Honeywell | CIU 888

Security Manual

Release R210

PREFACE

General

The CIU 888 features multiple security related measures designed to safeguard the system, data and services against unauthorized access. The security measures are implemented in multiple areas of the system and network, thus providing a resilient and reliable defense.

Purpose of this manual

The purpose of this manual is to provide information about security measures implemented in the CIU 888.

Target audience of this manual

This manual is primarily intended for:

- Service technicians who are responsible for commissioning and configuring the CIU 888, diagnosing and troubleshooting problems and errors, and servicing and maintaining the CIU 888.
- System administrators who are responsible for managing the CIU 888 and site network.
- IT managers who are responsible for implementing and maintaining the network infrastructure of the company’s network, monitoring the organization's operational requirements, researching strategies and technology solutions, and building the most cost-effective and efficient system to achieve the aforementioned goals.

How to report a security vulnerability

For the purpose of submission, a security vulnerability is defined as a software defect or weakness that can be exploited to reduce the operational or security capabilities of the software. Honeywell investigates all reports of security vulnerabilities affecting Honeywell products and services.

To report a potential security vulnerability against any Honeywell product, please follow the instructions at:

https://honeywell.com/pages/vulnerabilityreporting.aspx

Submit the requested information to Honeywell using one of the following methods:

- Send an email to security@honeywell.com.

or

- Contact your local Honeywell Technical Assistance Center (TAC) or support center listed in the Contacts section of this document.

TABLE OF CONTENTS

This page is intentionally left blank

CHAPTER 1 INTRODUCTION

The CIU 888 is designed with a multi-layered approach for security. In this approach, multiple security measures (defenses) are available within the network along with ample measures to physically secure the CIU 888 box. Should one security measure not be able to avert a security breach, others continue to protect resources and data thereby preventing or limiting any potential damage.

The security measures implemented in the CIU 888 vary in nature, and fundamentally support the same goal: protecting confidentiality, integrity and availability of data throughout it’s entire lifespan, i.e., from the initial creation of the data on through to the final disposal of the data.

In case of critical failures, the CIU 888 shuts down automatically when instant recovery is not possible, restarts in case of fatal failures when recovery is possible. If some manual recovery actions are involved requiring some information from CIU 888, then CIU 888 stops the core applications/services to enable suitable corrective actions to be taken. The ring of light turns red to indicate such failures. The reason for failure can be tracked from the Audit and event logs.

NOTE: The CIU 888 is located at a site and as such subject to site related security measures. The site specific security measures are beyond the scope of this document.

FIGURE 1-1 indicates measures to secure the CIU 888.

