Arrakis Mk4 Series

Version:
v1.2.0

Date:
24.11.2025

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	2014 2019+A1:2021
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 2013+A2:2021+AC:2022
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 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
ETSI EN 301 908-1	IMT cellular networks; Harmonised Standard for access to radio spectrum; Part 1: Introduction and common requirements Release 15	V15.1.1

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:

- XMR2024RG255CGL
- N7NEM75T
- XMR2021EM05G
- RYK-WHFQ262ACNIBT
- 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-EM75T
- 6158A-FQ262ACNIBT
- 6158A-PET236ACNBT
- 10224A-2021EM05G

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 … 3	
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 12V 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

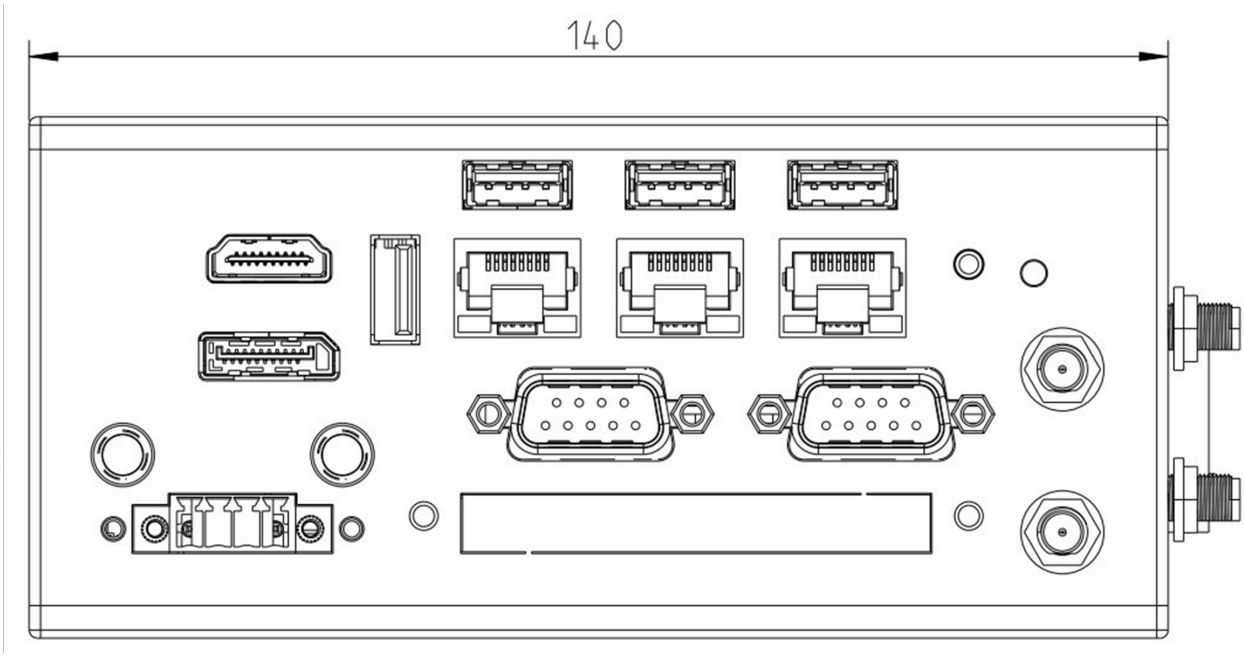
Feature	Specification	Details
Processor	CPU	Intel Atom® x6413E Processor, 1.5/3.0 GHz (Standard)
Memory	RAM	Up to 32GB DDR4 SoDIMM, 3200 MHz
Storage	NVMe	1x NVMe B+M Key, 2x PCIe 3.0 Lanes
	SATA	1x SATA DOM Connector
Security	TPM	TPM 2.0
I/O Ports	DisplayPort	1 port
	HDMI	1 port
	Gigabit Ethernet	3x RJ45 ports, 2.5 Gigabit, Intel i225/226-IT LAN chip
	USB 3.0	3 ports
	USB 2.0	1 port
	Serial Ports (RS232/422/485)	2 ports, with optional 2 additional RS232/422/485
Connectivity	Ethernet	3x (10/100/1000/2500 Base-T), Intel i225/226-IT LAN chip
	WLAN (optional)	Optional, via mPCIe
	WWAN (optional)	Optional 4G/5G
Expansion	SIM Slot	1x Nano SIM Slot, plus 2x optional Micro SIM Slots
Additional	Digital I/O and CAN	Optional Digital I/O, CAN available
	Watchdog Timer	System reset, 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	Power Supply	12-36V DC, 4-pin terminal block type and DC jack
	Power Adapter	Optional 60W, 24V/5A external, CR1220 CMOS Battery
Mounting	Options	Wall mount and DIN-Rail mounting kits available
Operating System	Compatibility	Windows 10/11, Ubuntu Linux, others upon request
Physical Build	Material/Color	Steel / Aluminum
	Ingress Protection	IP20
	Dimensions	64 x 140 x 92 mm
	Weight	800 g

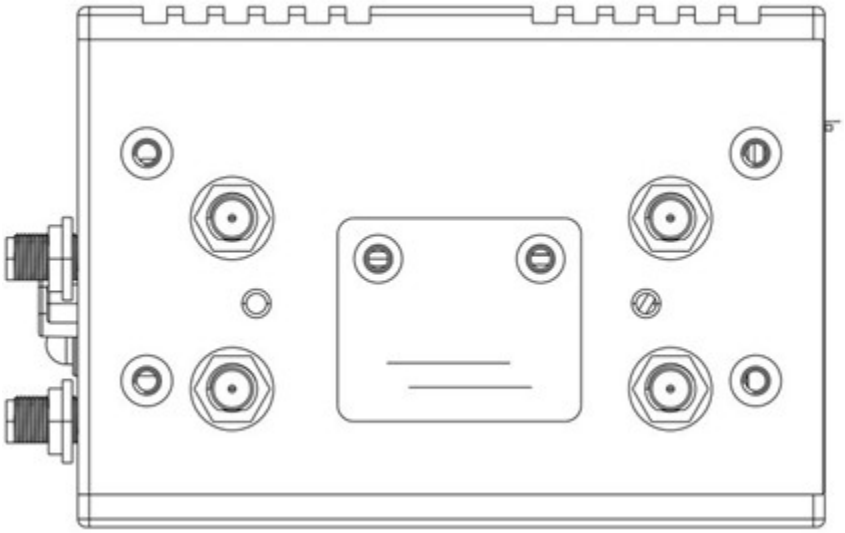
6 System Information

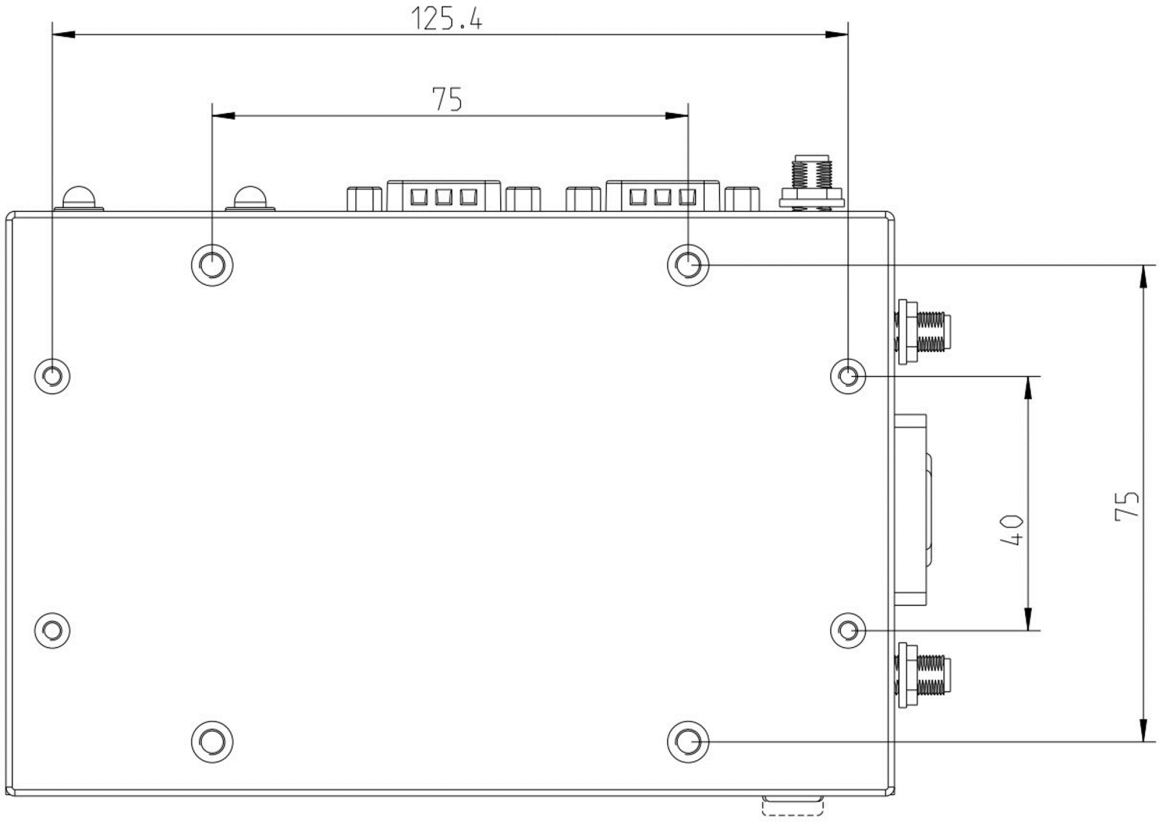
Being a powerful, yet small fanless system, the Arrakis Mk4 may reach very high surface temperatures in excess of 60°C/140°F with risk of injury. Users should ensure sufficient protection against touching.

