

RPAC-2858M Website User Manual

English

Ver. 1.0, May. 2026



WARRANTY

All products manufactured by ICP DAS are warranted against defective materials for a period of one year from the date of delivery to the original purchaser.

WARNING

ICP DAS assumes no liability for damages consequent to the use of this product. ICP DAS reserves the right to change this manual at any time without notice. The information furnished by ICP DAS is believed to be accurate and reliable. However, no responsibility is assumed by ICP DAS for its use, nor for any infringements of patents or other rights of third parties resulting from its use.

COPYRIGHT

Copyright © 2026 by ICP DAS. All rights are reserved.

TRADEMARK

Names are used for identification only and may be registered trademarks of their respective companies.

CONTACT US

If you have any questions, please feel free to contact us via email at:

service@icpdas.com, service.icpdas@gmail.com



Revision History

Revision	Date	Description	Note
1.0	2026/05	Initial issue	

Table of Contents

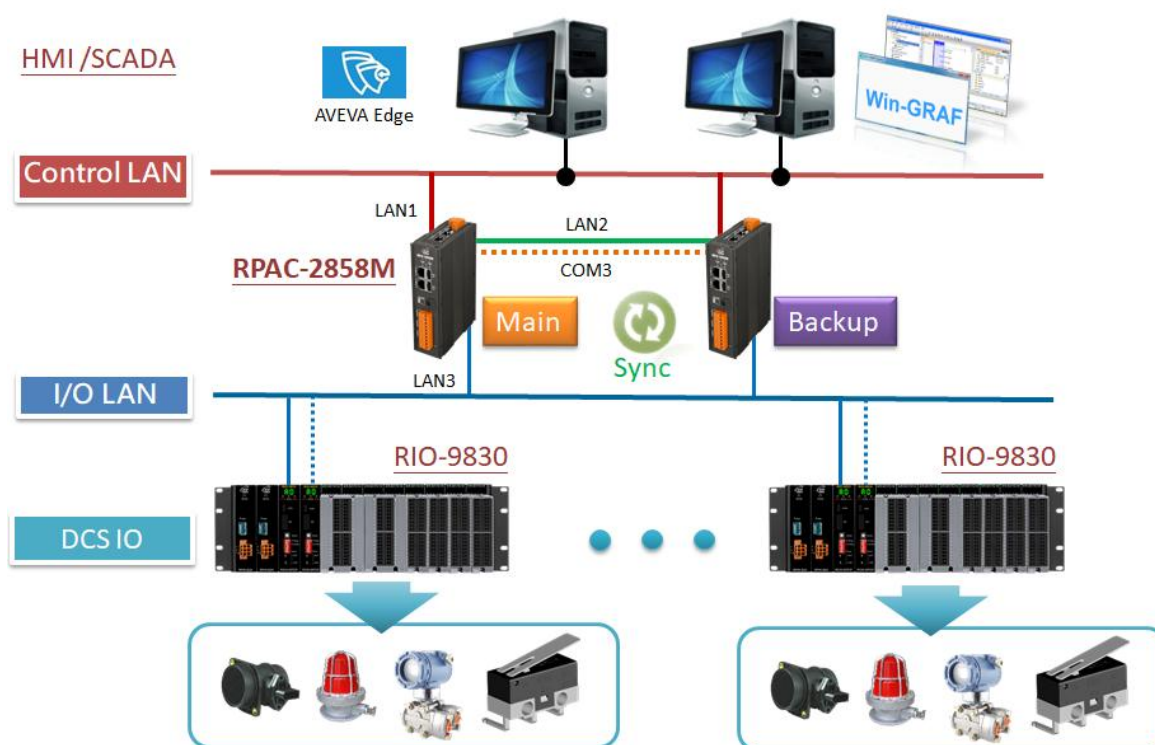
1.	Introduction	4
2.	Getting Started	5
2.1.	Login into the webpage	5
2.2.	Web Interface Introduction	8
3.	System General.....	14
3.1.	Date & Time	14
3.2.	Network	15
3.3.	Maintenance	17
4.	System Security	19
4.1.	White list.....	19
4.2.	Integrity Check	19
4.3.	Log	20
5.	System Log.....	22
5.1.	Log	22
6.	PLC	25
6.1.	Task.....	25
6.2.	Redundant.....	27
7.	OPC UA	29
7.1.	Server Certificate.....	29
8.	Account Settings	35
	Appendix A. eSearch Tool Software	37
	Appendix B. Hardware Interface	38

1. Introduction

RPAC-2858M is the new generation of Win-GRAF programmable automation controller (PAC) from ICP DAS. It adopts Cortex-A53 quad-core processor (1.6 GHz) to run Xenomai real-time kernel operating system to provide high performance and real-time control. Built-in industrial communication protocols, including OPC UA, and Modbus TCP/RTU, the RPAC-2858M uses a dual-controller redundancy architecture to ensure system safety and stability. Depending on system requirements, the RPAC-2858M can be equipped with ICP DAS redundant I/O and redundant power supply products to achieve an uninterruptible system architecture.

Win-GRAF programmable automation controllers running the Linux operating system offer the advantages of real-time functionality, high-performance precision control, and a PC-like operating environment for the PAC. In addition to supporting Win-GRAF (IEC61131-3 standard) software for developing control programs, the PAC also supports C or C++ for developing data management applications, and can exchange data with Win-GRAF applications to make application design more convenient and practical.

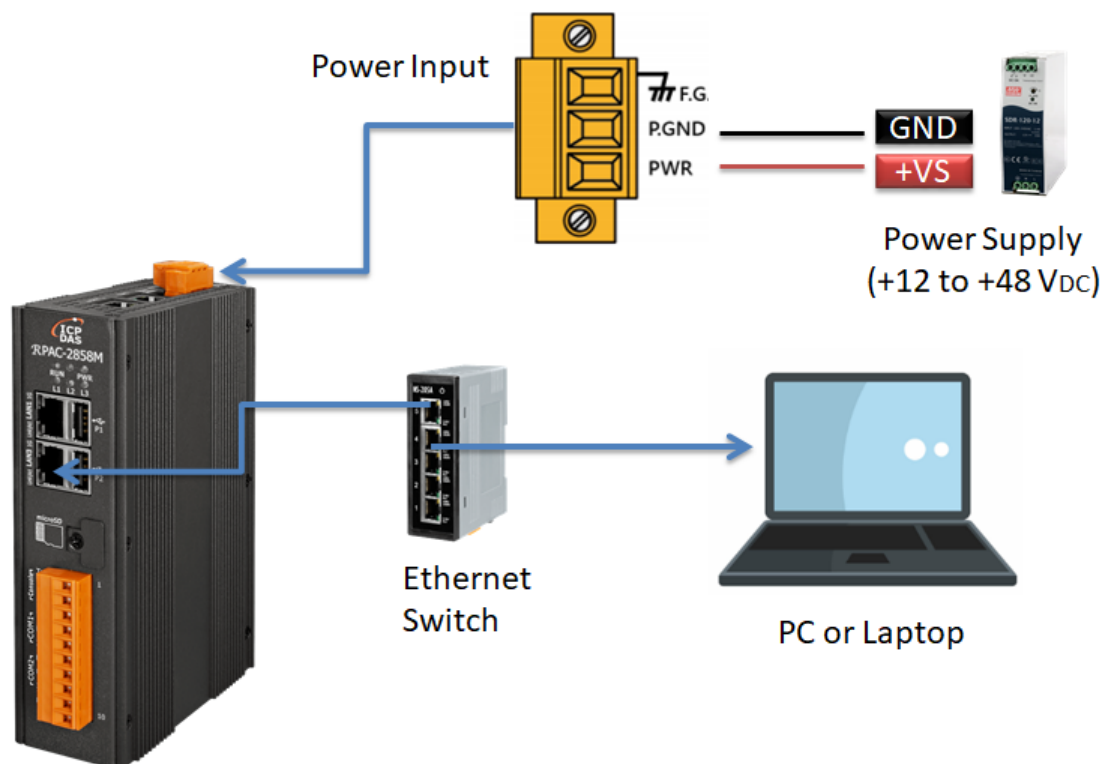
The RPAC-2858M is integrated with a web server, which allows users to connect to the web server via Ethernet network using a web browser to configure the controller functions such as network, system time, Win-GRAF runtime, OPC UA certificate management, etc. The RPAC-2858M is used for the following purposes in this manual. Each function is described in detail on each page of this manual.