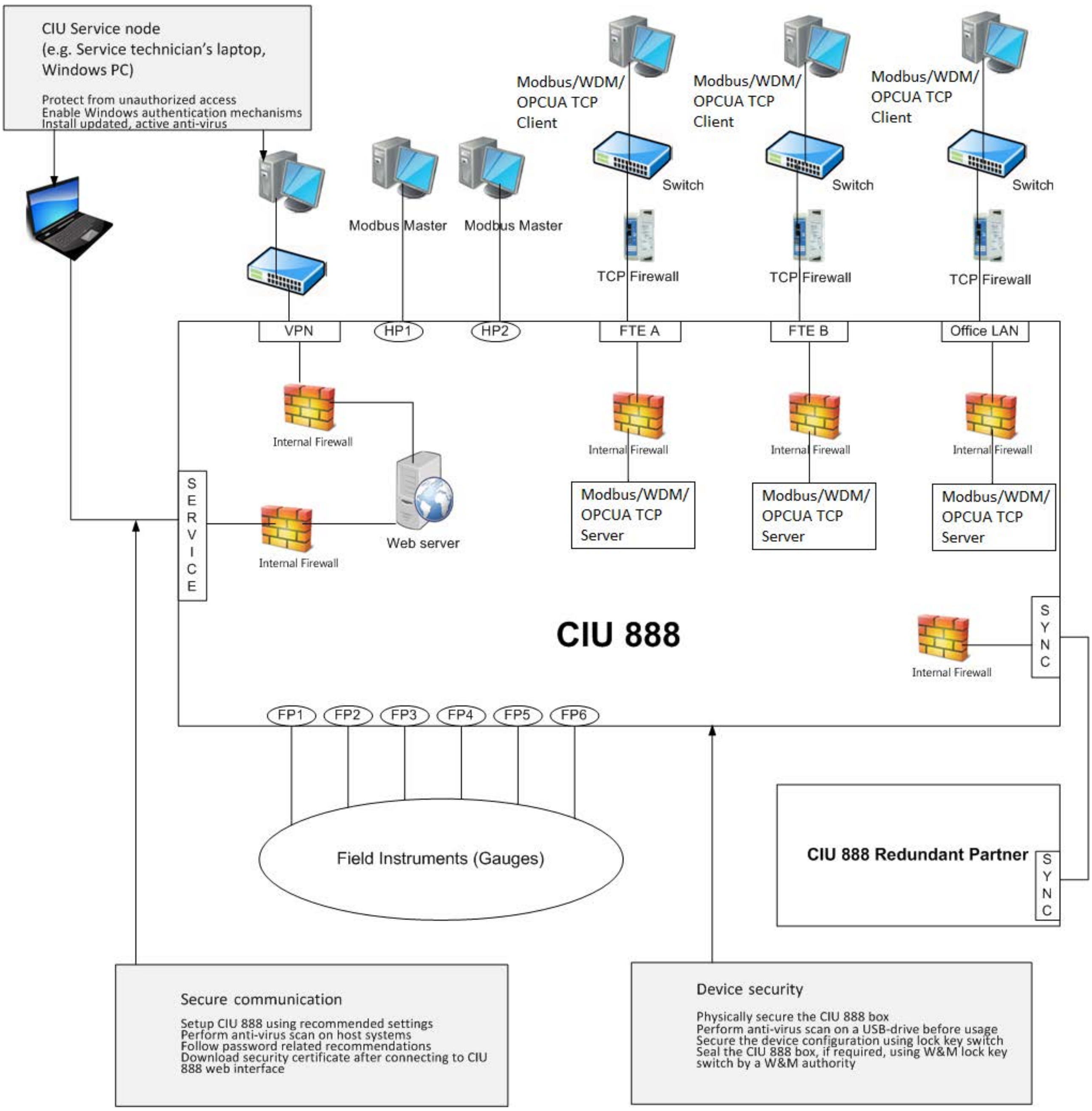

CIU Service node
(e.g. Service technician's laptop, Windows PC)
Protect from unauthorized access
Enable Windows authentication mechanisms
Install updated, active anti-virus
Modbus/WDM/ OPCUA TCP Client
Modbus/WDM/ OPCUA TCP Client
Modbus/WDM/ OPCUA TCP Client
Switch
Switch
Switch
Modbus Master
Modbus Master
TCP Firewall
TCP Firewall
TCP Firewall
VPN
HP1
HP2
FTE A
FTE B
Office LAN
Internal Firewall
Internal Firewall
Internal Firewall
Internal Firewall
Web server
SERVICE
Internal Firewall
Modbus/WDM/ OPCUA TCP Server
Modbus/WDM/ OPCUA TCP Server
Modbus/WDM/ OPCUA TCP Server
CIU 888
SYNC
Internal Firewall
FP1
FP2
FP3
FP4
FP5
FP6
Field Instruments (Gauges)
CIU 888 Redundant Partner
SYNC
Secure communication
Setup CIU 888 using recommended settings
Perform anti-virus scan on host systems
Follow password related recommendations
Download security certificate after connecting to CIU 888 web interface
Device security
Physically secure the CIU 888 box
Perform anti-virus scan on a USB-drive before usage
Secure the device configuration using lock key switch
Seal the CIU 888 box, if required, using W&M lock key switch by a W&M authority

FIGURE 1-1 Measures to Secure the CIU 888

1.1 Security Checklist

Presented here is a checklist of tasks you must complete to secure CIU 888 and its communications. Detailed procedures follow.

TABLE 1-1 Checklist of tasks to be performed to secure CIU 888

Sl. No.	Description
Securing the CIU 888 box	
1	Physically secure the CIU 888 box to prevent unauthorized access, see chapter 2 "Device Security".
2	Protect access to required USB ports. For example, use a physical lock on top of the USB drive, see section 2.1.
3	Perform anti-virus scan on a USB drive, see section 2.1.
4	Secure the CIU 888 configuration using the lock key switch, see section 2.2.
5	Seal the CIU 888 using W&M lock key switch authorized by a LM authority, see section 2.3. See the CIU 888 *Sealing Guide (Part No. 4417595)* for detailed instructions.
6	Regularly check the audit and event logs to view user activity pertaining to CIU 888 operations, see section 2.4.
Securing network nodes	
7	Ensure the CIU 888 is set up using the recommended settings, see section 3.1.
8	Ensure anti-virus scan is active and windows authentication is enabled on the host systems connected to CIU 888.
9	Protect site's communication network from unauthorized access.
10	Ensure the password related recommendations are followed, see section 3.2.3.
11	Download the security certificate to avoid getting the security related warnings after connecting to CIU 888 web interface, see section 3.2.2.
Securing the CIU service node	
12	Implement recommended protection measures on the CIU service node, including but not limited to: - Protect from unauthorized access - Enable windows authentication mechanisms - Ensure latest anti-virus installed and active.
13	Protect the data files, see section 4.2.
14	Perform anti-virus scan on the STRAP files before using them, see section 4.3.
15	Protect the files (for example database files, log files, STRAP files, etc.) in transit from the source to CIU 888, see section 4.4.

1.2 Multi-layered approach to security

The CIU 888 features a number of security measures to protect your data and prevent unauthorized access. These include:

- Device security
- Secure communications
- Securing CIU service node

CHAPTER 2 DEVICE SECURITY

Commonly, site policies will provide the first layer of defense against unauthorized access.

Recommendations are related to prevention of unsafe use of USB-sticks and unauthorized connections to one of the free communication ports.

Inbuilt measures prevent automatic access when connecting to an unused communication port, but attempts should be prevented by protecting the communication ports of the CIU 888 (for example, field ports, host ports and ethernet ports).

Follow company-mandated and country-specific security measures applicable to your site in addition to these measures.

2.1 USB ports

The CIU 888 has three USB ports: one located at the front (see FIGURE 2-1) and two at the back (see FIGURE 2-2).

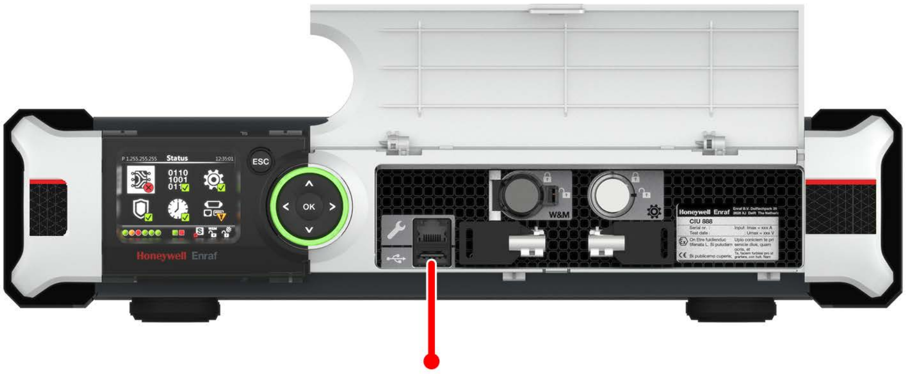


FIGURE 2-1 CIU 888: USB port located at the front

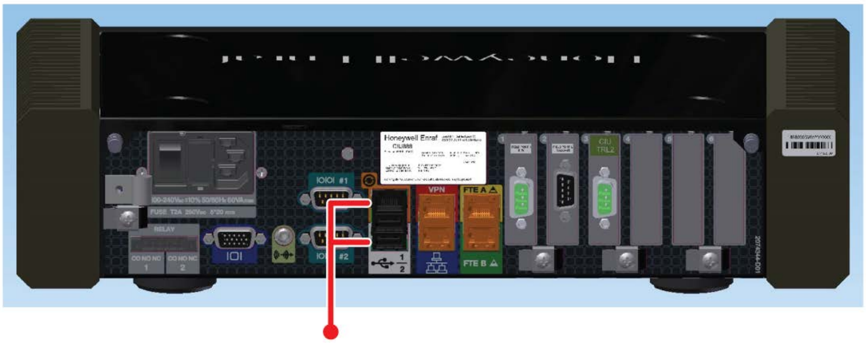


FIGURE 2-2 CIU 888: USB ports located at the back

By default, the USB ports are disabled to protect against virus and malware intrusion, and unauthorized access.