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

6.1 System Drawing

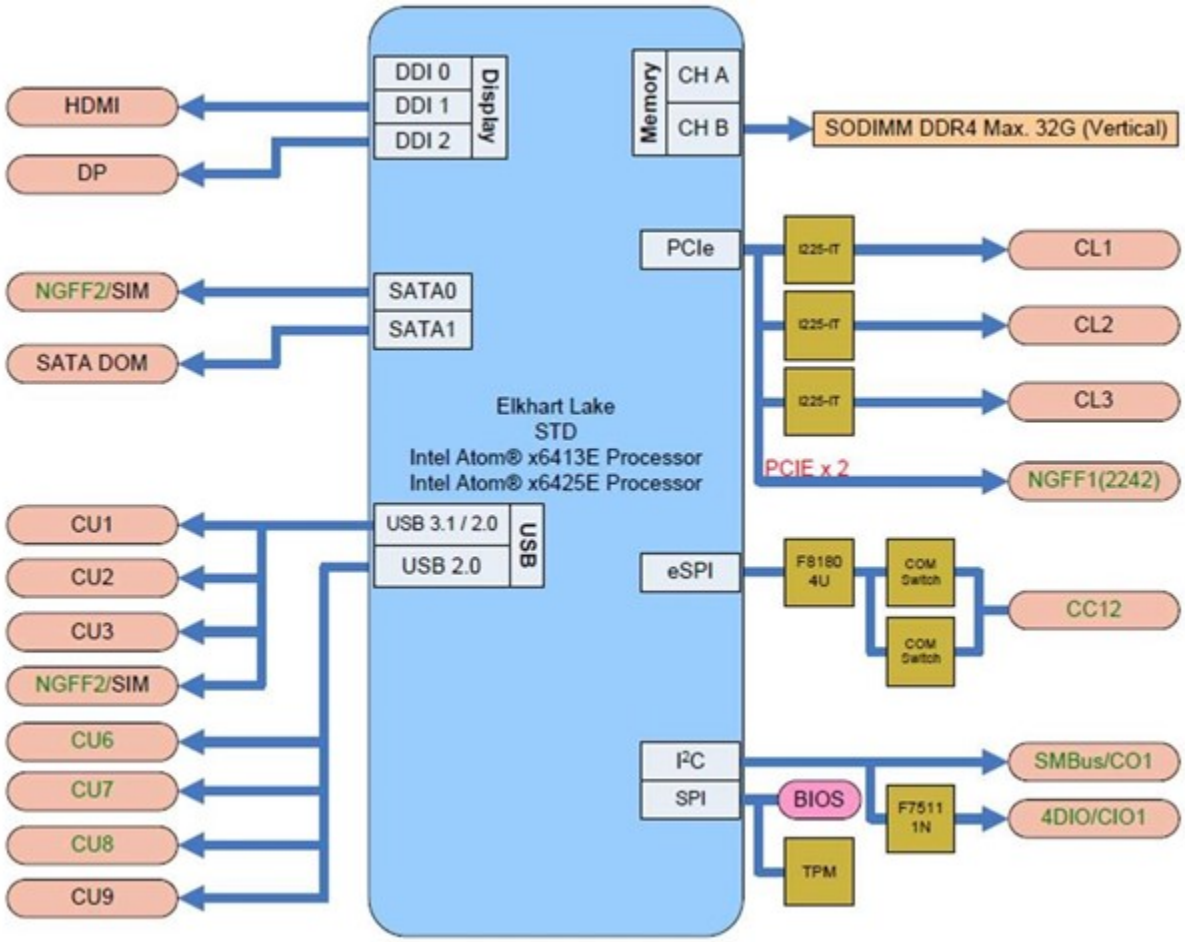





125.4
75
40
75

6.2 Mainboard Block Diagram

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



7 Power Supply

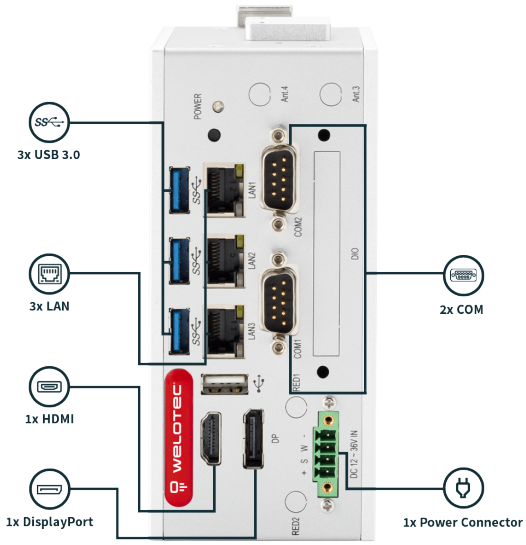
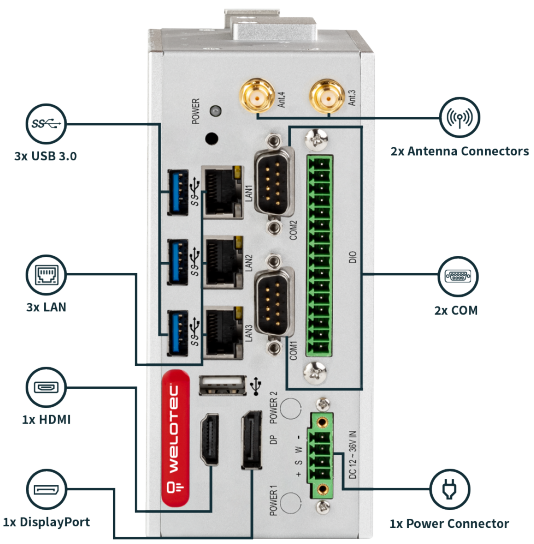
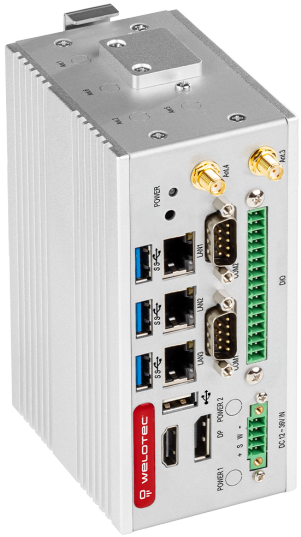
⚠ Please ensure no external voltage is applied to PSW! This could cause damage.

The Arrakis Mk4 can be powered using a **terminal block** or a **DC jack**, supporting a voltage range of **9–36V DC** for versatile connectivity - 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 Mk4 Series

Arrakis Mk4	Arrakis Mk4 (with optional Radio Module)
	
	
	

8.2 Antenna Configurations

Interface	ANT1	ANT2	ANT3	ANT4	ANT5	ANT6
LTE			Diversity	Main	GNSS	
5G		Diversity*	Diversity	Main	GNSS	Diversity
WiFi	X	(X)*				

*with 5G Antenna allocation is dependent on customer requirements

8.3 COM Port Pin out

RS232 Mode:

Pin	Description	Pin	Description
1	DCD	6	DSR
2	RXD	7	RTS
3	TXD	8	CTS
4	DTR	9	RI
5	GND		

RS422 Mode:

Pin	Description	Pin	Description
1	TX-	6	NC
2	TX+	7	NC
3	RX+	8	NC
4	RX-	9	NC
5	GND		

RS485 Mode:

Pin	Description	Pin	Description
1	TX-	6	NC
2	TX+	7	NC
3	NC	8	NC
4	NC	9	NC
5	GND		

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

The Arrakis Mk4 may contain the following RF Modules:

- Quectel EM05-G
- Quectel RG255C-GL
- Sierra Wireless EM7590
- Sierra Wireless MC7430
- SparkLAN WZ-WNFQ-262ACNI(BT)
- SparkLAN WZ-WPET-236ACN(BT)

9.1 LTE

Quectel EM05-G	Supported Bands
LTE	FDD B1/ B2/ B3/ B4/ B5/ B7/ B8/ B12/ B13/ B14/ B18/ B19/ B20/ B25/ B26/ B28/ B66/ B71 TDD B38/ B39/ B40/ B41
WCDMA	B1/ B2/ B4/ B5/ B6/ B8/ B19