2. Getting Started

2.1. Login into the webpage

Connect the device to the power supply and network cable, and connect the computer's network to LAN3 on the device, as shown in the figure below.



Before accessing the webpage, please configure your PC's network settings. The device's factory default network settings are as follows:

Factory Default		
Network Setting	IP (LAN3)	192.168.255.1
	Net mask	255.255.255.0

1. Change the PC's network settings to the same network segment as the device, for example:

Network Setting	IP	192.168.255.10
	Net mask	255.255.255.0

2. Make sure the device and PC are properly connected to the network. Start the browser and type "http://192.168.255.1" in the address bar to enter the login page.

3. Enter the account and password on the login page, and click the "Login" button to log in.
 - Default account: admin
 - Default password: admin



 Username

 Password

Login

4. When using the default account and password to log in for the first time, the system will require the user to change the password. Please log in again after changing the password.



You must change your password before logging on the first time.

Username

admin

Old password

New password

Confirm new password

Change

5. After logging into the webpage, change the hardware network settings according to the actual network environment. For detailed network setting, please refer to the section Network.
6. Users can also modify the network settings through the eSearch Utility software. For details, please refer to Appendix A. eSearch Tool Software.

2.2. Web Interface Introduction

As shown in Figure 2-1, the web interface consists of the following parts:

1. Toolbar
2. Navigation area
3. Workspace
4. Error/Message Notification Box

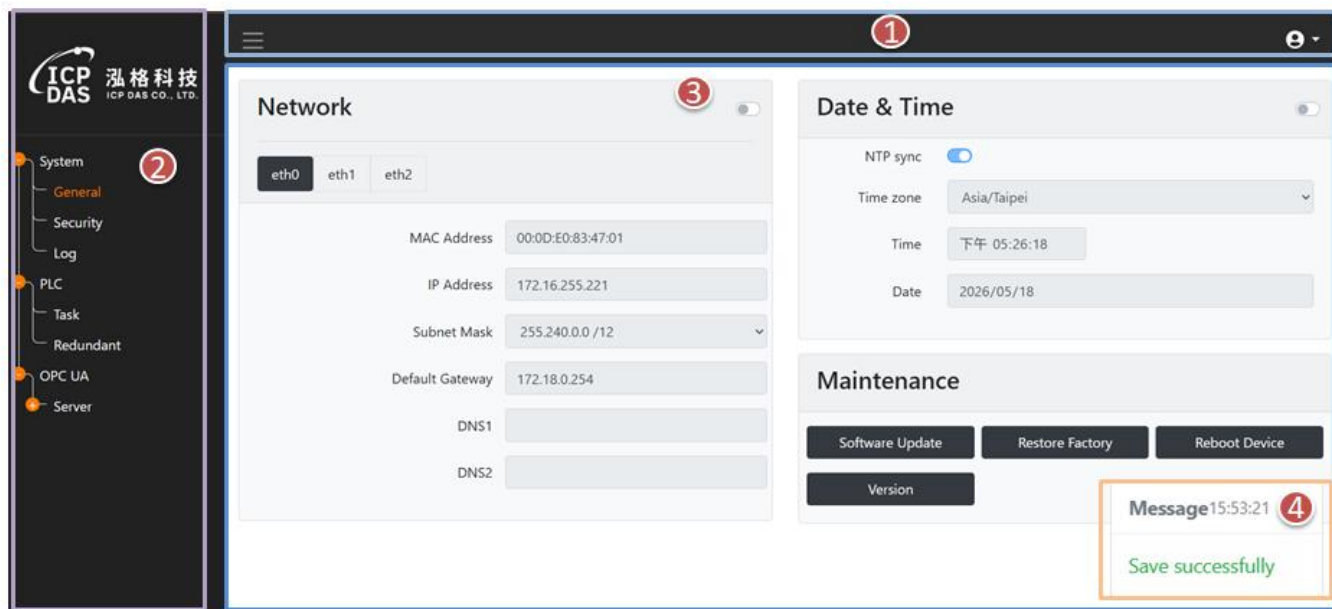


Figure 2-1

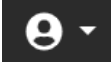
2.2.1. Toolbar

The toolbar (shown as Figure 2-2) is always displayed at the top of the web interface.



Figure 2-2

The toolbar has the following controls:

-  - Account drop down menu.
 -  admin - Login account name.
 -  Password - To change the password, please refer to the section: Account Settings for detailed information.
 -  Logout - Log out of account.

2.2.2. Navigation Area

The Navigation Area is shown in Figure 2-3, which is located on the left side of the web interface. You can use the toolbar "Show/Hide Navigation Area Button" to display and hide it. The default is the display state. The main purpose of the Navigation Area is to switch the workspace to different work pages.

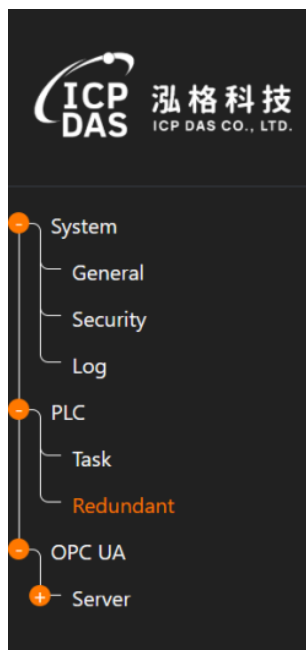


Figure 2-3

The following are the accessible work pages:

- System->General
This page allows you to configure system parameters such as network settings, date and time, software updates, software version information, etc. Please refer to the System General section for further information.
- System->Security
This page contains system-related security settings and log information. Please refer to the System Security section for details.
- System->Log
This page displays various log information. Please refer to the System Log section for details.
- PLC->Task
This page can perform operations of task (start, stop). Please refer to section PLC Task for detailed information.
- PLC->Redundant

This page shows the LAN1 、LAN3 network settings for PLC Redundant. Please refer to section PLC Redundant for detailed information.

