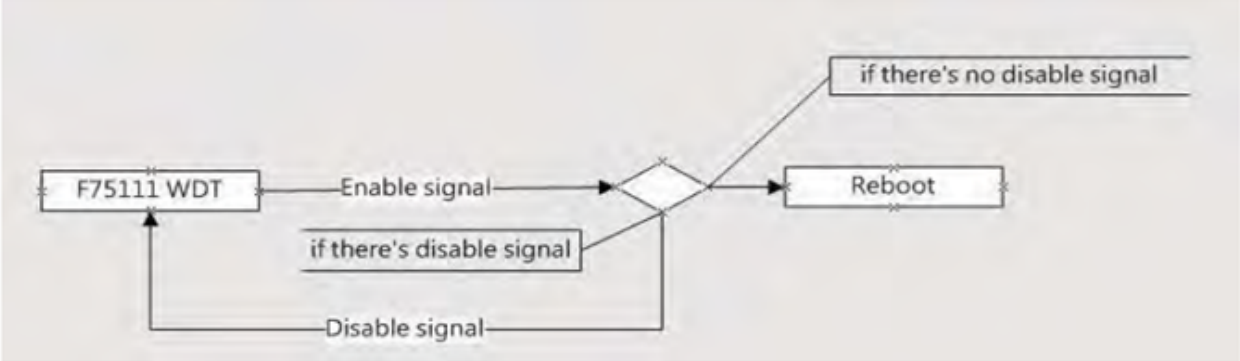
13.1 Watchdog Timer Usage in DOS

The necessary software resources for programming the watchdog timer can be accessed from the Driver Download section:

- **Source File:** `F75111_Dos_Src.rar`
- **Binary File:** `F75111_Dos_Bin.rar`
- **Access Credentials:** Username & Password: `sf`

13.1.1 Steps to Utilize the Demo Application:

1. Boot into the MS-DOS operating system.
2. Run the `75WDT.EXE` executable file.
3. Enter `1` to activate the watchdog timer, or `0` to deactivate it.
4. Specify the countdown duration in seconds for the timer, which will subsequently reset the computer.



13.1.2 Programming Example:

Below are examples of how to interact with the watchdog timer using I2C communication:

- **Activate and set the watchdog timer:**

```
WriteI2CByte(I2CADDR, CONFIG, 0x03); // Configure watchdog timer function
WriteI2CByte(I2CADDR, WDT_TIMER, timer); // Set timer range 0-255 seconds
WriteI2CByte(I2CADDR, WDT_TIMER_CTL, 0x73); // Enable timer in second and pulse mode
```

- **Deactivate the watchdog timer:**

```
WriteI2CByte(I2CADDR, WDT_TIMER_CTL, 0x00); // Disable watchdog timer
```