Quectel RG255C GL	Supported Bands
LTE	FDD B1/ B2/ B3/ B4/ B5/ B7/B8/ B12/ B13/ B14/ B17/ B18/ B19/ B20/ B25/ B26/ B28/ B30/ B66/ B70/ B71 TDD B34/ B38/ B39/ B40/ B41/ B42/ B43/ B48 DL 2x2 MIMO B1/ B2/ B3/ B4/ B5/ B7/ B12/ B13/ B14/ B17/ B18/ B19/ B20/ B25/ B26/ B28/ B30/ B34/ B38/ B39/ B40/ B41/ B42/ B43/ B48/ B66/ B71/ B71
5G	NR 3GPP Release 17 RedCap SA operation, Sub-6 GHzNRSA n1/ n2/ n3/ n5/ n7/ n8/ n12/ n13/ n14/ n18/ n20/ n25/ n26/ n28/ n30/ n38/ n40/ n41/ n48/ n66/ n70/ n71/ n77/ n78/ n79 DL 2x2 MIMO n1/ n2/ n3/ n5/ n7/ n8/ n12/ n13/ n14/ n18/ n20/ n25/ n26/ n28/ n30/ n38/ n40/ n41/ n48/ n66/ n70/ n71/ n77/ n78/ n79

Sierra Wireless EM7590	Supported Bands
LTE	FDD B1/ B2/ B3/ B4/ B5/ B7/ B8/ B12/ B13/ B14/ B18/ B19/ B20/ B25/ B26/ B28 B29/ B32/ B66 /B71 TDD B38/ B39/ B40/ B41 B42/ B43/ B48
WCDMA	B1/ B2/ B4/ B5/ B6/ B8/ B9/ B19

Sierra Wireless MC7430	Supported Bands
LTE	FDD B1/ B3/ B5/ B7/ B8/ B18/ B19/ B21/ B28TDD B38/ B39/ B40/ B41
WCDMA	B1/ B5/ B6/ B8/ B9/ B19
TD-SCDMA	B39

9.2 WiFi

9.2.1 SparkLAN WZ-WNFQ-262ACNI(BT)

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

9.2.2 SparkLAN WPET-236ACN(BT)

WiFi Output Power & Sensitivity

IEEE Standard	Data Rate	Tx ± 2dBm	Rx Sensitivity
802.11b	11Mbps	15dBm	-80dBm
802.11g	54Mbps	14dBm	-70dBm
802.11n / 2.4GHz (HT20)	MCS7	13dBm (1TX)16dBm (2TX)	-61dBm
802.11n / 2.4GHz (HT40)	MCS7	13dBm (1TX)16dBm (2TX)	-61dBm
802.11a	54Mbps	13dBm	-70dBm
802.11n / 5GHz (HT20)	MCS7	12dBm (1TX)15dBm (2TX)	-60dBm
802.11n / 5GHz (HT40)	MCS7	12dBm (1TX)15dBm (2TX)	-60dBm
802.11ac (VHT80)	MCS9	9dBm (1TX)12dBm (2TX)	-51dBm
Bluetooth	3Mbps	0 Output Power 4 dBm	<0,1%BER at -70dBm>

Notes

- **Down/RX:** Refers to the downlink frequency range.
- **Up/TX:** 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) resides in the Flash Memory on your motherboard, serving as the essential link between hardware and the operating system. When the computer starts, the BIOS takes control, performing the POST (Power-On Self Test) to verify the functionality of hardware components. After detecting and configuring hardware parameters, the BIOS hands over control to the operating system. As the central communication channel between hardware and software, the BIOS ensures system stability and peak performance.

In the BIOS setup menu, various configuration options are available. Below are the navigation keys for modifying these settings:

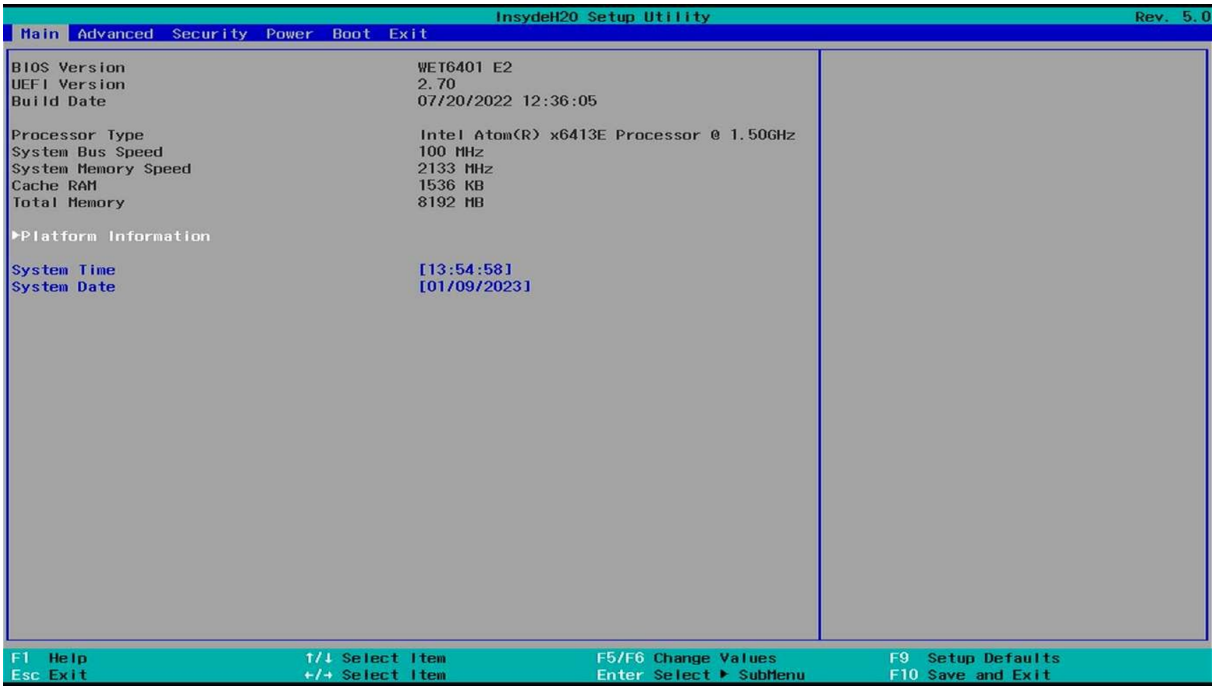
- **Esc:** Exit the BIOS Setup.
- **Arrow keys (↑↓←→):** Navigate through options.
- **F10:** Save changes and exit the setup.
- **Page Up/Page Down or +/-:** Modify values for the selected option.

10.2 Accessing BIOS

To enter the BIOS Setup:

1. Power on the system and press the `Del` key immediately.
2. If you miss the initial prompt, restart the system by turning it off and back on, or use `Ctrl` + `Alt` + `Delete` for a soft reboot.

10.3 BIOS Menu and Function Keys



The BIOS menu is organized into multiple tabs, each offering distinct configuration options. Use the following keys to navigate and modify settings:

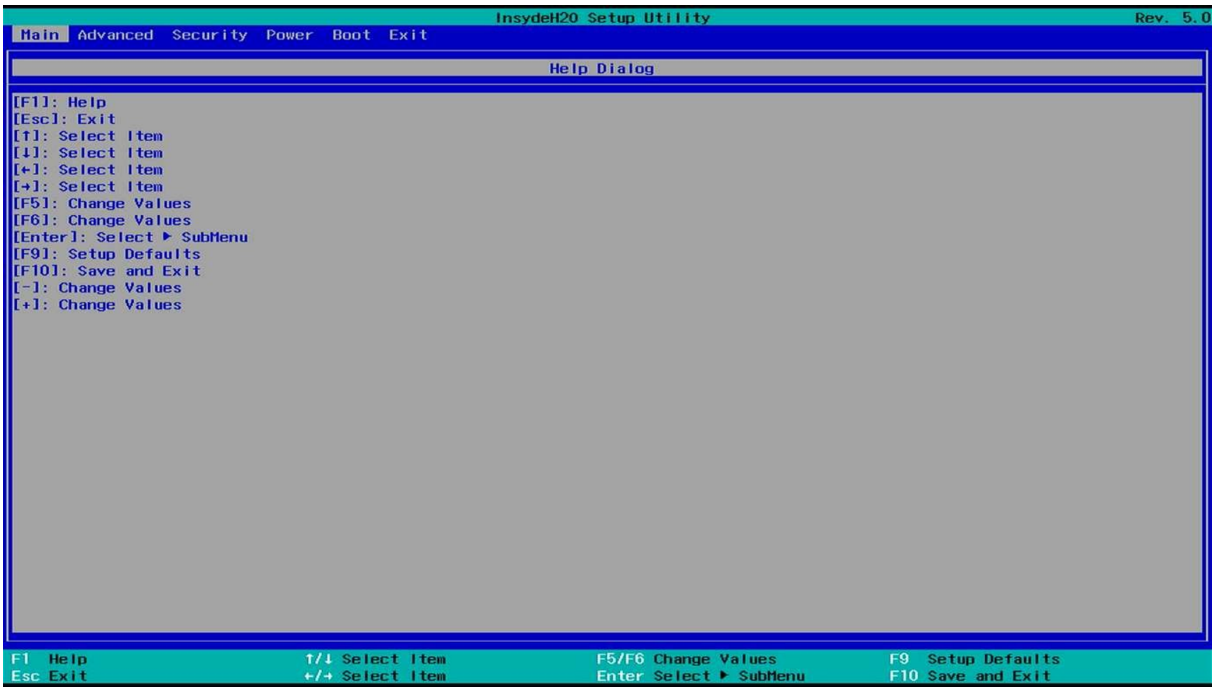
- **Navigation:**
  - Use ← and → to switch between tabs.
  - Use ↑ and ↓ to highlight menu options.
- **Selection and Modification:**
  - Press `Enter` to select options for editing.
  - Adjust values using + or − keys.
- **Shortcut Keys:**
  - `F1`: Displays general help.
  - `F2`: Restores the previous value.
  - `F3`: Loads optimized default settings.
  - `F4`: Saves changes and resets the system.
  - `Esc`: Exits the BIOS Setup.