- OPC UA
This page manages the server's certificate files to ensure secure communication. See the OPC UA section for more information.

2.2.3. Workspace

The workspace is located at the right side of the web interface; it will display the work page the user selected from the Navigation area. The content of the work page is composed of multiple card content container as shown in Figure 2-4, each card represents a function, and these functions can be status, parameter setting or operations of functions.

The screenshot displays the workspace of the RPAC-2858M web interface, organized into three main sections:

- Network:** Features a toggle switch and two tabs labeled 'eth0' and 'eth1'. Below the tabs are input fields for MAC Address (00:0D:E0:00:00:D1), IP Address (172.16.255.235), Subnet Mask (255.240.0.0 /12), Default Gateway, DNS1, and DNS2.
- Date & Time:** Includes a toggle switch, an 'NTP sync' toggle (checked), a 'Time zone' dropdown menu (set to Asia/Taipei), and input fields for 'Time' (下午 02:31:29) and 'Date' (2025/04/14).
- Maintenance:** Contains four buttons: 'Software Update', 'Restore Factory', 'Reboot Device', and 'Version'.

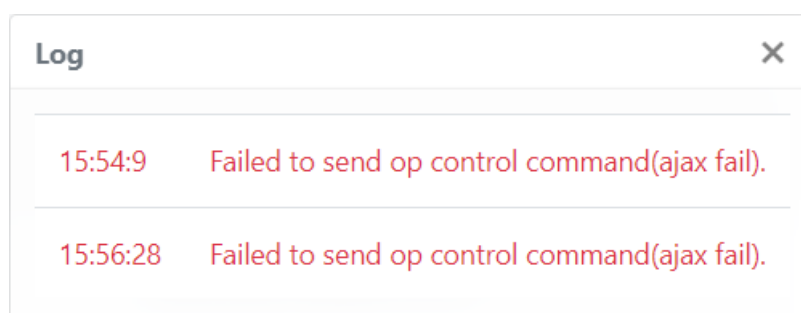
Figure 2-4

2.2.4. Error/Message Notification Box

The error/message notification box usually will not appear on the web interface, it only pops up when there is an error or message requires to be notified to the user. Notification boxes include the following types:

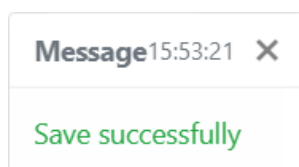
- Error notification box

When an error occurs during the operation of web interface, this notification box will pop up and inform the user of the detailed error message. The notification box will appear on the web interface, and the last error message will be added to the list and will not be cleared until the user closes the notification box.



- Message notification box

The message notification box will notify the user whether the operations on the web interface is successful or not and will prompt additional information if required. After the notification box pops up, it will appear for 3 seconds, and will automatically close after 3 seconds.



3. System General

The system general page is for parameter settings such as host name, network setting, date & time, software update, etc. The following are the functions.

3.1. Date & Time

The date and time settings of the controller are shown in Figure 3-1. The parameters and function buttons are as follows:

Figure 3-1

-  The switch on the right side of the title is used to enable or disable the date and time setting function. When it is disabled, it will only display the current date and time. If it is enabled, a  write button will appear.
- NTP sync
Enable or disable NTP synchronization. The NTP network time protocol will synchronize the system time of the controller to the system time on the network.
- Time zone
Time zone.
- Time
Time. Can only be set when NTP sync is disabled.
- Date
Date. Can only be set when NTP sync is disabled.
-  Write new Settings to the controller, which only appears if the settings function is enabled.

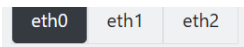
3.2. Network

The network settings of the controller are shown in Figure 3-2, and the descriptions of the parameters and function buttons are as follows:

The screenshot shows a 'Network' configuration window with a toggle switch in the top right corner. Below the title, there are three tabs: 'eth0' (selected), 'eth1', and 'eth2'. The configuration fields are as follows:

Parameter	Value
MAC Address	00:0D:E0:83:47:01
IP Address	172.16.255.223
Subnet Mask	255.240.0.0 /12
Default Gateway	172.18.0.254
DNS1	8.8.8.8
DNS2	168.95.1.1

Figure 3-2

-  The switch is used to enable or disable the network settings. When it is disabled, it will only display the current network interface and network configuration. If it is enabled, a  write button will appear.
-  Click the eth switch button; clicking it will display the settings information below.
- MAC Address
MAC address.
- IP Address
IP Address.
- Subnet Mask
Subnet mask.

- Default Gateway
Default gateway.
- DNS1
DNS server 1.
- DNS2
DNS server 2.
- Connection Type
Connection Type will only appear when the setting is enabled.

Static IP: Static IP address.

DHCP: Request an IP address by using DHCP.
-  Write new Settings to the controller, which only appears if the settings function is enabled.

3.3. Maintenance

The maintenance function of the controller is shown in Figure 3-3, which can be used to update the software, display the software version, etc. The function buttons are as follows:

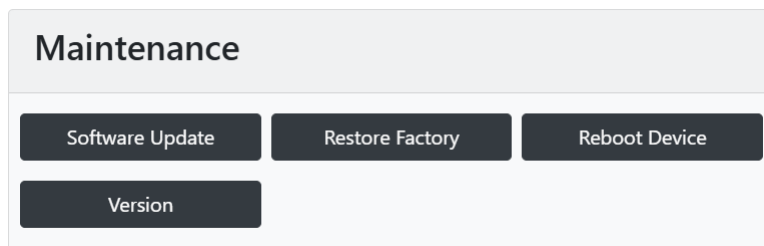
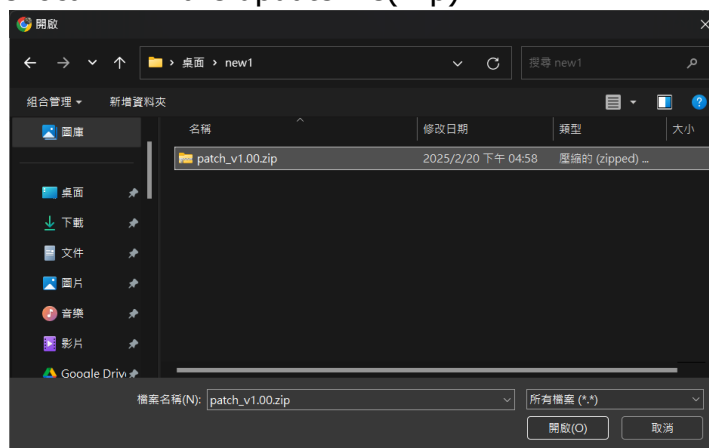


Figure 3-3

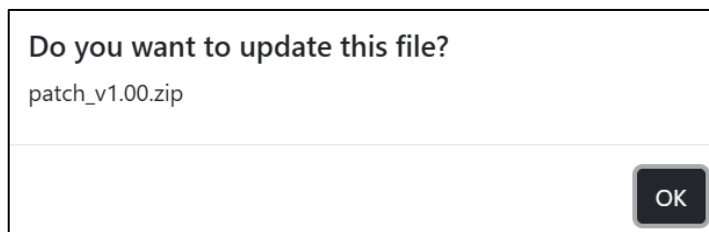
- Software Update

The software update button is used to update the relevant software inside the system. The update steps are as follows:

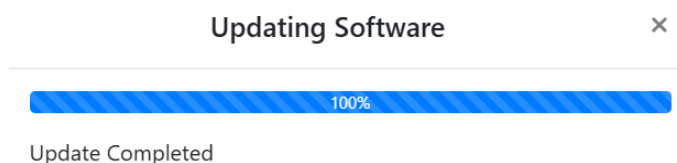
1. After clicking the "Software Update" button, the open file dialog box will appear, select the local firmware update file(.zip).