- **Sample code to pause operation using assembly language:**

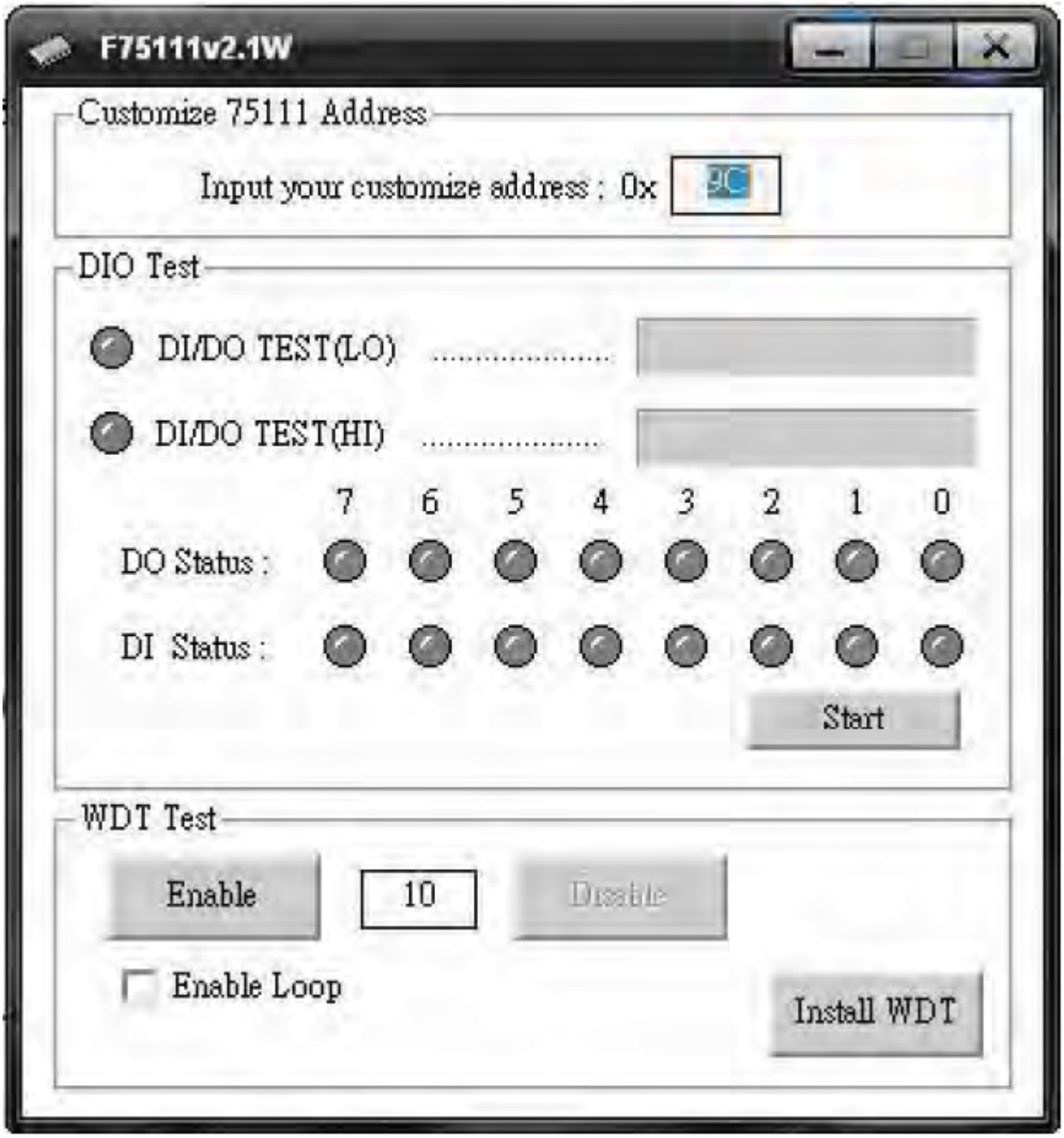
```
void pause(int time) {
    asm mov ah, 0h; // Set to read system time counter
    asm int 1ah;    // Read time from counter, store in DX
    asm add dx, time;
    asm mov bx, dx;
label:
    asm int 1ah;
    asm cmp bx, dx;
    asm jne label;
}
```

13.2 Watchdog Timer and DIO Configuration

You can find the necessary software resources in the Driver Download section under the DIO folder:

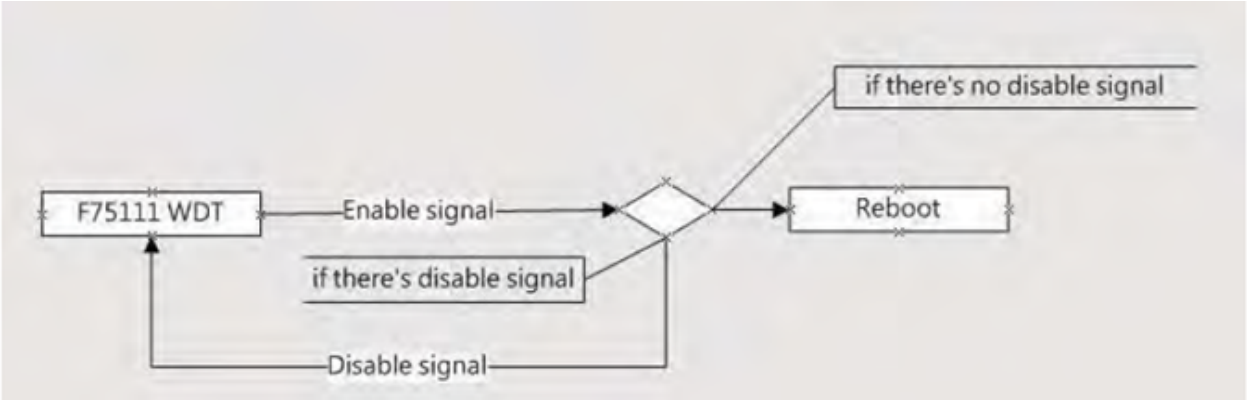
- **Source File**: `F75111_DIOSrc.rar`
- **Binary File**: `F75111_DemoBin.rar`
- **Access Credentials**: Username & Password: `sf`

13.2.1 Using the Demo Application



To test and configure the DIO and Watchdog Timer functions, follow these steps:

1. Click the `Start` button to begin testing the DIO functionality.
2. Click the `Enable` button to activate the Watchdog Timer (WDT).
3. Click the `Disable` button to deactivate the WDT.
4. To conduct a loop test, check the `Enable Loop` box and press `Enable`.
5. Use the `Install WDT` button to configure the system to auto-run this application at boot. Click again to remove the auto-run setting. An icon indicates when this setting is active.



13.2.2 Command Functions

- **Watchdog Timer Initialization**: Configure the initial internal F75111 port settings and enable necessary functions.
- **Digital Output (DO)**: Set digital output values.
- **Digital Input (DI)**: Retrieve digital input values.
- **Watchdog Timer Enable/Disable**: Activate or deactivate the Watchdog Timer.

Examples of Code Implementation:

1. Initialize Watchdog Timer and Ports:

```
// Initialize F75111 internal settings for input and output configurations
InitInternalF75111();
```