10.3.1 Menu Tabs Overview

- **Main:** Adjust basic system settings.
- **Advanced:** Configure advanced system options.
- **Security:** Set BIOS passwords for added security.
- **Power:** Manage ACPI and wake device settings.
- **Boot:** Control boot sequence and related settings.
- **Exit:** Save, discard, or restore default settings before exiting.

The selected menu is highlighted for clarity.

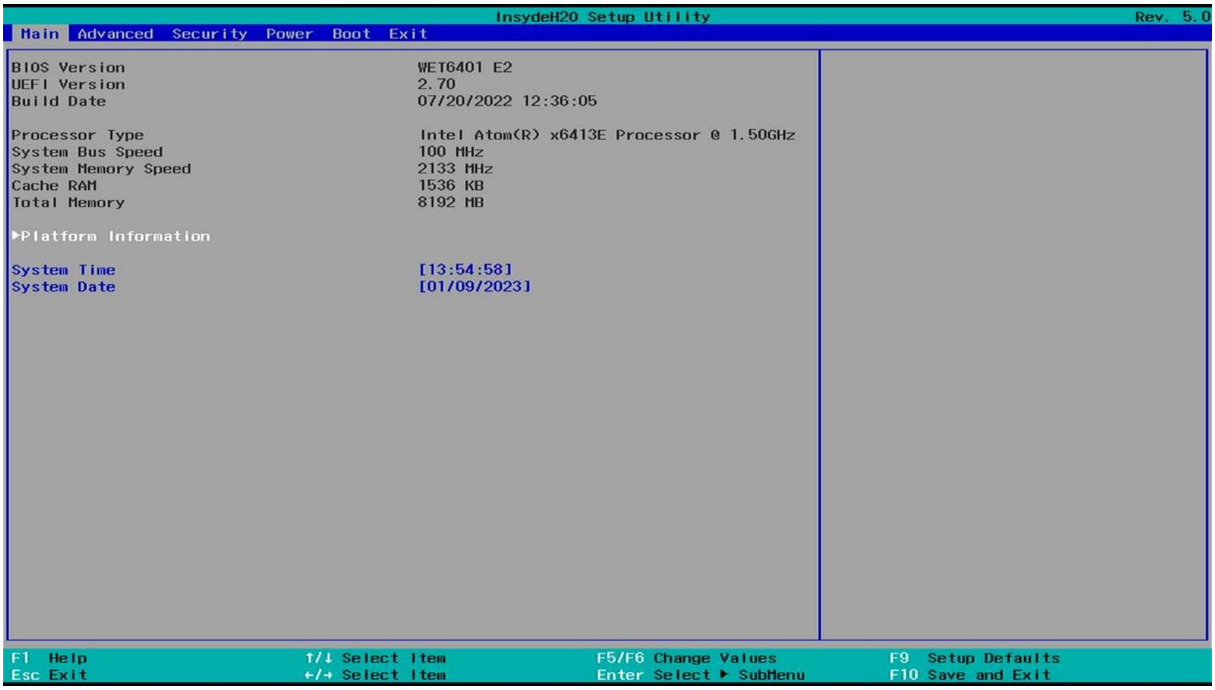
10.4 BIOS Help



For assistance with BIOS settings, press `F1`. This displays a detailed help window with information about the highlighted option, the available settings, and navigation tips. Press `Esc` to close the Help window.

10.5 Menu Options

10.5.1 Main Menu

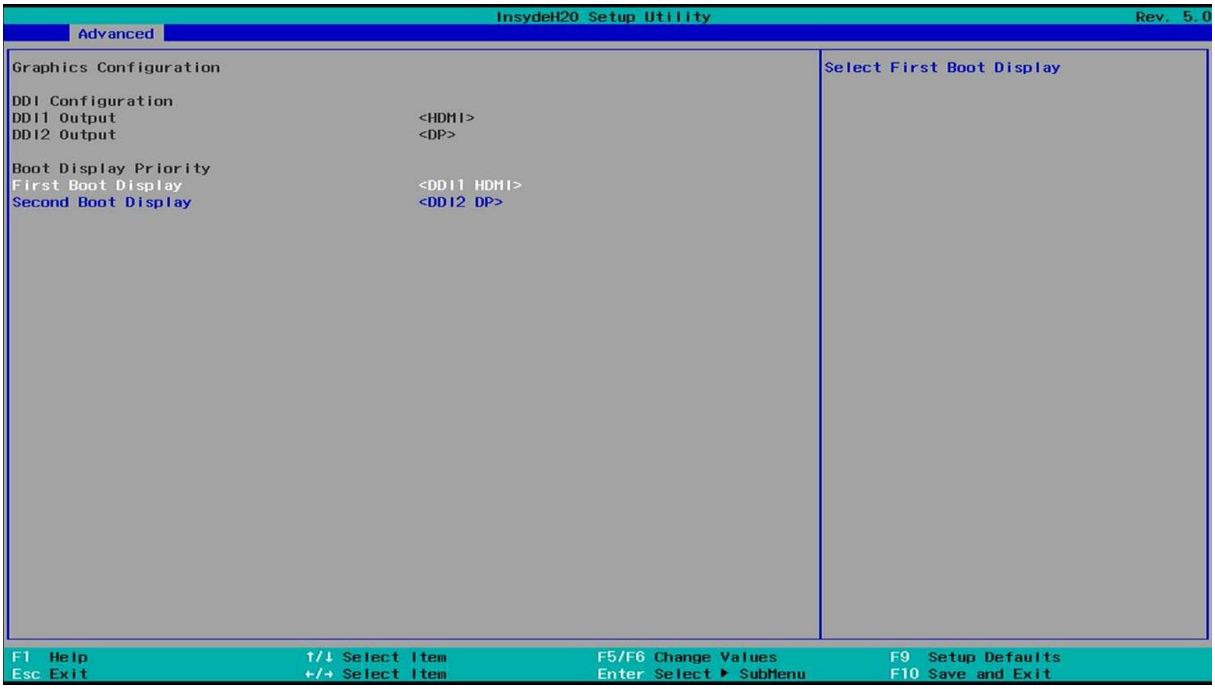


The **Main** tab displays basic system information and allows you to adjust key settings:

- **System Date:** Set the system's date. Use the `Tab` key to switch between day, month, and year fields.
- **System Time:** Adjust the system clock. Use `Tab` to navigate between hour, minute, and second fields.

10.6 Advanced BIOS Settings

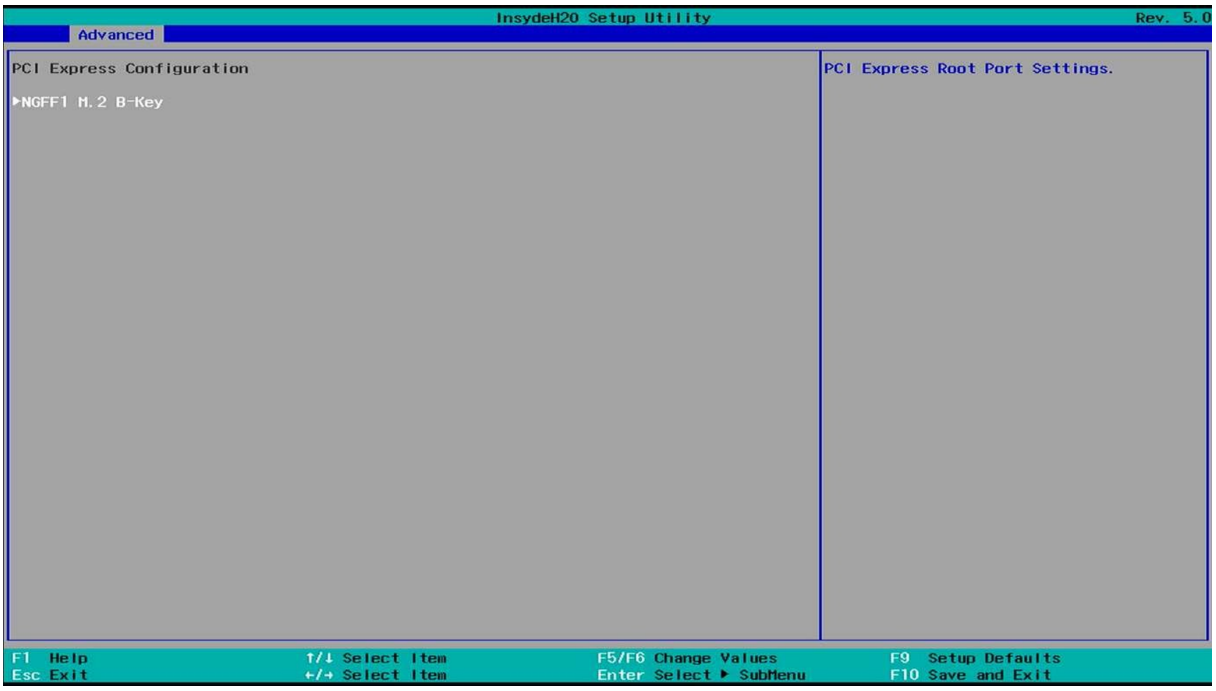
10.6.1 Graphics Configuration



Manage display settings to optimize the graphics output:

- **First Boot Display:** Select the primary display for boot. Options include eDP, DDI1 HDMI, DDI2 HDMI (default is HDMI).
- **Second Boot Display:** Set the secondary display priority. Options include DDI1 HDMI, DDI2 HDMI (default is DP).