2. Then a file confirmation dialog box will appear. Click "OK" button to confirm the update.



3. Start the software update process, wait until the progress bar reaches 100% without any error, it means the software update is successful.



- **Restore Factory**
When pressed, requires the controller to be rebooted for the settings to take effect.
- **Reboot Device**
Reboot controller.
- **Version**
Show software version information. The following version information dialog box will appear after clicking this button.

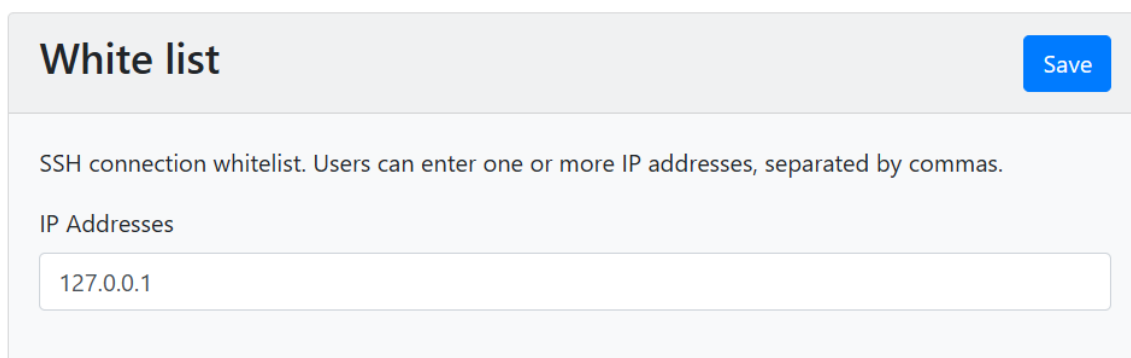
Version			
Name	Version	Architecture	Description
OS Version	OS Version 4.14.78 #30 SMP PREEMPT Mon Apr 14 13:04:22 CST 2025 release		
Application Version	1.00 B1		License: OK
WinGRAF Version	WG14.0 v1.00 B01 20250410		Project: emp_t1, Extra_port: null, Elapsed time : 0. 2:20:35

4. System Security

This workspace can be used to set up a controller connection whitelist and view controller security-related logs. The following will explain each function.

4.1. White list

The whitelist setting function is shown in Figure 4-1. This whitelist setting is mainly designed for SSH network connections. If a user wants to connect to the controller via SSH, they must add their local IP address to this whitelist before the connection can be allowed. Multiple IP addresses can be set in the whitelist at the same time, separated by commas.



White list Save

SSH connection whitelist. Users can enter one or more IP addresses, separated by commas.

IP Addresses

127.0.0.1

Figure 4-1

4.2. Integrity Check

The controller proactively records the permissions and content of internal files, documents, and programs in a related database. If unauthorized intrusion is suspected, resulting in content alteration, this function can be used for comparison to clarify whether the content has been modified. This information is primarily for user reference; modifications may also include changes made during routine operations.

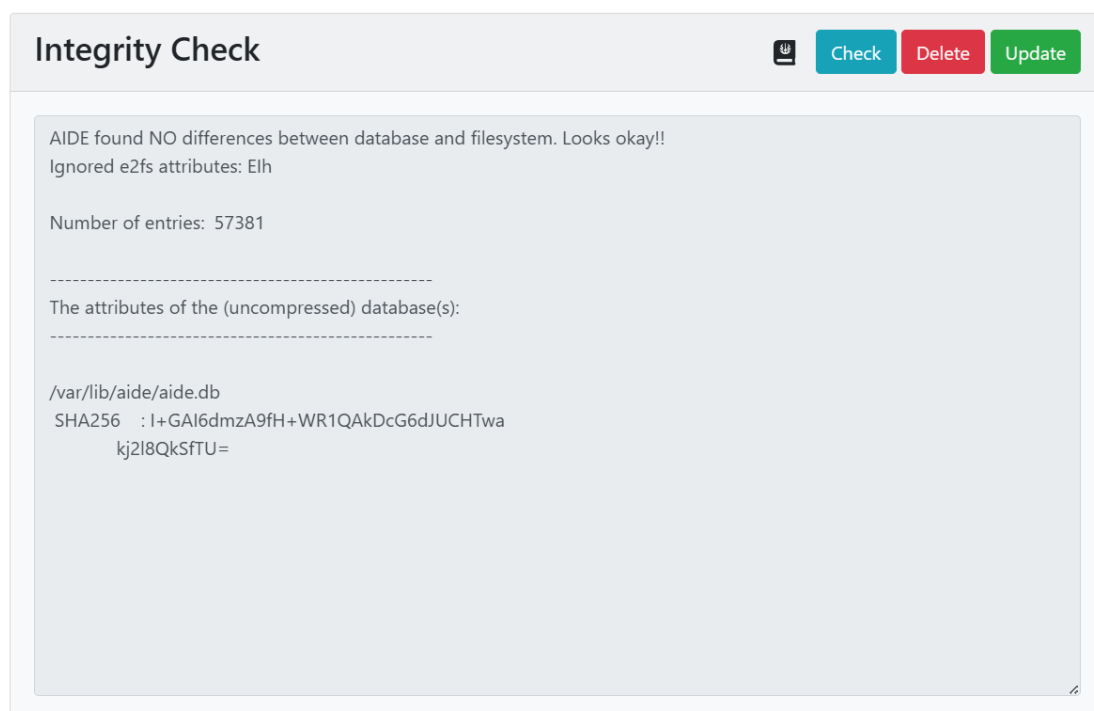


Figure 4-2

-  The "Update Content" button allows you to update the integrity check information.
-  Check
Check button: Click this button to perform an integrity check.
-  Delete
Delete button: Click this button to delete all changes.
-  Update
The "Update Database" button allows you to update the complete database and set the current system status as the benchmark for the next comparison.

4.3. Log

The logging function, as shown in Figure 4-3, records the controller's internal systems, web login records, and network alerts. This logging function allows users to understand whether there are unauthorized login attempts or suspicious network traffic.



Figure 4-3

The log types to be displayed are as follows:

- Login History
System login records.
- Failed Login History
Failed system login record.
- Web Login History
Webpage login history content.
- IDS Alert
Suspicious network traffic logs.