2. Set Output Values:

```
// Output a specific byte value to digital output
InterDigitalOutput(byteValue);
```

3. Retrieve Input Values:

```
// Get input values from digital input
BYTE inputStatus = InterDigitalInput();
```

4. Manage Watchdog Timer:

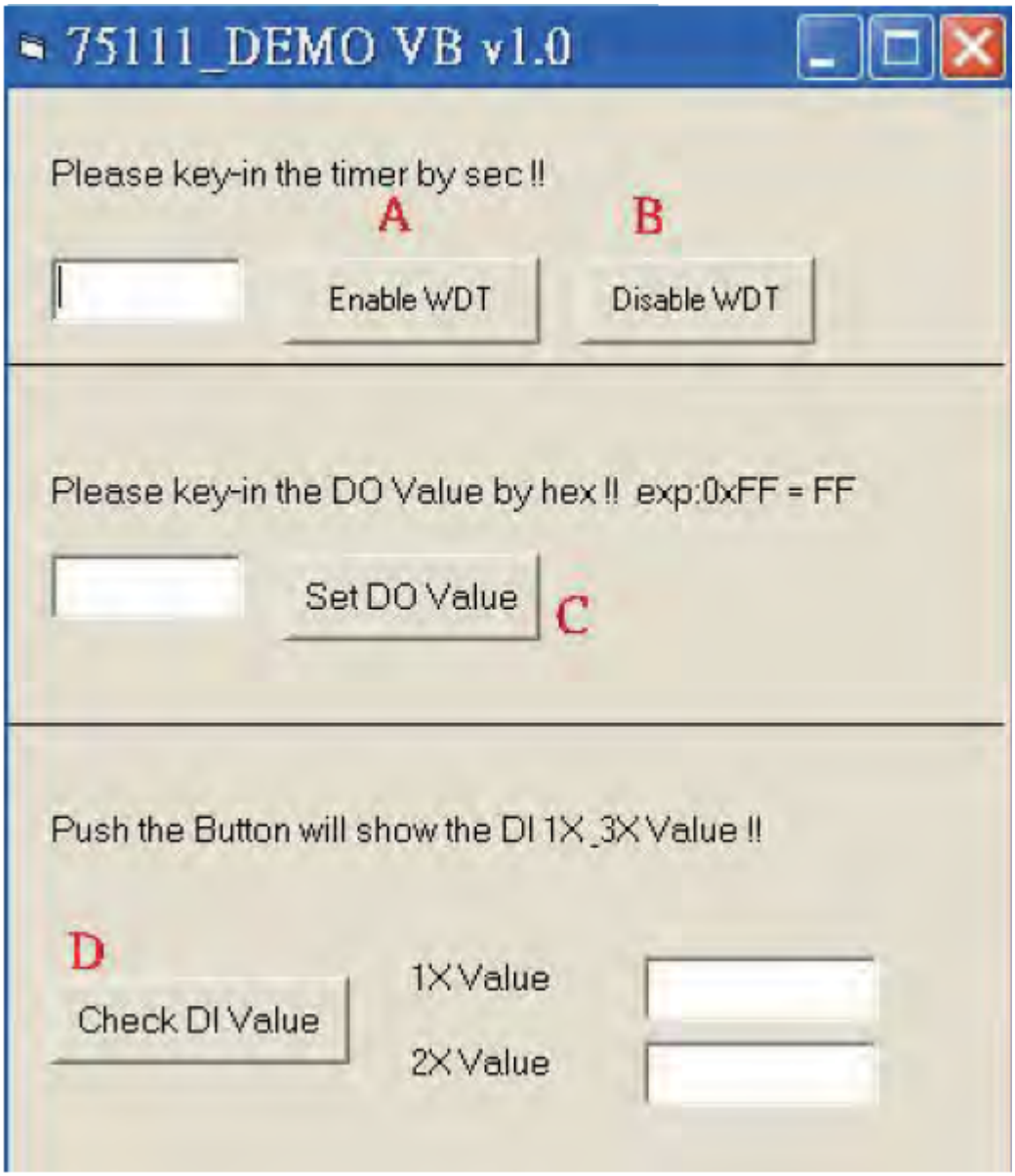
```
// Enable the Watchdog Timer with a specific timeout
F75111_SetWDTEnable(timerValue);
// Disable the Watchdog Timer
F75111_SetWDTDisable();
```

13.3 IO Device: F75111 VB6 under Windows

You can find the necessary software resources in the Driver Download section under the DIO folder:

- **Source File**: `75111_VB_v10.rar`
- **Binary File**: `75111_VB_Src.rar111_DemoBin.rar`
- **Access Credentials**: Username & Password: `sf`

13.3.1 How to Use the Demo Application



A. Enable WDT Timer: Enter the desired time in seconds, then the system will reboot after the specified time. **B. Disable WDT Timer**: Press the button to clear the WDT timer value. **C. Set DO Value**: Enter the DO value in hexadecimal and press the button. **D. Check DI Value**: The right-side text boxes display the DI 1X & 2X values when the button is pressed.

13.3.2 SDK Function Introduction

Function `EnableWDT`**:**

```
Function EnableWDT(timer As Integer)
    Call WriteI2CByte(&H3, &H3)
    Call WriteI2CByte(&H37, timer)
    Call WriteI2CByte(&H36, &H73)
End Function
```

Function `DisableWDT`**:**

```
Function DisableWDT()
    Call WriteI2CByte(&H36, &H0)
End Function
```

Function `SetDOValue`:

```
Function SetDOValue(dovalue As Integer)
    Call WriteI2CByte(&H23, &H0)
    Call WriteI2CByte(&H20, &HFF)
    Call WriteI2CByte(&H2B, &HFF)
    Call WriteI2CByte(&H21, dovalue)
End Function
```

Function `CheckDIValue`:

```
Function CheckDIValue()
    Dim GPIO1X As Integer
    Dim GPIO3X As Integer
    Dim DI1Xhex As String
    Dim DI3Xhex As String

    Call ReadI2CByte(&H12, GPIO1X)
    Call ReadI2CByte(&H42, GPIO3X)

    DI1Xhex = Hex(GPIO1X)
    DI3Xhex = Hex(GPIO3X)

    Text3.Text = "0x" + DI1Xhex
    Text4.Text = "0x" + DI3Xhex
End Function
```