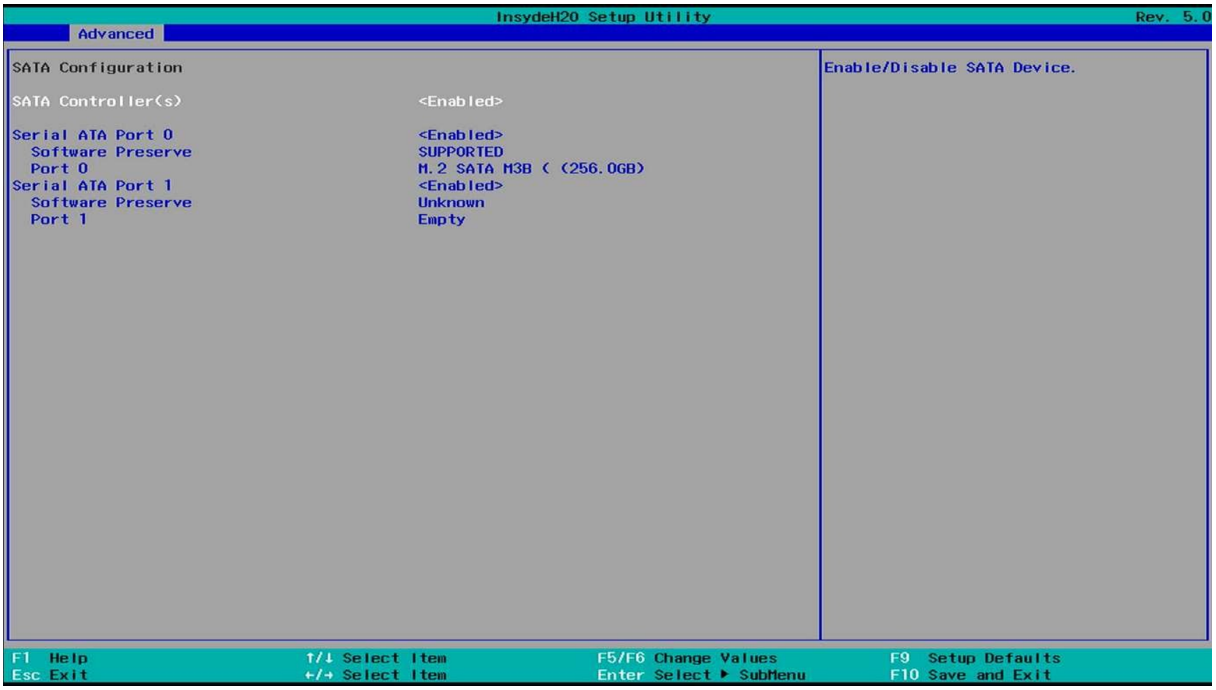
10.6.2 PCI Express Configuration



Control the functionality of PCI Express slots:

- **PCIe Slots:** Enable or disable specific PCI Express slots.
- **Speed Settings:** Configure the PCIe slot speed. Available options include Auto, Gen1, Gen2, and Gen3.

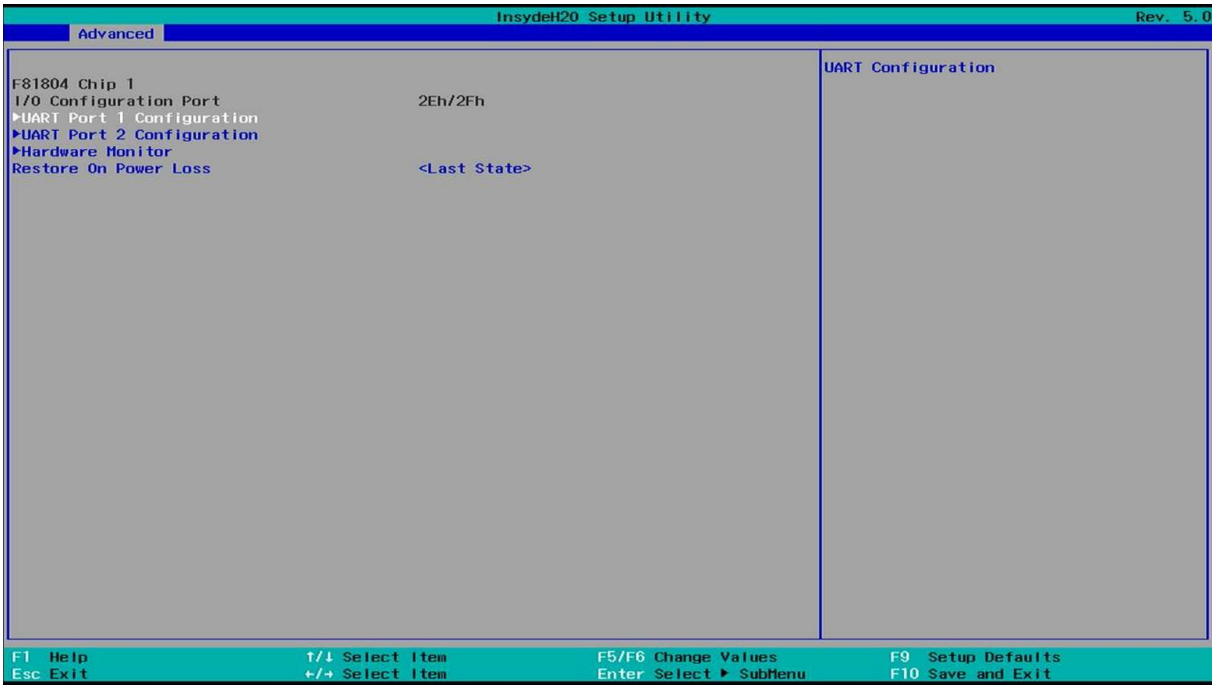
10.6.3 SATA Drives Configuration



Enable or disable SATA interfaces and manage connected drives:

- **SATA1 & NGFF1 M.2 Devices:** Toggle the activation of these interfaces for connected storage devices.

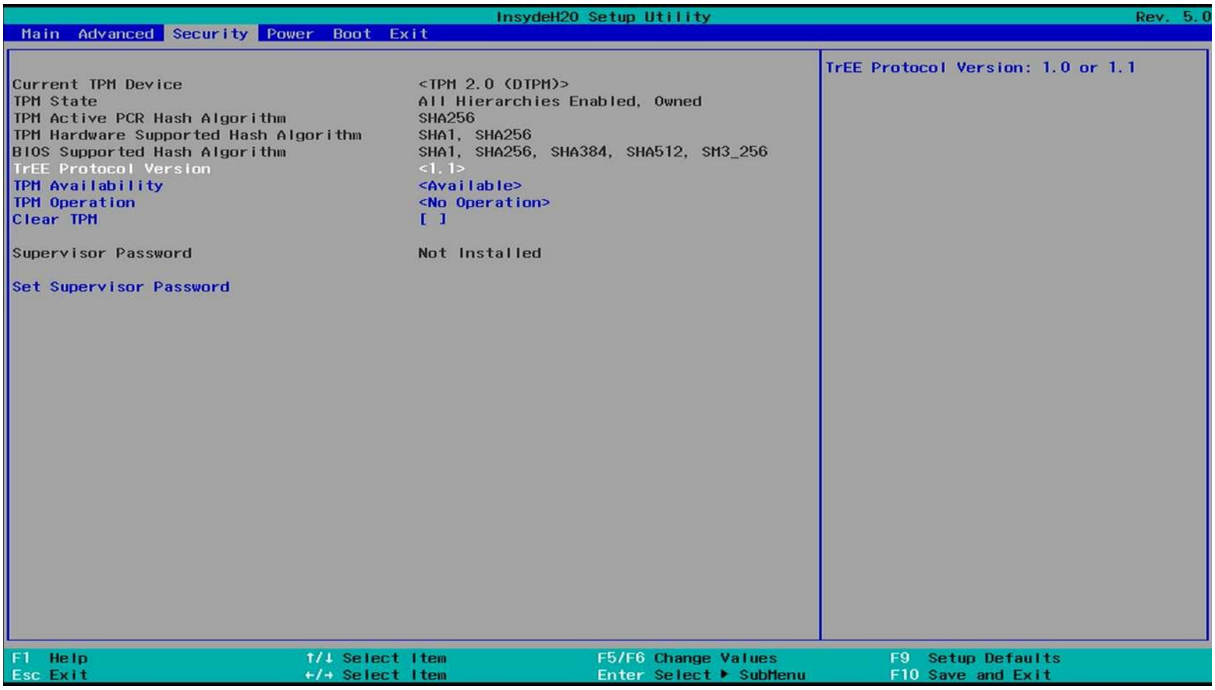
10.6.4 SIO Configuration (FINETEK 81804)



Configure serial ports and system recovery settings:

- **Serial Ports 1/2:** Enable or disable COM1 and COM2 ports. Default is Enabled.
- **Base I/O Address / Interrupt:** Set custom I/O addresses and IRQs:
  - Default for COM1: `IO=3F8h; IRQ=4`
  - Default for COM2: `IO=2F8h; IRQ=3`
- **Restore on Power Loss:**
  - **Last State** (default): Restores the previous system state after power is restored.
  - **Always On:** The system powers on automatically.
  - **Always Off:** The system remains off after power loss.