Click the button to retrieve the log content of the selected log type. When you click this button, the relevant records will be displayed according to the selected item.

5. System Log

This working page can be used to view the status of the controller service program and view the related logs of the controller. The functions are as follow.

5.1. Log

The controller log function is shown in Figure 4-1, which records the errors, warnings and other prompt messages generated by the internal program of the controller. These messages allow developers to understand the operation status of the program and the cause of the error.

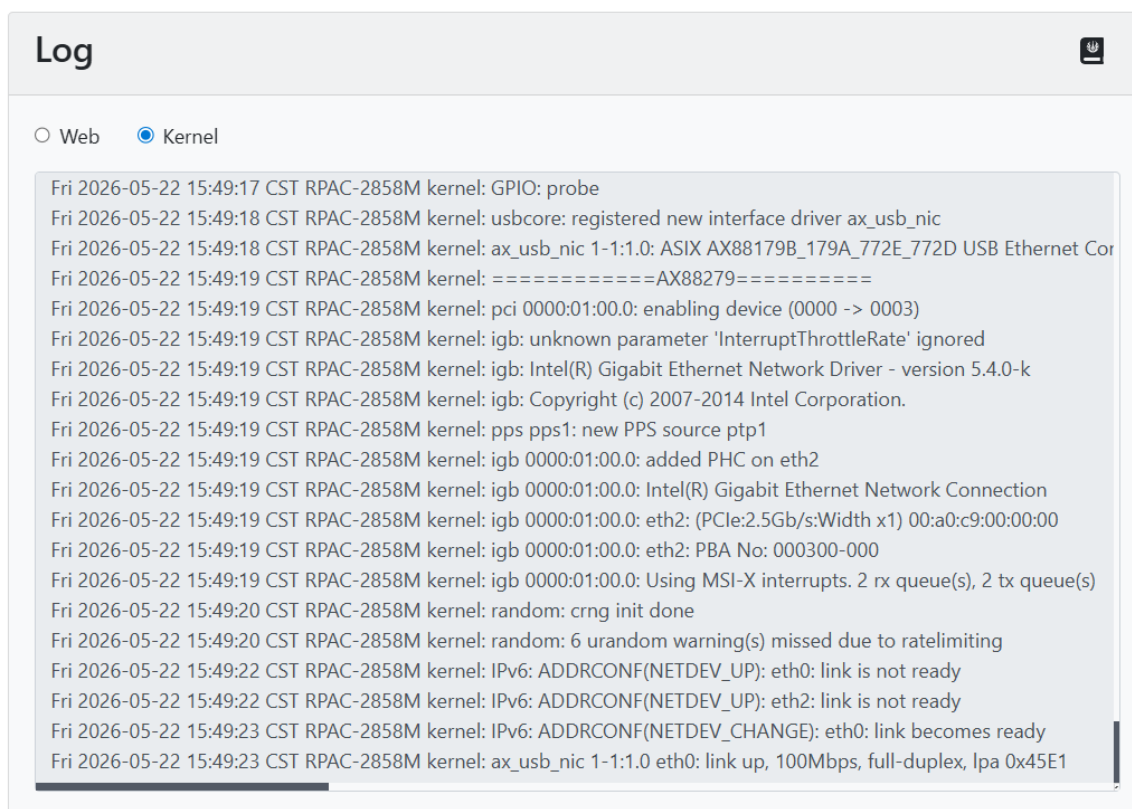


Figure 5-1

The types of logs to be displayed are as follows:

- Web
Logs of web interface.
- Kernel
Logs of kernel.



The button is used to access the content of the selected log. After clicking the button, the following Log Filter dialog box will appear, and the records within the range of the log time will be filtered according to the filter items.

Log Filter (Max. 200)

☒ Today ☐ Yesterday ☐ All

☐ Since

Until

☐ lines 25 ☐ First ☒ Last

OK

Filter items are as below:

- Today
Filter logs within today.
- Yesterday
Filter logs within yesterday.
- All
All logs.
- Since - Until
Filter logs within the specified time range.

The display restriction items are as follows:

- lines
Limit the number of lines displayed in the log. By default, no matter what filter item is selected, the maximum number of displayed lines is 200 lines. The parameter can be set to limit the number of lines to less than 200 lines.

- First
Based on the filter range, the logs that are order in time will be displayed.
- Last
Based on the filter range, the logs that are later in time will be displayed.

6. PLC

This page is mainly used to set up and control the PLC runtime, and each function is described below.

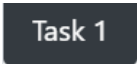
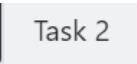
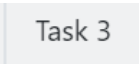
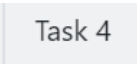
6.1. Task

As shown in Figure 6-1, this part allows users to obtain the information of each PLC task and perform PLC task control without using Win-GRAF Workbench.

The screenshot displays the 'Task Control' window. At the top, there are four tabs: 'Task 1' (selected), 'Task 2', 'Task 3', and 'Task 4'. To the right of the tabs are several control icons: a toggle switch, a PLC symbol, a play button, a pause button, a fast-forward button, and a delete button. Below the tabs, the window is titled 'Application - RUN'. It contains two main sections. The first section, 'Application Information', has four input fields: 'Name' (gg), 'Version' (V41), 'CRC' (0x8c86d23c), and 'Date' (2022-05-25-14:29:04). The second section, 'Cycle Time', has four input fields: 'Period (μs)' (0), 'Last (μs)' (28), 'Max. (μs)' (242), and 'OverFlow' (0).

Figure 6-1

The function buttons are as follows:

-    

Switch to the task by clicking on specific task tab. The information of the task will be displayed below, and the user can perform control of the task by the function buttons on the right hand side.
- 

Automatically update information of task cycle time.
- 

Start or stop the task.
- 

Pause cycle to cycle mode.
- 

Resume cycle to cycle mode. Can only be used when the cycle to cycle mode is paused.

-  Execute a single cycle. Can only be used when the cycle to cycle mode is paused.
-  Delete the code file of the task.

The task information is as follows:

- Application - "xxx"
"xxx" is the running status of the task, the status are as follows:

IDLE: Stop task execution.

RUN: The task is being executed.

STOP: The task is paused.
 - Name
Task or project name
 - Version
Program version
 - CRC
CRC check code of the program
 - Date
Program creation time
- Cycle Time
Task cycle time information.
 - Period (μ s)
The task period, in microseconds.
 - Last (μ s)
The task execution time, taking the latest cycle as the last cycle time, in microseconds.
 - Max. (μ s)
The maximum execution time of the task, in microseconds.
 - OverFlow
The count times when the task execution time exceeds the cycle time.

6.2. Redundant

This setting is primarily used to configure the IP, Mask, and Gateway settings for LAN1 and LAN3 when the controller is in redundancy mode.

As shown in Figure 6-2, "For upper layer networks" refers to the network settings for LAN1 in redundancy mode. When redundancy mode is enabled, the LAN1 network will be configured according to these settings.