Only after starting an upgrade, the front USB will be enabled for a limited time. After the firmware upgrade package is read, the port will be automatically disabled.

The USB-ports at the back are reserved for future use and currently disabled.

To secure the USB ports:

- It is recommended to protect access to the required USB ports, for example by using a physical lock on top of the USB drive.
- It is recommended to perform an anti-virus scan on the USB drive before inserting it into the CIU 888 USB port.

2.2 Configuration lock key switch

The CIU 888 provides a Configuration lock key switch (see FIGURE 2-3) to lock the configuration settings of CIU 888 (both LM relevant and non-LM relevant), preventing unauthorized changes to the configuration.

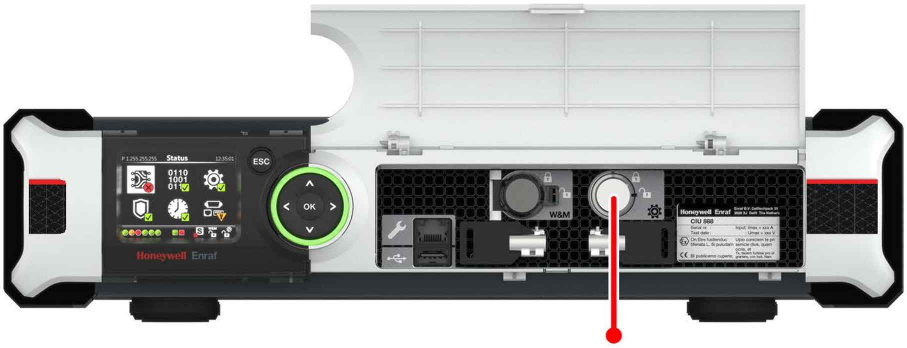


FIGURE 2-3 CIU 888: Configuration lock key switch

2.3 W&M lock key switch and W&M sealing

Tank Inventory systems subject to Legal Metrology can be required to be sealed.

In those applications, specific parameters with effect on the inventory calculations, need to be sealed after inspection. During the inspection, a notified body will seal the correct settings of the CIU 888 and prevent undetected changes to these settings.

The W&M lock with sealing provisions allow easy, clear and secure sealing.

NOTE: Refer to the CIU 888 Introduction Manual (Part No. 4417591) for more information.

During custody transfer, a high level of accuracy and consistency of data is of great importance to both the company delivering the product and the eventual recipient, when transferring a product.

The CIU 888 provides a W&M lock key switch that can be used to seal the device and provide LM approved data.

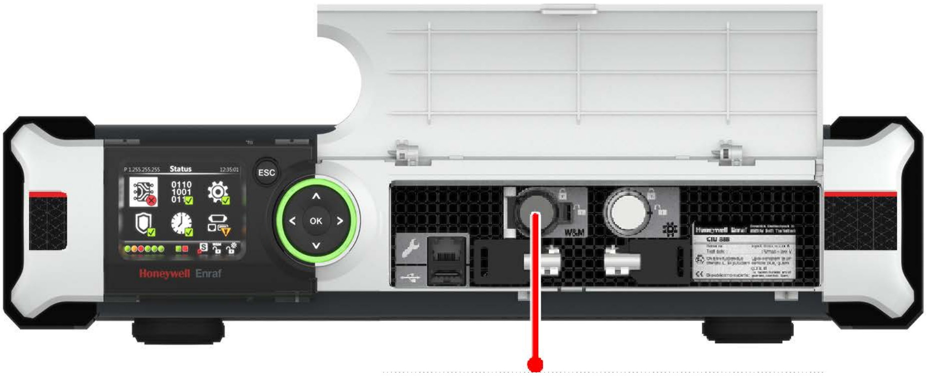


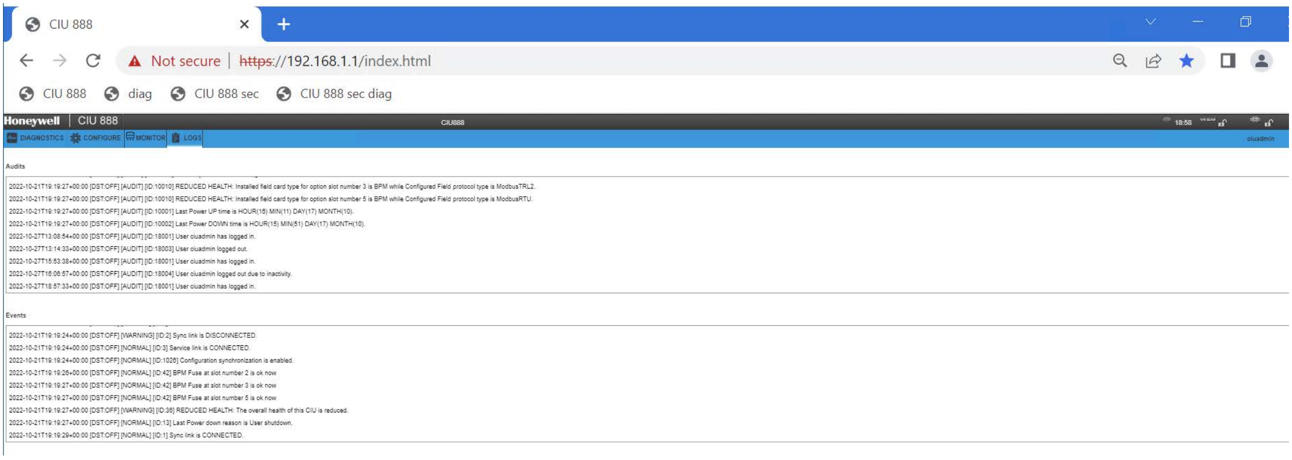
FIGURE 2-4 CIU 888: W&M lock key switch

The CIU 888 can be sealed by a Legal Metrology (LM) authority (e.g. NMi) in order to support W&M certified applications for custody transfer, accounting and duties. By sealing the CIU 888, the LM authority states that the system performs all calculations (e.g. volume/mass) correctly according the applicable standards, and that the settings used are corresponding the application.