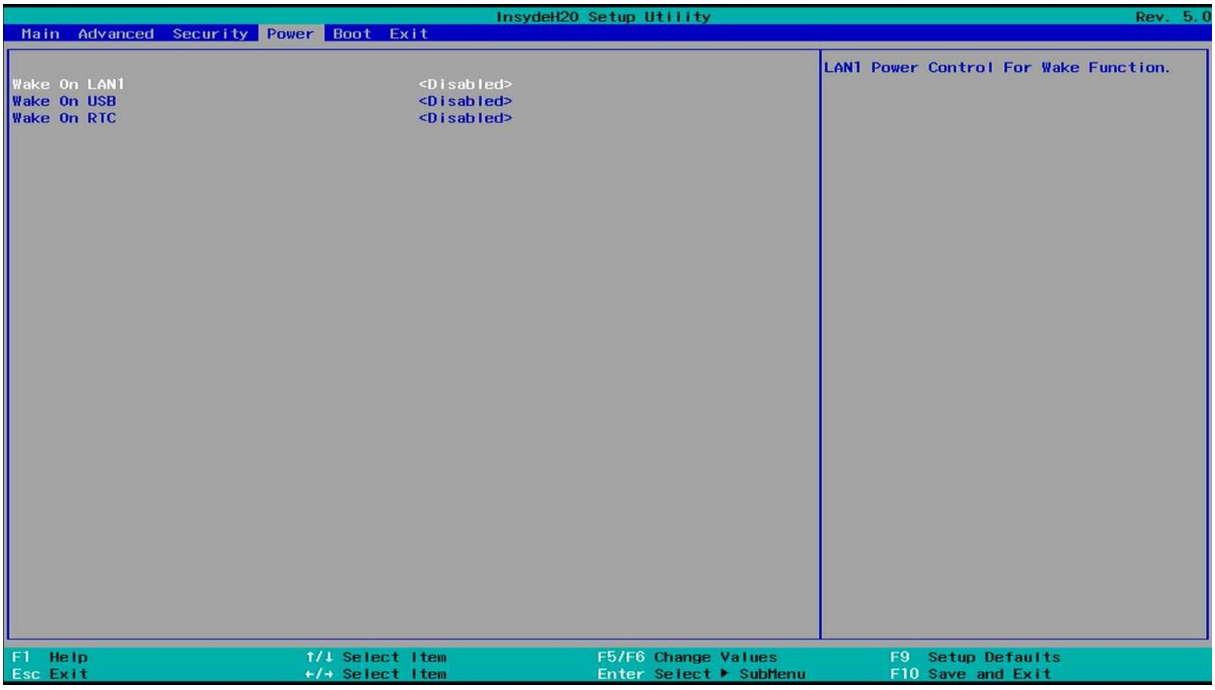
10.7 Security Settings



Set up passwords to protect BIOS access:

- **Supervisor Password:** Create or modify a password:
  1. Select “Supervisor Password.”
  2. Enter a password (3–10 characters).
  3. Press `Enter` to confirm.

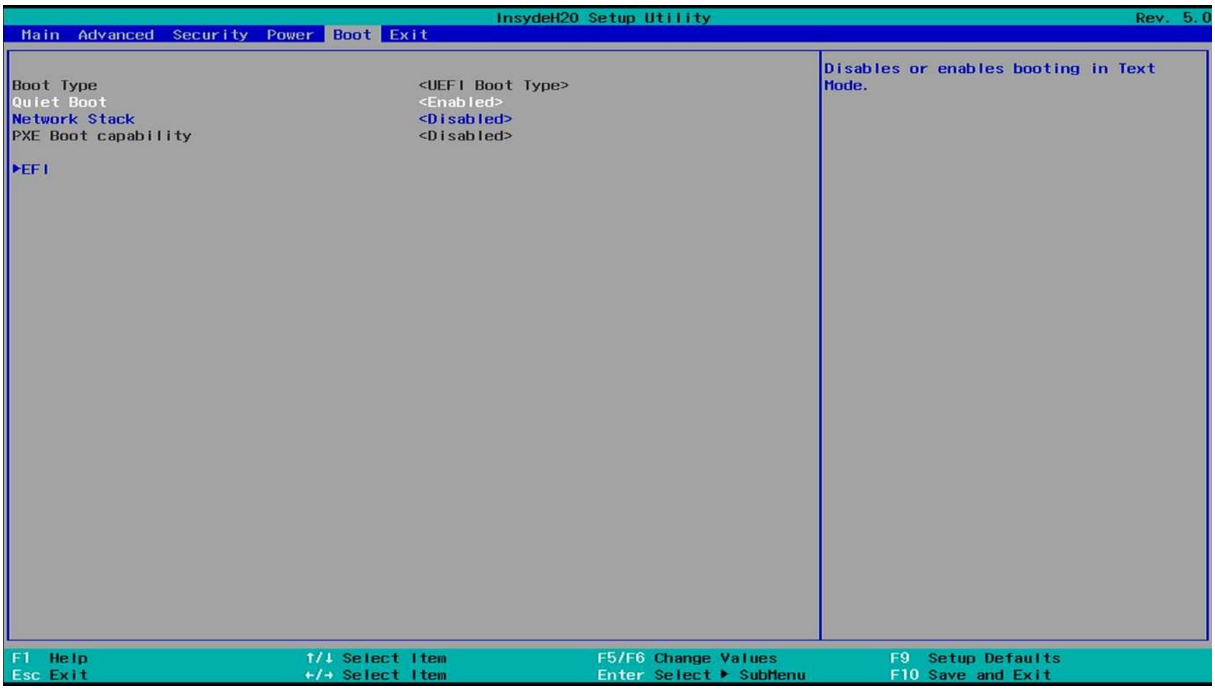
10.8 Power Management



Configure power-related settings:

- **Wake on LAN:** Enable the system to wake from S3/S5 states via LAN. Options include S3, S5, S3/S5, and Disabled (default).
- **ACPI S3:** Enable or disable the ACPI S3 sleep state. Default is Disabled.

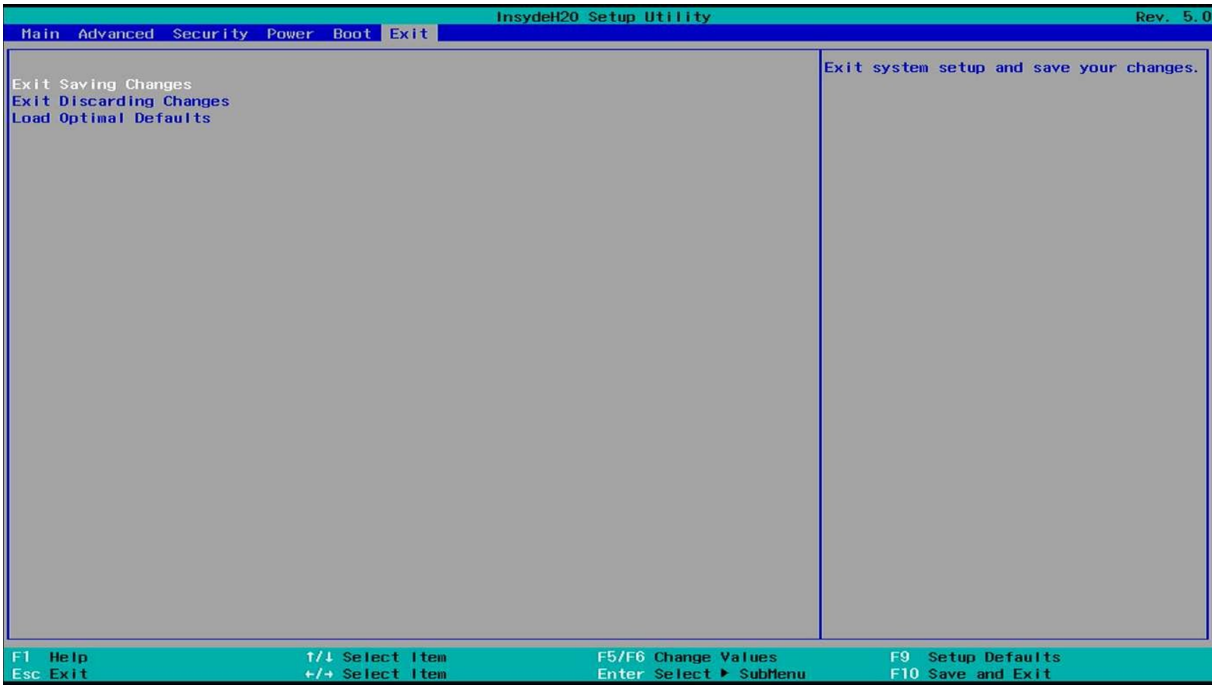
10.9 Boot Settings



Manage system boot priorities and behavior:

- **Boot Type:** Supports UEFI Boot only.
- **Quiet Boot:** Choose whether to display boot messages (`Enabled` by default).
- **PXE Boot Capability:** Select the network protocol for PXE boot:
  - Disabled (default), UEFI IPv4, UEFI IPv6.
- **EFI Boot Priority:** Specify the EFI storage device to boot from, displayed only if EFI is detected.