Figure 6-2

As shown in Figure 6-3, "For lower layer networks" refers to the network settings of LAN3 in redundancy mode. When redundancy mode is enabled, the LAN3 network will be configured according to these settings.

Figure 6-3

- 

The switch is used to enable or disable the network settings. When it is disabled, it will only display the current network interface and network configuration. If it is enabled, a  write button will appear.
- IP Address

IP Address.

- Subnet Mask
Subnet mask.
- Default Gateway
Default gateway.
-  Write new Settings to the controller, which only appears if the settings function is enabled.

7. OPC UA

OPC UA (Open Platform Communications Unified Architecture) is an open standard communication protocol designed for facilitating data exchange and communication between different devices and systems. Its primary goal is to provide interoperability across platforms, networks, and vendors while ensuring high scalability and security.

7.1. Server Certificate

The contents of this page are used to manage the certificate files of the Win-GRAF Runtime OPC UA Server to ensure the security of communications. The following is a detailed description of the contents of each tab:

- Own

This tab displays existing server certificates and allows the creation of new self-signed certificates. Detailed information about server certificates can be accessed through the General/Subject/SAN tabs. The following details are explained:

- General: General information.

General Subject SAN		+	↓	↑	🗑️
Issuer	Thumbprint				
UaServer:EMP-OPCUA	7832CFF1D5512CE8815C1A440524F55522F0DA13				
Valid From	Valid To				
Mon Jan 08 2024 13:06:25 GMT+0800 (台北標準時間)	Tue Jan 07 2025 13:06:25 GMT+0800 (台北標準時間)				

- Issuer: Issuer name.
- Thumbprint: This is commonly called a “fingerprint”.
- Valid From: Start date of certificate.
- Valid To: Expiry date of a certificate.

- **Subject:** Subject field.

The screenshot shows the 'Subject' tab of a configuration window. At the top, there are three tabs: 'General' (blue), 'Subject' (black with white text), and 'SAN' (blue). To the right of the tabs are four icons: a plus sign, a download arrow, an upload arrow, and a trash can. The main area contains six input fields arranged in three rows. The first row has 'Common Name' (containing 'UaServer:EMP-OPCUA') and 'Organization' (containing 'Organization'). The second row has 'Organization Unit' (containing 'Unit') and 'Locality' (empty). The third row has 'State' (empty) and 'Country' (empty).

- **SAN:** Subject Alternative Name.

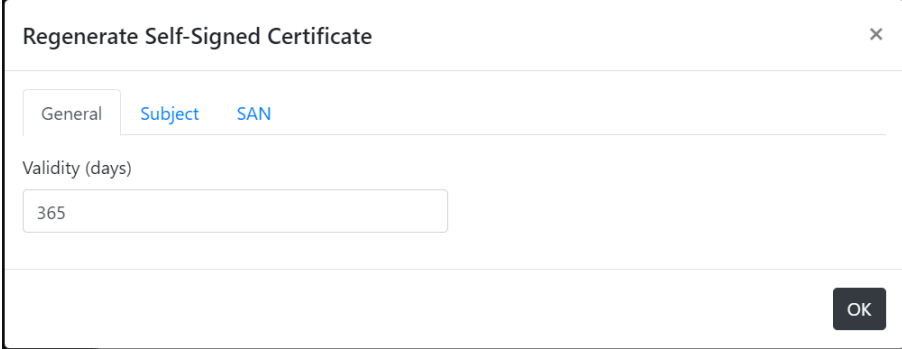
The screenshot shows the 'SAN' tab of a configuration window. At the top, there are three tabs: 'General' (blue), 'Subject' (blue), and 'SAN' (black with white text). To the right of the tabs are four icons: a plus sign, a download arrow, an upload arrow, and a trash can. The main area contains three input fields. The first is 'URI' (containing 'urn:Company:Product:UA_Serverurn:Company:Product:UA_Server2'). The second is 'DNS' (containing 'EMP-OPCUA,EMP-OPCUA2'). The third is 'IP' (containing '192.168.2.82,192.168.2.83').

- **URI:** Uniform Resource Identifier.
- **DNS:** Domain Name System. Use commas to separate multiple entries.
- **IP:** IP Address. Use commas to separate multiple entries.

Buttons on the right:



Create Self-Signed Certificate. After clicking the button, the following dialog box will appear, and each parameter is described as follows:



The dialog box titled "Regenerate Self-Signed Certificate" has a close button (X) in the top right corner. It contains three tabs: "General", "Subject", and "SAN". The "General" tab is selected. Below the tabs, there is a label "Validity (days)" and a text input field containing the value "365". An "OK" button is located in the bottom right corner.

- General: General Settings.
 - Validity (days): Certificate validity period, unit days.
- Subject: Please refer to the Subject SubjectSubjectdescription in the Own server certificate information.
- SAN: Please refer to the SAN SubjectSubjectdescription in the Own server certificate information.



Download the server certificate.



Upload the server certificate. After clicking the button, the following dialog box appears, select public key or private key to upload server certificate.



The dialog box titled "Upload Own Certificates" has a close button (X) in the top right corner. It contains two sections: "Public key" and "Private key". Each section has a text input field with the placeholder "Choose file" and a "Browse" button. An "OK" button is located in the bottom right corner.



Delete the server certificate.

- Trusted

Used to manage server trust and rejected certificates. You can also trust or reject specific certificates.

Own	Trusted	Issuers
Certificates		
MyCA2 [4310F510486C708D57B01F8323939C5690CFA787].der		
UaExpert@DESKTOP-Q36M1JG [76EF881F3033B2C1DD33600913225EDCDDC8F8D5].der		
Rejected		
UaExpert@DESKTOP-FSVMGHH [785DD568D4A6C30EF14AB5365CAE80B83CD1CA64].der		
Certificate Revocation Lists		
MyCA2 [4310F510486C708D57B01F8323939C5690CFA787].crl		

- Certificates: List of trusted certificates.
- Rejected: List of rejected certificates.
- Certificate Revocation Lists: Certificate Revocation Lists of trusted certificates.

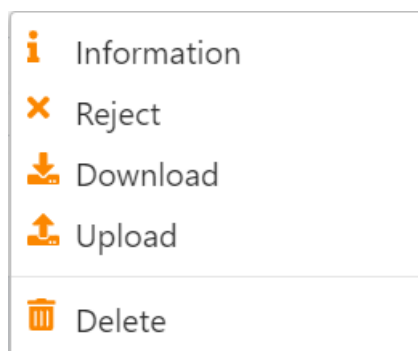
- Issuers

Manage issuer certificates. An issuer certificate is used to verify the legality and authenticity of other certificates. It establishes a trust chain to ensure that it comes from a trusted source.

Own	Trusted	Issuers
Certificates		
RootCA [D1FE74C48BABAFAF0DB26B2CB2CBD85C7ACC234D2C].der		
MyCA1 [DE551C4BA4C24FED4288B7754F34A4BCE2361A7A].der		
Certificate Revocation Lists		
MyCA1 [DE551C4BA4C24FED4288B7754F34A4BCE2361A7A].crl		

- Certificates: List of issuer certificates.
- Certificate Revocation Lists: Certificate Revocation Lists of issuer certificates.