13.4 Watchdog Timer and DIO under Linux

You can find the necessary software resources in the Driver Download section under the DIO folder:

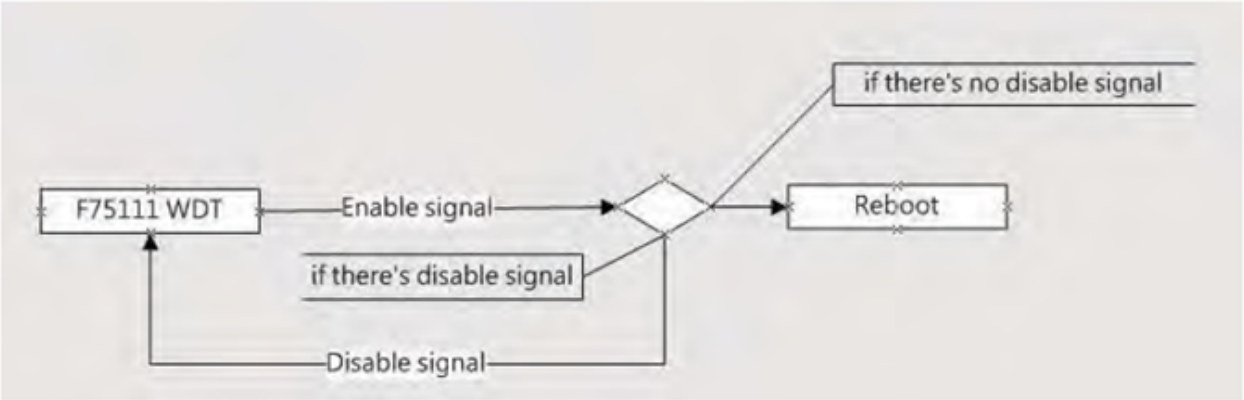
- **Source File**: `F75111v2.0L.tar.gz`
- **Binary File**: `F75111v2.0LBin.tar.gz`
- **Access Credentials**: Username & Password: `sf`

13.4.1 How to Compile Source Code

1. **Compile Source Code with Code::Blocks**
    - Install Code::Blocks with the command: `apt-get install codeblocks`
    - Open the existing project (`F75111.cbp`) in Code::Blocks and click the compile button
    - Add the option `'pkg-config --libs gtk+-2.0 gthread-2.0'` in `Project->Build Options->Linker Settings->Other linker options`
2. **Compile Source Code with `make`**
    - Navigate to the F75111 directory: `cd F75111`
    - Compile the source code: `make`
    - Execute the binary file: `src/f75111`

13.4.2 How to Use the Demo Application

1. Press the `Start` button to test the DIO function
2. Press the `Enable` button to test the WDT function
3. Press the `Disable` button to disable the WDT
4. Check the `Enable Loop` box and press `Enable` to perform a WDT loop test
5. Press `Install` to set the system to autorun this application when booting, and press `Uninstall` to remove it from autorun
6. If WDT is enabled, the system icon will blink



F75111 will send `F75111_SetWDTEnable(BYTE byteTimer)` with a parameter `timer`. If there is no disable signal (`F75111_SetWDTDisable()`) before the timer counts down to 0, the system will reboot. If a disable signal is received, it will resend the enable WDT signal to prevent a reboot loop.