10.10 Exit Options



Choose how to save or discard changes made in the BIOS:

- **Exit Saving Changes:** Save all changes and reboot the system.
- **Save Changes Without Exit:** Save changes but remain in the BIOS.
- **Exit Discarding Changes:** Reboot the system without saving changes.
- **Load Optimal Defaults:** Restore factory default settings.
- **Discard Changes:** Cancel all unsaved changes.

11 Driver Installation

The Arrakis Mk4 is usually shipped with an Operating System preinstalled (recommended)

In case you have chosen to purchase an Arrakis Mk4 without preinstalled operating system or need to reinstall, you can download all available System drivers from this address:

To Install the Drivers, please execute the driver installation programs according to the on-screen instructions.

12 Appendix A: Power Consumption

12.1 System Specifications

Component	Details
CPU	Intel® Atom® x6413E
RAM	DDR4 8GB, 2400MHz
Operating System	Windows 10 IoT 2019 LTSC
Test Program	PassMark® Performance Test
Storage (NVMe)	64GB

Note: Specifications are for reference purposes only and may vary based on system configuration.

12.2 Power Consumption Data

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 varies based on hardware configuration, connected peripherals, and software applications.

13 Appendix B: F75111N DIO & Watchdog Device

The Arrakis Mk4 system provides optional DIO (Digital Input/Output) ports. This appendix explains the programming of these features, focusing on the Watchdog Timer under DOS.

13.1 Watchdog Timer Setup for DOS

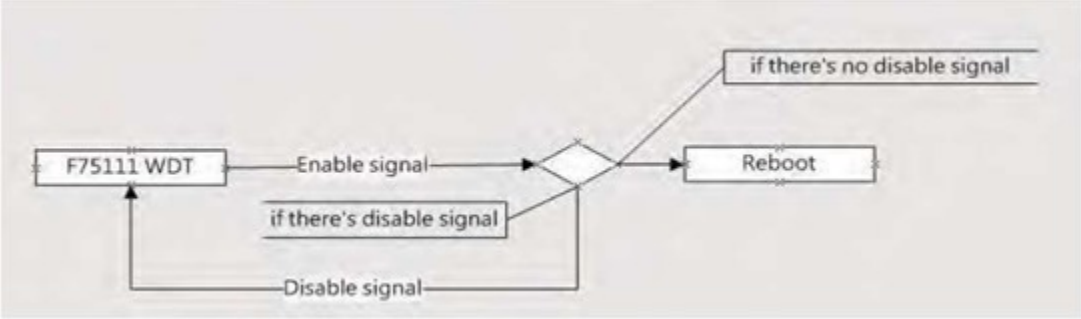
You can access the necessary source and binary files here.

- **Source file:** `F75111_Dos_Src.rar`
- **Binary file:** `F75111_Dos_Bin.rar`

13.1.1 Using the Demo Application

To use the Watchdog Timer demo application, follow these steps:

1. Boot the system into the MS-DOS operating system.
2. Locate and run the `75WDT.EXE` binary file.
3. When prompted:
   - Input `1` to enable the Watchdog Timer.
   - Input `0` to disable it.
4. Enter the desired countdown duration (in seconds) for the timer. When the countdown completes, the system will reset automatically.



13.1.2 Introduction

Using the Watchdog Timer Demo

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

Alternatively:

```
WriteI2CByte(I2CADDR, WDT_TIMER_CTL, 0x00);
```

Pause Function Example

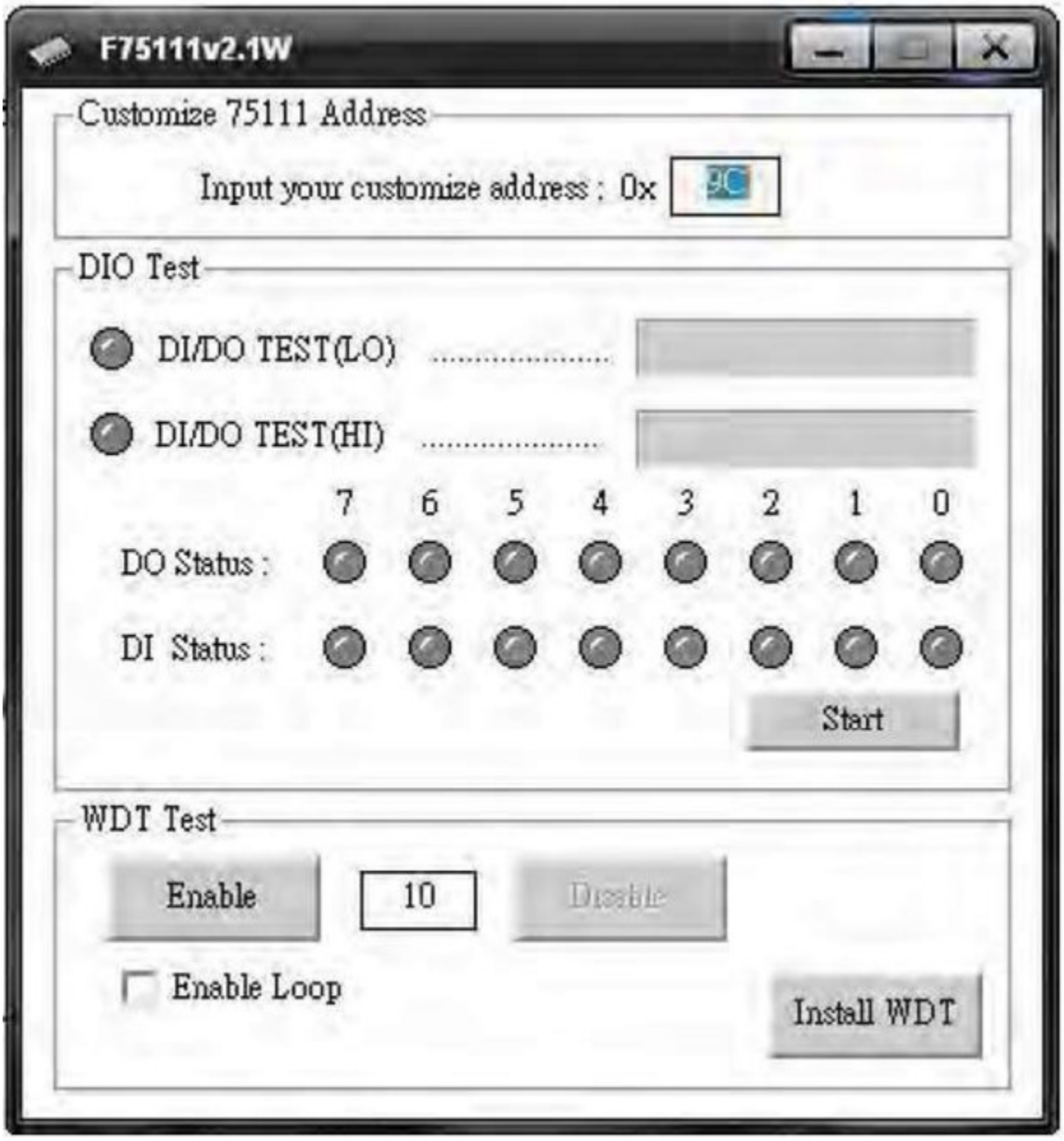
```
void pause(int time) {
    asm mov ah,0h; // Read system time counter
    asm int 1ah;
    asm add dx,time;
    asm mov bx,dx;
label:
    asm int 1ah;
    asm cmp bx,dx;
    asm jne label;
}
```

13.2 Watchdog Timer and DIO under Windows

You can access the necessary source and binary files here.

- **Source file:** `F75111_DIOSrc.rar`
- **Binary file:** `F75111_DemoBin.rar`

13.2.1 How to Use the Demo Application



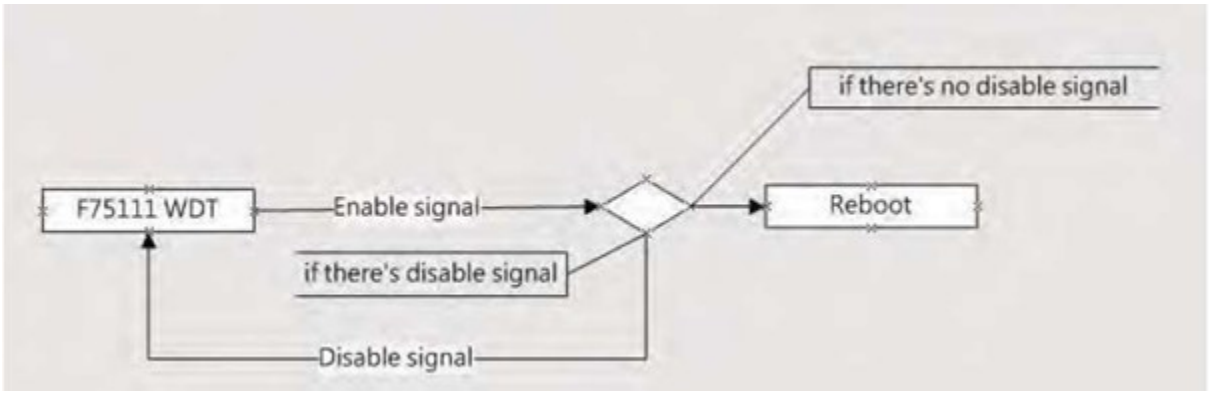
13.2.2 Using the Demo Application

Follow these steps to operate the DIO and Watchdog Timer (WDT) functions:

1. **Test the DIO Function:**
   - Press **Start** to begin testing the DIO functionality.
2. **Enable the Watchdog Timer:**
   - Press **Enable** to activate the Watchdog Timer (WDT).
3. **Disable the Watchdog Timer:**
   - Press **Disable** to deactivate the WDT.