The right-click menu of the Certificates/Rejected/Certificate Revocation Lists file list is as follows:



- Information: Display detailed information for certificates or certificate revocation lists. The instructions are as follows:

- Certificate Information

Please refer to the description of the Own server certificate information.

Certificate Information
×

General
Subject
SAN

Issuer	Thumbprint
MyCA1	4310F510486C708D57B01F8323939C5690CFA787
Valid From	Valid To
Wed Oct 04 2023 10:30:46 GMT+0800 (台北標準時)	Sat Sep 28 2024 10:30:46 GMT+0800 (台北標準時)

- Certificate Revocation Lists (CRL) Information

Certificate Information
×

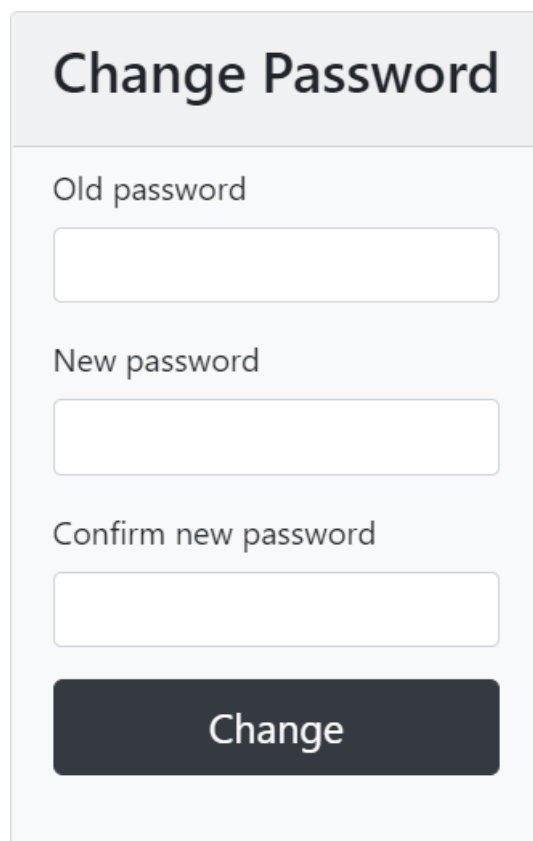
General
Subject
SAN

CRL Number	Issuer
03	ICPDAS Root CA
Last Update	Next Update
Fri Nov 10 2023 10:15:42 GMT+0800 (台北標準時)	Sun Dec 10 2023 10:15:42 GMT+0800 (台北標準時)
Thumbprint	
3C1685F48676E49AC0E57C964004759DC7F6E986	

- General: General information.
 - Subject: Please refer to the Subject description in the Own server certificate information.
 - SAN: Please refer to the SAN SubjectSubjectdescription in the Own server certificate information.
-
- Download: Download certificate or certificate revocation lists file.
 - Upload: Upload certificate or certificate revocation lists file.
 - Delete: Delete certificate or certificate revocation lists file.
 - Reject: Move the certificate to the rejected certificate list. (This option is available only in the trusted certificate list.)
 - Trust: Move the certificate to the trusted certificate list. (This option is available only in the rejected certificate list.)

8. Account Settings

This page can be used to modify the user account password on the web interface. After the user logs in the web interface for the first time (using the factory default account/password), please change the password as soon as possible. The password change is shown as Figure 10-1.

A web form titled "Change Password" with a light gray header. Below the header, there are three input fields: "Old password", "New password", and "Confirm new password". Each field is a simple white rectangle with a thin gray border. At the bottom of the form is a dark gray button with the word "Change" in white text.

Change Password

Old password

New password

Confirm new password

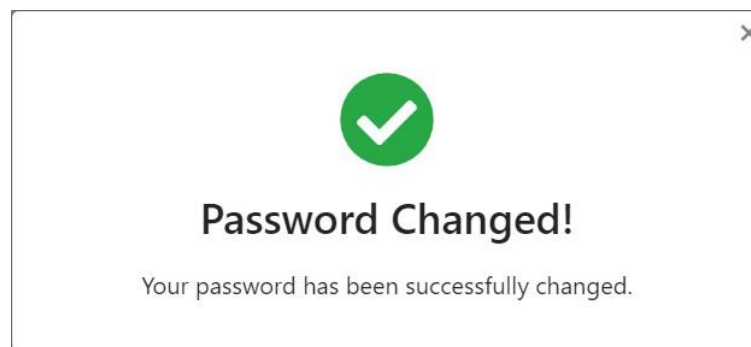
Change

Figure 11-1

The modification steps are as follows:

1. Enter the old password in the "Old password" input box.
2. Enter a new password in the "New password" input box.
3. Enter the new password again in the "Confirm new password" input box to confirm the password accuracy.
4. Click the "Change" button. After the password is successfully changed, the following dialog box will appear. When you log in to the web interface next time, please log in with the new password. The new password features the following verification restrictions:

- Which checks the similarity between the password and a set of attributes of the user.
- Which checks whether the password meets a minimum length, the default is 8 characters.
- Which checks whether the password occurs in a list of common passwords. By default, it compares to an included list of 20,000 common passwords.
- Which checks whether the password isn't entirely numeric.



5. If there is an error in changing the password, an error message will be displayed below each input box, as shown in the figure below.

Change Password

Old password

- Your old password was entered incorrectly. Please enter it again.

New password

Confirm new password

- The two password fields didn't match.

Change

Appendix A. eSearch Tool Software

eSearch Utility

(http://www.icpdas.com/en/product/guide+Software+Utility_Driver+eSearch__Utility) is a set of easy-to-use portable software, which can be used to search and configure ICP DAS network communication devices on the Ethernet network. For software usage, please follow the steps below:

[Steps]

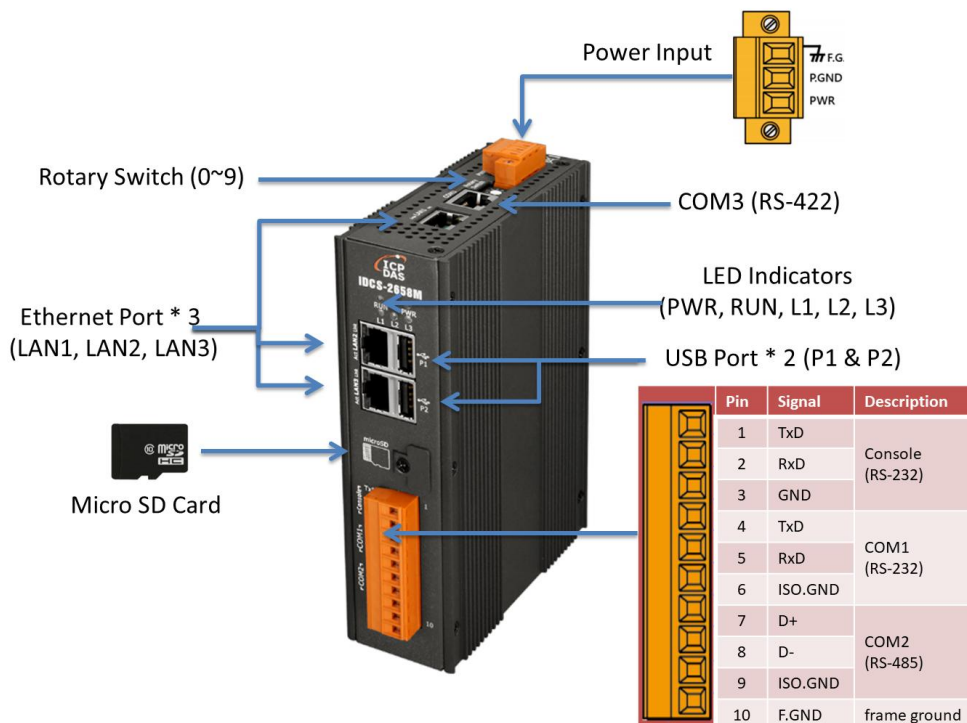
Search for RPAC-2858M devices on the Ethernet network.