13.4.3 Introduction

IO Function in `SMBus.c`:

```
void SMBusIoWrite(BYTE byteOffset, BYTE byteData) {
    outb(byteData, m_SMBusMapIoAddr + byteOffset);
}

BYTE SMBusIoRead(BYTE byteOffset) {
    DWORD dwAddrVal;
    dwAddrVal = inb(m_SMBusMapIoAddr + byteOffset);
    return (BYTE)(dwAddrVal & 0x0FF);
}
```

Initialize Internal F75111:

```
void F75111::InitInternalF75111() {
    this->Write_Byte(F75111_INTERNAL_ADDR, GPIO1X_CONTROL_MODE, 0x00); // Set GPIO1X to Input␣
↪function
    this->Write_Byte(F75111_INTERNAL_ADDR, GPIO3X_CONTROL_MODE, 0x00); // Set GPIO3X to Input␣
↪function
    this->Write_Byte(F75111_INTERNAL_ADDR, GPIO2X_CONTROL_MODE, 0xFF); // Set GPIO2X to Output␣
↪function
    this->Write_Byte(F75111_INTERNAL_ADDR, F75111_CONFIGURATION, 0x03); // Enable WDT OUT function
}
```

Set Output Value:

```
void F75111::InterDigitalOutput(BYTE byteValue) {
    BYTE byteData = 0;
    byteData = (byteData & 0x01) ? byteValue + 0x01 : byteValue;
    byteData = (byteData & 0x02) ? byteValue + 0x02 : byteValue;
    byteData = (byteData & 0x04) ? byteValue + 0x04 : byteValue;
    byteData = (byteData & 0x80) ? byteValue + 0x08 : byteValue;
    byteData = (byteData & 0x40) ? byteValue + 0x10 : byteValue;
    byteData = (byteData & 0x20) ? byteValue + 0x20 : byteValue;
    byteData = (byteData & 0x10) ? byteValue + 0x40 : byteValue;
    byteData = (byteData & 0x08) ? byteValue + 0x80 : byteValue; // Get value bit by bit
    this->Write_Byte(F75111_INTERNAL_ADDR, GPIO2X_OUTPUT_DATA, byteData); // Write byteData value␣
↪via GPIO2X output pin
}
```

Get Input Value:

```
BYTE F75111::InterDigitalInput() {
    BYTE byteGPIO1X = 0;
    BYTE byteGPIO3X = 0;
    BYTE byteData = 0;
    this->Read_Byte(F75111_INTERNAL_ADDR, GPIO1X_INPUT_DATA, &byteGPIO1X); // Get value from GPIO1X
    this->Read_Byte(F75111_INTERNAL_ADDR, GPIO3X_INPUT_DATA, &byteGPIO3X); // Get value from GPIO3X
    byteGPIO1X = byteGPIO1X & 0xF0; // Mask unuseful value
    byteGPIO3X = byteGPIO3X & 0x0F; // Mask unuseful value
    byteData = (byteGPIO1X & 0x10) ? byteData + 0x01 : byteData;
    byteData = (byteGPIO1X & 0x80) ? byteData + 0x02 : byteData;
    byteData = (byteGPIO1X & 0x40) ? byteData + 0x04 : byteData;
    byteData = (byteGPIO3X & 0x01) ? byteData + 0x08 : byteData;
    byteData = (byteGPIO3X & 0x02) ? byteData + 0x10 : byteData;
    byteData = (byteGPIO3X & 0x04) ? byteData + 0x20 : byteData;
    byteData = (byteGPIO3X & 0x08) ? byteData + 0x40 : byteData;
    byteData = (byteGPIO1X & 0x20) ? byteData + 0x80 : byteData; // Get correct DI value from␣
↪GPIO1X & GPIO3X
    return byteData;
}
```

Enable WatchDog:

```
void F75111_SetWDTEnable(BYTE byteTimer) {
    WriteByte(F75111_INTERNAL_ADDR, WDT_TIMER_RANGE, byteTimer); // Set WatchDog range and timer
    WriteByte(F75111_INTERNAL_ADDR, WDT_CONFIGURATION, WDT_TIMEOUT_FLAG | WDT_ENABLE | WDT_PULSE |␣
↪WDT_PSWIDTH_100MS);
    // Enable WatchDog, Setting WatchDog configure
}
```

Disable WatchDog:

```
void F75111_SetWDTDisable() {
    WriteByte(F75111_INTERNAL_ADDR, WDT_CONFIGURATION, 0x00); // Disable WatchDog
}
```