NOTE: *Refer to the CIU 888 Sealing Guide (Part No. 4417595) for more information.*

2.4 Audit and event logging

The CIU 888 Web interface features a log function, which enables authorized users to view audit and event records that were logged during operation of the CIU 888.



Audits

```
2022-10-21T19:19:27+00:00 [DST:OFF] [AUDIT] [ID:10010] REDUCED HEALTH: Installed field card type for option slot number 3 is BPM while Configured Field protocol type is ModbusTRL2.
2022-10-21T19:19:27+00:00 [DST:OFF] [AUDIT] [ID:10010] REDUCED HEALTH: Installed field card type for option slot number 5 is BPM while Configured Field protocol type is ModbusRTU.
2022-10-21T19:19:27+00:00 [DST:OFF] [AUDIT] [ID:10001] Last Power UP time is HOUR(16) MIN(11) DAY(17) MONTH(10).
2022-10-21T19:19:27+00:00 [DST:OFF] [AUDIT] [ID:10002] Last Power DOWN time is HOUR(15) MIN(51) DAY(17) MONTH(10).
2022-10-27T13:08:54+00:00 [DST:OFF] [AUDIT] [ID:18001] User ciuadmin has logged in.
2022-10-27T13:14:33+00:00 [DST:OFF] [AUDIT] [ID:18003] User ciuadmin logged out.
2022-10-27T15:53:38+00:00 [DST:OFF] [AUDIT] [ID:18001] User ciuadmin has logged in.
2022-10-27T16:06:57+00:00 [DST:OFF] [AUDIT] [ID:18004] User ciuadmin logged out due to inactivity.
2022-10-27T18:57:33+00:00 [DST:OFF] [AUDIT] [ID:18001] User ciuadmin has logged in.
```

Events

```
2022-10-21T19:19:24+00:00 [DST:OFF] [WARNING] [ID:2] Sync link is DISCONNECTED.
2022-10-21T19:19:24+00:00 [DST:OFF] [NORMAL] [ID:3] Service link is CONNECTED.
2022-10-21T19:19:24+00:00 [DST:OFF] [NORMAL] [ID:1026] Configuration synchronization is enabled.
2022-10-21T19:19:26+00:00 [DST:OFF] [NORMAL] [ID:42] BPM Fuse at slot number 2 is ok now
2022-10-21T19:19:27+00:00 [DST:OFF] [NORMAL] [ID:42] BPM Fuse at slot number 3 is ok now
2022-10-21T19:19:27+00:00 [DST:OFF] [NORMAL] [ID:42] BPM Fuse at slot number 5 is ok now
2022-10-21T19:19:27+00:00 [DST:OFF] [WARNING] [ID:36] REDUCED HEALTH: The overall health of this CIU is reduced.
2022-10-21T19:19:27+00:00 [DST:OFF] [NORMAL] [ID:13] Last Power down reason is User shutdown.
2022-10-21T19:19:29+00:00 [DST:OFF] [NORMAL] [ID:1] Sync link is CONNECTED.
```

FIGURE 2-5 CIU 888 Web interface: *Logs* window

Regularly check the audit and event logs to view user and system activity pertaining to CIU 888 operations.

Audit and event records can provide a means to help accomplish several security related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification.

- Individual accountability
  Log data support accountability by providing a trace of user actions. While users cannot be prevented from using resources to which they have legitimate access authorization, analysis of audit and event logs can be used to examine their actions.
- Reconstruction of events
  Log data can be reviewed chronologically to determine what was happening both before and during an event.
- Intrusion detection
  Log data can be reviewed to detect unusual or unauthorized events, e.g. failed login attempts, network activity levels, memory utilization, key data access, etc.
- Problem identification
  Log data can be used to identify problems that need to be addressed, e.g. resource utilization, trending, etc.

A regular check of the audit and event log can identify unnoticed activities during operations, such as attempts to access or change settings. Detection will help improve site security and data integrity.

2.5 Users and Roles

CIU 888 Web Interface supports only one user. The user of CIU 888 web interface would be typically the Service Engineer who commission CIU 888.

The following operations are possible via Web interface:

1. View of CIU 888 configuration
2. View of CIU 888 diagnostics
3. Upload / View of License
4. View / download of Logs
5. Monitor tank data

This page is intentionally left blank

CHAPTER 3 SECURE COMMUNICATIONS

3.1 Network security

The increased need for continuous availability of data results in challenges to connect networks that are traditionally separated from one other, for example control networks and business networks. By segregating the company's site network into smaller (sub) networks and by enforcing a ruleset controlling which computing devices are permitted to communicate with other computing devices, the methods and level of access to sensitive information can be minimized and an intruder's ability to move across networks is limited.

In order to address the aforementioned challenges, the CIU 888 fully supports Ethernet based infrastructures. The CIU 888 has six dedicated Ethernet ports as shown in FIGURE 3-1 and FIGURE 3-2.

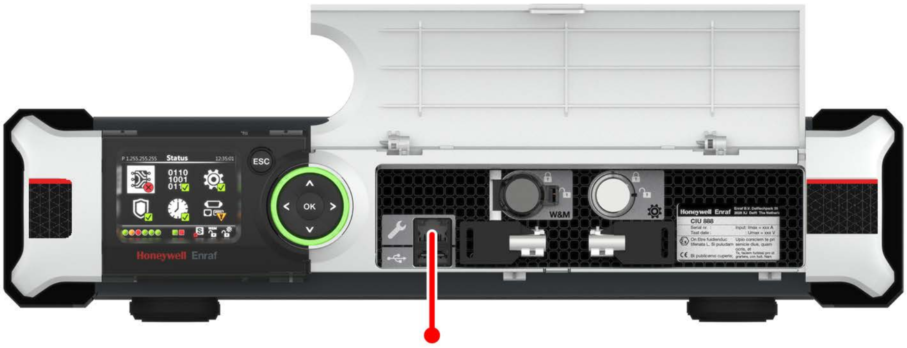
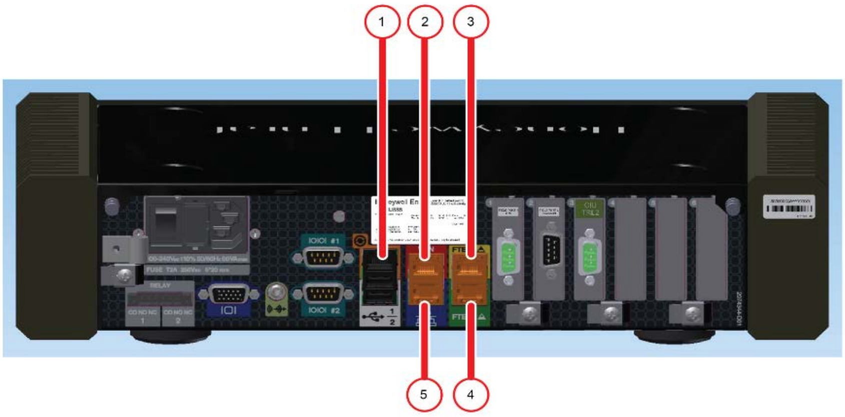


FIGURE 3-1 CIU 888: Service port at the front



1. Sync Link port
2. VPN port
3. FTE port A
4. FTE port B
5. Office LAN port

FIGURE 3-2 CIU 888: Ethernet ports at the back

The function of each port is described in TABLE 3-1.

TABLE 3-1 Description of the Ethernet ports of the CIU 888

Ethernet port	Description
Service port	The Service port is used to set up a point-to-point connection between the CIU 888 and a service PC/laptop allowing service technicians to configure the CIU 888 including field instruments connected to the CIU 888, and to view diagnostics. The Service port is also used to perform firmware upgrades and to view/update the license of the CIU 888. Note: The Service port is provided with a fixed non-routable IP-address.
Sync Link port	The Sync Link port is used as a dedicated, private synchronization link (point-to-point) between two CIU 888s in a redundant system setup. Note: The Sync Link port is provided with a non-routable IP address.
VPN port	The VPN port is used to set up a local network connection between the CIU 888 and a service PC/laptop allowing service technicians to configure the CIU 888 including field instruments connected to the CIU 888 and to view diagnostics. The VPN port is also used to perform firmware upgrades and to view/update the license of the CIU 888. Note: The VPN port is provided with a configurable non-routable IP-address. Multiple CIU 888s can be connected to the Service node via a local network switch.
FTE ports	The FTE ports are used to provide tank inventory data from CIU 888 to Modbus and / or to OPC UA TCP host system. Note: FTE ports can be enabled / disabled for Modbus TCP functionality with configuration option.
Office LAN port	The Office LAN port is used to provide tank inventory data from CIU 888 Modbus and / or to OPC UA TCP host system. Note: Office LAN ports can be enabled / disabled for Modbus TCP functionality with configuration option.

Network segregation is supported by the CIU 888 - an embedded firewall ensures that only the required socket ports are opened for each enabled Ethernet port. For example, HTTP (port 80) and HTTPS (port 443) are enabled only on the Service port and VPN port. The firewall monitors and identifies all incoming and outgoing network traffic and blocks all unwanted network traffic.

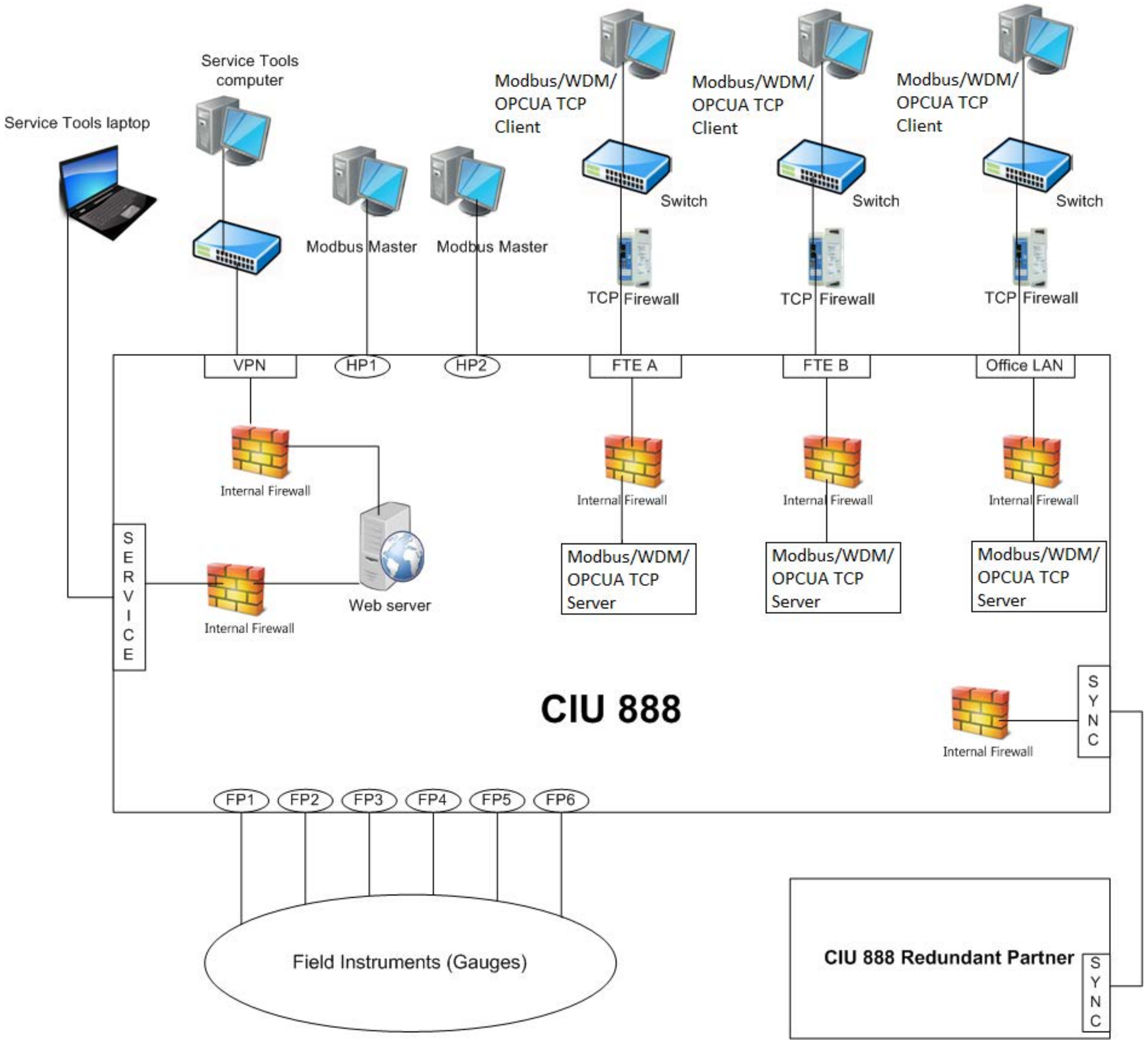


FIGURE 3-3 Network segregation within the CIU 888.

NOTE: The firewall is fully configured within the CIU 888 on delivery.

Customers must ensure CIU 888 is segregated from the external network.

The field devices, host systems/applications, and networks involving the CIU 888 field/host ports should be protected.

3.2 Interface-level security

3.2.1 HTTPS communication between Web clients and CIU 888 web server

HTTPS is used to ensure secure communication between the Web clients (CIU 888 web interface, CIU 888 Service Tool and Ensite Pro to CIU 888 Migration tool) and the CIU 888.

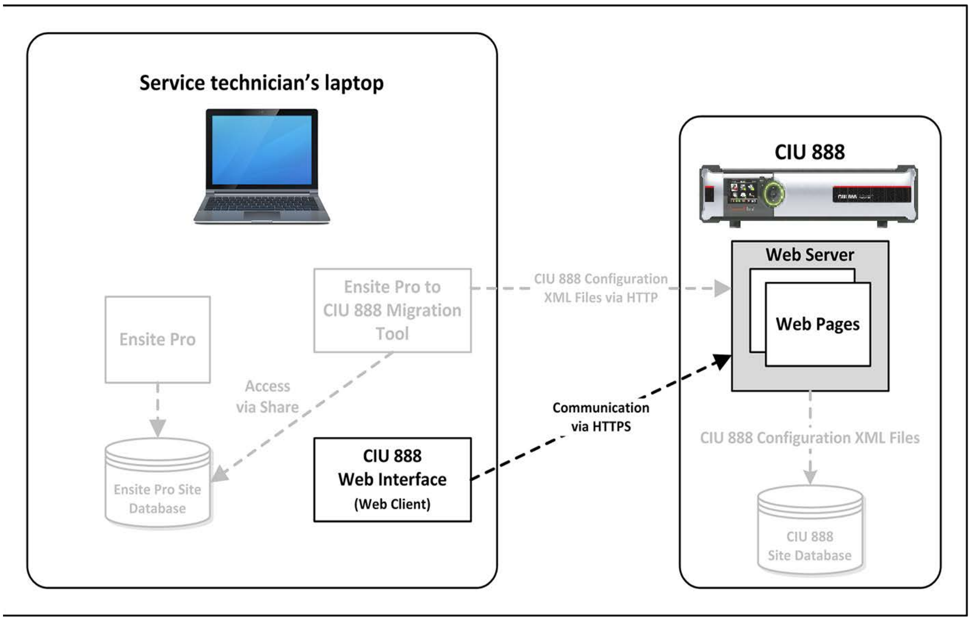

Service technician's laptop
Ensite Pro
Ensite Pro to CIU 888 Migration Tool
Access via Share
Ensite Pro Site Database
CIU 888 Web Interface (Web Client)
CIU 888 Configuration XML Files via HTTP
Communication via HTTPS
CIU 888
Web Server
Web Pages
CIU 888 Configuration XML Files
CIU 888 Site Database

FIGURE 3-4 HTTPS communication between Web clients and CIU 888

3.2.2 Download security certificate

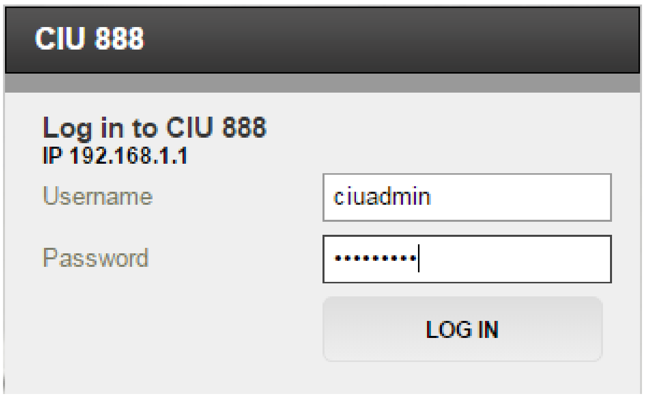
Download and install CIU 888 certificate to ensure the connection is recognized as safe, preventing unnecessary security warnings. After that the HTTPS connection can be established. See *CIU 888 Configuration Manual (Part No. 4417584)* for detailed instructions.

3.2.3 Login protection for web access

In order to prevent unauthorized access, the Web clients communication to CIU 888 box is secured by username and password authentication (see FIGURE 3-5). Only strong passwords are allowed, i.e., passwords that meet the following criteria:

- The password must not be the same as the previous password
- The password must not be a dictionary word (e.g. password)
- The password must be at least eight characters long
- The password must contain at least one number and one special character
- The password must not contain special characters **!** (exclamation mark), **'** (single quotation mark) and **"** (double quotation mark)

NOTE: *It is highly recommended to change the password at regular intervals, for example every 6 months. See the CIU 888 System Administration Manual (Part No. 4417598) for detailed information regarding recommendations for passwords, enforcement of password changes, and so on.*



CIU 888

Log in to CIU 888
IP 192.168.1.1

Username: ciuadmin

Password: ••••••••••

FIGURE 3-5 *CIU 888 login* window

Only one Web client instance is allowed to be active at a time. If a user tries to start another session, the system prompts the user to terminate the active session before proceeding.

Furthermore, if there is no user activity in the Web client for 10 minutes, the session is timed out.

If the user enters wrong password twice consecutively, then the user will not be allowed to login for 10 minutes (check)

3.2.4 CRC protection

To protect the integrity of the site configuration data, the contents of this database are validated using the method of Cyclic Redundancy Checks (CRCs). Also during startup, CIU 888 validates its configuration with corresponding CRCs. If there is a mismatch, then CIU 888 will not start its intended functions.

The tank records exposed via Modbus also contain CRCs that can be used for validation by the Modbus hosts using the data.

This error-detecting method makes it possible to easily detect accidental changes to data, and provides quick and reasonable assurance of the integrity of data.

NOTE: *See the Protocol Manual - Modbus / OPC UA TCP Host CIU 888 (Part No. 4417588) for more information.*

3.2.5 TCP Communication between TCP Clients and CIU 888 TCP Server

CIU 888's internal firewall is configured such that only required software ports are allowed via FTEA, FTEB and Office LAN ports. In case of CIU 888 integration with third party systems, FTEA, FTEB and Office LAN ports should be configured in different subnets. In case of CIU 888 integration with Experion PKS system via FTE network, FTEA and FTEB ports should be configured in same subnet and Office LAN port should be configured in different subnet. In case of CIU 888 connected to a gateway device, the gateway device's IP address should be configured in CIU 888.

3.2.5.1 Modbus communication between Modbus TCP Clients and CIU 888 Modbus TCP Server

An external Modbus TCP firewall (like Honeywell Tofino Modbus TCP firewall (EPS9211-ET-HN1-2)) is recommended to prevent unwanted TCP/IP traffic (bursts of messages) entering into CIU 888.

It is recommended to disable Modbus TCP functionality on the unused Ethernet host ports through CIU 888's configuration option. It is also recommended to configure the Modbus Server Idle Timeout parameter per host Ethernet port, the Turnaround Delay parameter per Modbus client in CIU 888, and IP address filtering per host Ethernet port. See the CIU 888 Configuration Manual (Part No. 4417584) for detailed instructions.

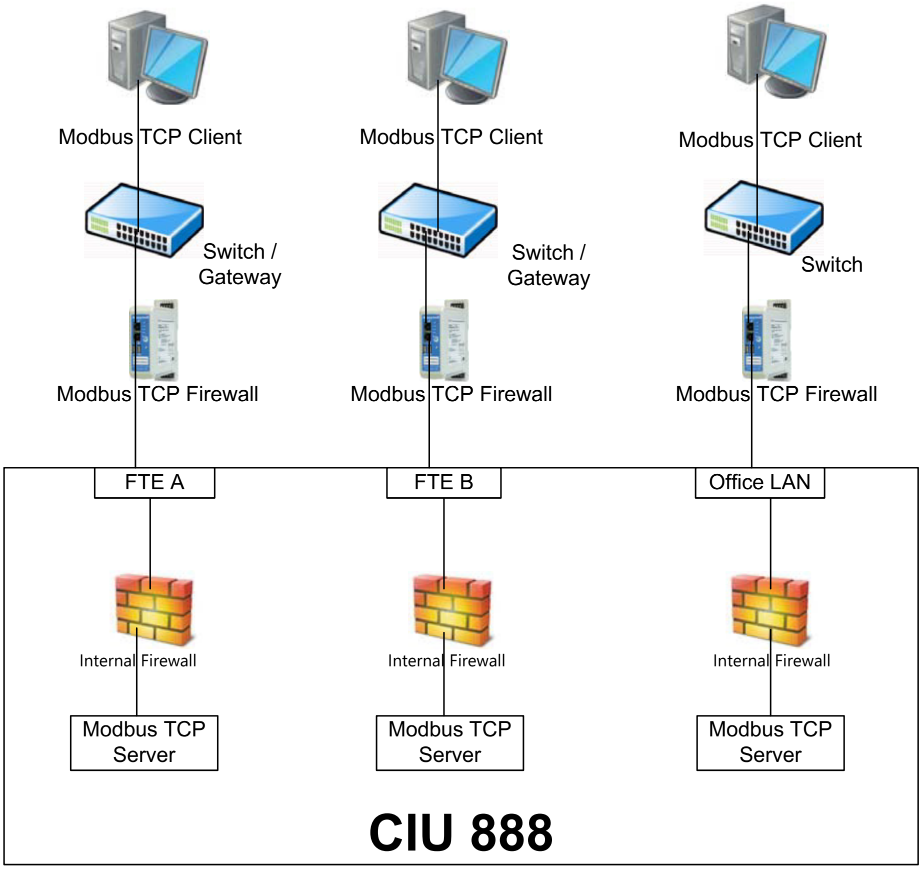


FIGURE 3-6 Modbus communication between Modbus TCP Clients and CIU 888 Modbus TCP Server

3.2.5.2 OPC UA communication between OPC UA TCP Clients and CIU 888 OPC UA TCP Server

Security in OPC UA

OPC UA provides security by authenticating clients and servers and encrypting communications using X.509v3 application instance certificates. Asymmetric public key algorithms are used for symmetric key generation and exchange periodically, with most client/server communication secured with symmetric algorithms.

A secure server must be provisioned with a certificate during commissioning. This can either be done by generating a default self-signed certificate on the device or by storing a certificate on the device that is generated elsewhere and signed by CA.

Note: It is strongly recommended that the end user of the OPC UA product install a corporate-signed certificate. The use of a self-signed certificate is highly discouraged. Once a secure channel is established between a client and a server, user authentication and permissions are then handled at the session level. We only support anonymous.

Supported Transport Protocol

UA-TCP UA-SC Binary (commonly known as opc.tcp)

Supported Security Facet

- Security Policy – None
- Security Policy – Basic256Sha256.
- Security Policy - AES128SHA256_RSA_OAEP
- Security Policy - AES256SHA256_RSA_PSS

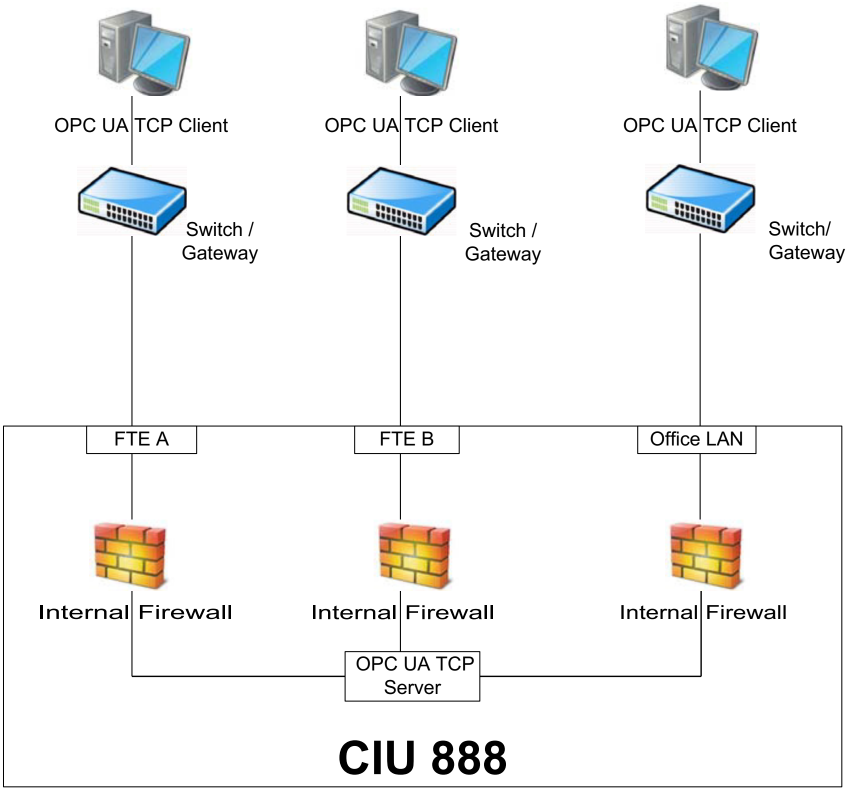


FIGURE 3-7 OPC UA communication between OPC UA TCP Clients and CIU 888 OPC UA TCP Server

CHAPTER 4 SECURING CIU SERVICE NODE

The CIU Service node is used for commissioning and maintaining the CIU 888 box, see FIGURE 3-3. The CIU Service node could be Service technician's laptop or a Windows desktop that connects to CIU 888. The CIU Service node hosts the following applications:

- CIU 888 web interface
- CIU 888 Service Tool
- Ensite Pro + Migration Tool

NOTE: *Though not typical, these applications may run/reside on different Service nodes*

4.1 General Service node security tasks

CIU Service node connects to CIU 888, hence ensure the following:

1. Protect from unauthorized access by applying site specific measures such as physical access control.
2. Enable Windows authentication for the CIU Service node.
3. Install anti-virus software on the CIU Service node.
4. Ensure that anti-virus has the latest updates and
5. Ensure that anti-virus is active and on-demand scan is enabled

4.2 Protect the data files

CIU 888 Service Tool and Ensite Pro store the configuration information in local database files. These applications also store and refer external files such as STRAP files and Entis Pro INI files. Ensure that these files are protected from unauthorized access.

Protect files such as STRAP files, log files, Entis Pro INI files when they are being transferred from source to CIU 888 or from CIU 888 to a different system/location.

4.3 Anti-virus scan

While providing external files as inputs for CIU 888 Service Tool or Ensite Pro, ensure that the files are scanned with anti-virus software. If an USB drive is used during this procedure, ensure that USB drive is also scanned with anti-virus software before usage.

4.4 CIU 888 Service Tool security measures

CIU 888 Service Tool performs input validation while accepting inputs such as, Device configuration files, user defined product tables etc..,

Some input files for CIU 888 Service Tool are signed with certificates to ensure integrity.

Installation files provided for CIU 888 Service Tool are signed with certificates to ensure appropriate identification.

APPENDIX A LIST OF ABBREVIATIONS

Abbreviation	Description
API	American Petroleum Institute
CIU	Communication Interface Unit
CRC	Cyclic Redundancy Check
DCS	Distributed Control System
DDOS	Distributed Denial of Service attack
FTE	Fault Tolerant Ethernet
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
NMi	Netherlands Measurement Institute (Nederlands Meetinstituut)
OIML	International Organization of Legal Metrology (from French: *__O__rganisation __I__nternationale de __M__étrologie __L__égale*)
PLC	Programmable Logic Controller
PTB	Physikalisch-Technische Bundesanstalt
USB	Universal Serial Bus
VPN	Virtual Private Network
W&M	Weights and Measures
LM	Legal Metrology

This page is intentionally left blank

For service-related questions, contact:

Technical Assistance Centre

Phone:

+1 800 423 9883 or

+1 215 641 3610

E-mail:

HFS-TAC-SUPPORT@honeywell.com

For More Information

To learn more about Honeywell Enraf's solutions, contact your Honeywell Enraf account manager or visit www.honeywellenraf.com.

Americas

Honeywell Enraf Americas, Inc.
1250 West Sam Houston Pkwy S.
Houston, TX 77042
USA
Phone: +1 (480) 293-2042
Email: enraf-us@honeywell.com

Europe, Middle East and Africa

Honeywell Enraf
Delftechpark 39
2628 XJ Delft the Netherlands Phone:
+31 (0)15 2701 100
Email: enraf-nl@honeywell.com

Asia Pacific

Honeywell Pte Ltd.
17 Changi Business Park Central 1
Singapore 486073
Phone: +65 6355 2828
Email: enraf-sg@honeywell.com

4417597_Rev14
December2022

Honeywell