- (1) Click the "Search Server" button to start searching for devices.
- (2) The RPAC-2858M device will appear in the search list and select RPAC-2858M.
- (3) Click the "Web" button to automatically open the default browser of the system.

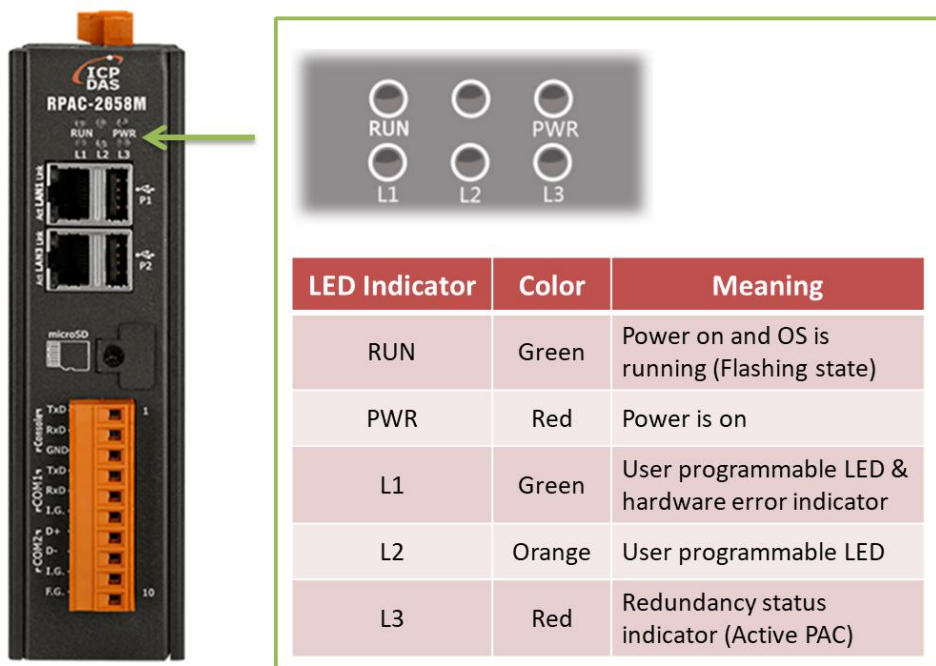


Appendix B. Hardware Interface

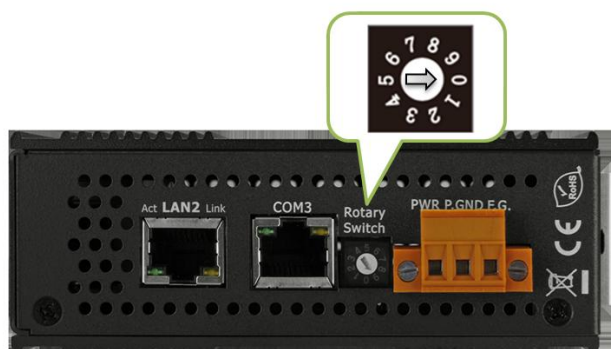
● Hardware Interface Diagram



● LED indicator lights

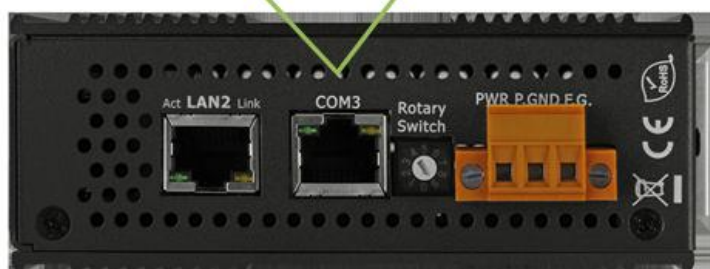
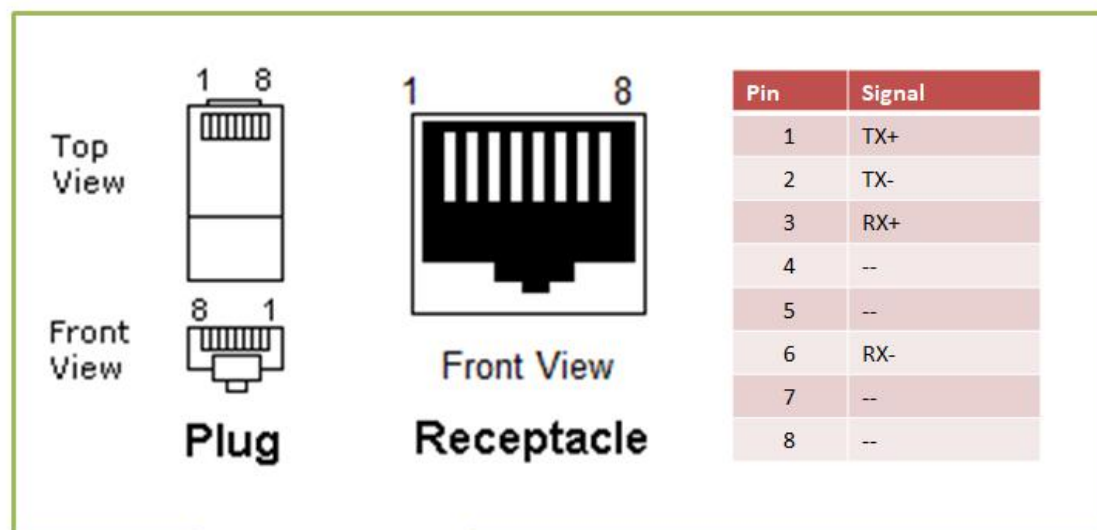


● Rotary switch definition



Rotary Switch Position	Description
0	Normal Mode
1	Don't start user application
2	LAN1: DHCP Mode
3	LAN1: Static IP Mode (IP: 192.168.255.1, Mask 255.255.0.0)
4	System runs in default mode
5	Firmware Update Mode
7	Redundancy Mode: Main PAC
9	Redundancy Mode: Backup PAC

● COM3 (RS-422) pin definitions



● Hardware Dimensions