4. **Perform a WDT Loop Test:**
   - Check the **Enable Loop** box, then press **Enable** to initiate a loop test for the WDT.
5. **Configure Autorun for the Application:**
   - Use **Install WDT** to set up the application to automatically run at system startup.
   - Press **Install WDT** again to remove the autorun configuration.

When the Watchdog Timer is active, the following icon will be displayed on the system:



13.2.3 Introduction

Watchdog Timer (WDT) Signal Handling

To enable the Watchdog Timer (WDT), use the following function:

```
F75111_SetWDTEnable(BYTE byteTimer);
// If no disable signal (F75111_SetWDTDisable()) is received before the timer countdown reaches 0,␣
↪the system reboots.
```

Initial Port Address Configuration

The initial internal port address for the F75111 device is `0x9C`.
Use this address to define GPIO pins for input/output operations and to enable the WDT function pin.

Setting Digital Output Value: Sample Code

```
void F75111::InterDigitalOutput(BYTE byteValue) {
    BYTE byteData = 0;
    byteData = (byteData & 0x01) ? byteValue + 0x01 : byteValue;
    // Additional bitmask adjustments can be applied here.
    this->Write_Byte(F75111_INTERNAL_ADDR, GPIO2X_OUTPUT_DATA, byteData);
}
```

Getting Digital Input Value: Sample Code

```
BYTE F75111::InterDigitalInput() {
    BYTE byteGPIO1X = 0, byteGPIO3X = 0, byteData = 0;
    this->Read_Byte(F75111_INTERNAL_ADDR, GPIO1X_INPUT_DATA, &byteGPIO1X);
    this->Read_Byte(F75111_INTERNAL_ADDR, GPIO3X_INPUT_DATA, &byteGPIO3X);
    // Adjustments to GPIO values can be made here before returning byteData.
    return byteData;
}
```

Enabling/Disabling WDT: Sample Code

- **Enable WDT**

```
void F75111_SetWDTEnable(BYTE byteTimer) {
    WriteByte(F75111_INTERNAL_ADDR, WDT_TIMER_RANGE, byteTimer);
    WriteByte(F75111_INTERNAL_ADDR, WDT_CONFIGURATION, WDT_TIMEOUT_FLAG | WDT_ENABLE | WDT_PULSE |␣
↪WDT_PSWIDTH_100MS);
}
```

- **Disable WDT**

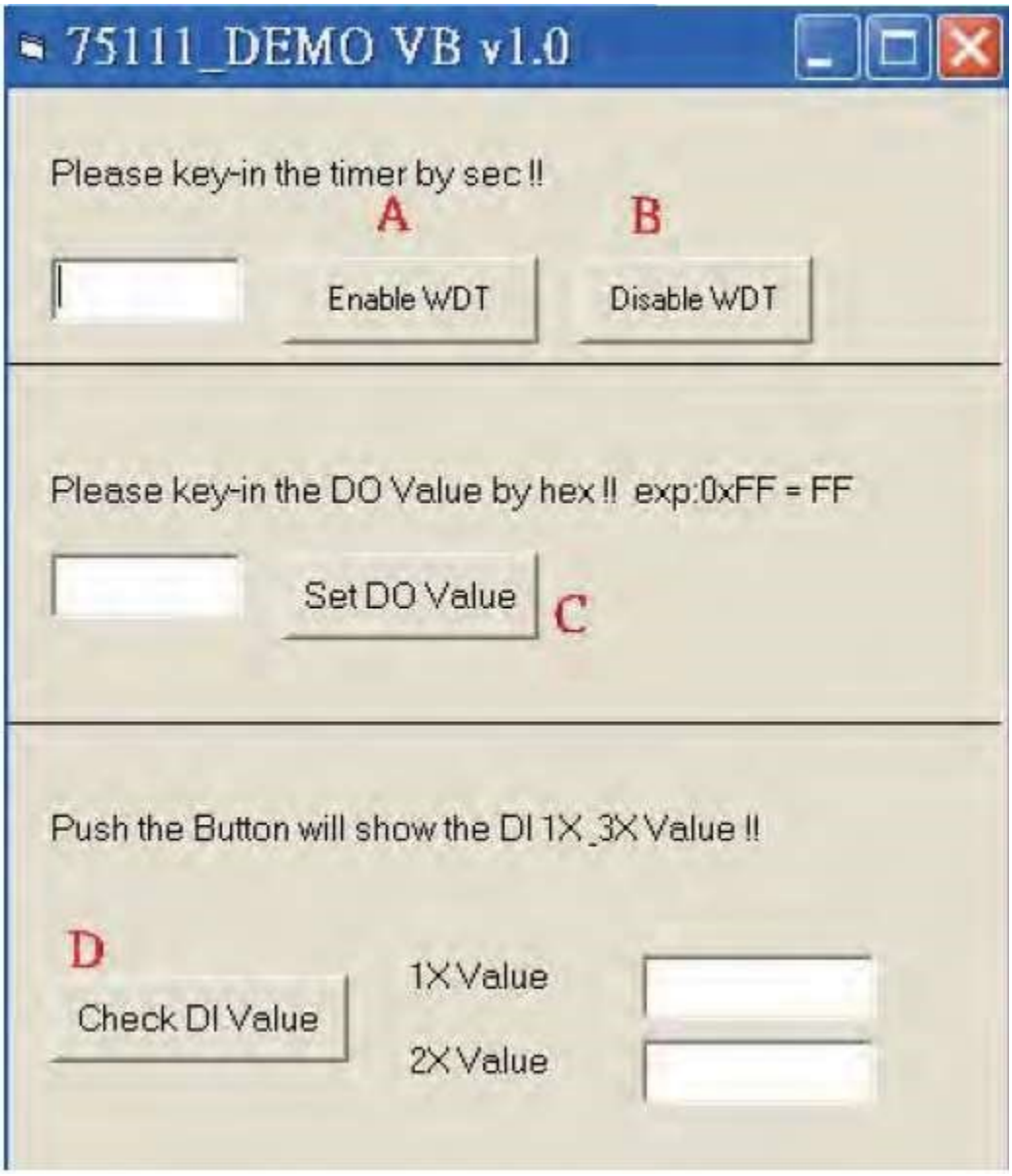
```
void F75111_SetWDTDisable() {
    WriteByte(F75111_INTERNAL_ADDR, WDT_CONFIGURATION, 0x00);
}
```

13.3 IO Device: F75111 in VB6 on Windows

You can access the necessary source and binary files here.

- **Source File:** `75111_VB_v10.rar`
- **Binary File:** `75111_VB_Src.rar`

13.3.1 Using the Demo Application



1. **Enable the WDT Timer:** Enter the countdown value (in seconds) in the left text box, then press **Enable**.
2. **Disable the WDT Timer:** Press the corresponding **Disable** button to stop the timer.
3. **Set Digital Output (DO) Value:** Input the desired hexadecimal value and press the corresponding button.
4. **Check Digital Input (DI) Value:** Press the button to display DI 1X & 2X values in the right text boxes.

13.4 Watchdog Timer and DIO in Linux

You can access the necessary source and binary files here.

- **Source File:** `F75111v2.0L.tar.gz`
- **Binary File:** `F75111v2.0LBin.tar.gz`

13.4.1 Compiling the Source Code

1. **Using Code::Blocks:**
   - Install Code::Blocks using `apt-get install codeblocks`.
   - Open the existing project file (`F75111.cbp`) and compile it.
   - Add the following linker option:
     `pkg-config --libs gtk+-2.0 gthread-2.0`
     Navigate to **Project -> Build Option -> Linker Settings -> Other Linker Options** to set this.
2. **Using Make:**

```
cd F75111
make
./src/f75111  # Run the compiled binary
```

13.4.2 Using the Demo Application

1. **Start DIO Testing:** Press **Start** to begin testing the DIO function.
2. **Enable the WDT:** Press **Enable** to activate the Watchdog Timer.
3. **Disable the WDT:** Press **Disable** to deactivate the Watchdog Timer.
4. **Perform a WDT Loop Test:** Check the **Enable Loop** box and press **Enable** to initiate loop testing.
5. **Configure Autorun:**

- Use **Install** to set up the application to run automatically at system startup.
- Use **Uninstall** to remove the autorun configuration.

When active, the system icon will blink: