PROCESS INSTRUMENTATION AND CONTROLS

MODBUS NETWORKS IMPLEMENTATION STANDARD

DOCUMENT NO. ESF-500-STD-411

Watercare

Version: 1

Published Date: 19 August 2025

Copyright information

Disclaimer

Watercare Services Limited has endeavoured to ensure material in this document is technically accurate and reflects legal requirements. However, the document does not override governing legislation.

Watercare Services Limited does not accept liability for any consequences arising from the use of this document. If the user of this document is unsure whether the material is correct, they should refer directly to the relevant legislation and contact Watercare Services Limited.

More information

If you have further queries, please contact the **Digital Control Systems** team at:
DigitalControlSystems@water.co.nz

DOCUMENT CONTROL

Document owner	Control Systems Manager
Review	Control Systems Manager

Version history

Version	Description of revision	Published By	Date
1.0	First release	W. Strydom	19/08/2025

This document takes effect on the date of release and supersedes all prior versions.

Approvers / Reviewers

Name	Title	Role
Rodney Micallef	Control Systems Architect	Author / Reviewer
Preesen Moodley	Control Systems Team Lead	Reviewer
Jerome Chung	Control Systems Team Lead	Reviewer
Fernan Abuid	Control Systems Asset Specialist	Reviewer
Anthony Yung	Control Systems Manager	Approver / Document Owner

Table of contents

1. Purpose

1.1 Background

1.1.1 Objectives

The objective of this document is to provide clear guidance for the design and implementation of networks utilising the Modbus protocol within Watercare's control systems environments. It sets out standardised practices to ensure the correct selection of network topology, the use of appropriate networking infrastructure and Modbus-compatible slave devices, and the application of reliable and compliant wiring methods.

This standard applies to both new installations and upgrade projects involving Modbus communications within control systems environments. For new projects, it provides a foundation for designing reliable, future-proof networks that align with modern best practices. For upgrade scenarios, it offers guidance on transitioning from legacy systems, such as Modbus RTU over serial, to more scalable and maintainable solutions like Modbus TCP over Ethernet.

This Modbus implementation guideline also includes an addendum that outlines key rules and considerations for implementing EtherNet/IP in operational environments. While Modbus TCP remains the primary focus, the addendum provides high-level guidance for scenarios where EtherNet/IP is selected, ensuring consistency in design, device selection, and integration practices across both protocol types.

1.1.2 Audience

This document is intended for Watercare personnel, contractors and consultants involved in the electrical and control systems design of water and wastewater transmission sites, network sites and treatment plants. These include control systems architects, consultants and electrical design engineers designing the control systems and networking components of new sites and upgrades of existing sites.

1.1.3 Scope

This standard applies to sites where Modbus is used as a communication protocol between controllers and field devices. It encompasses Modbus networks used to interface with a range of equipment including variable speed drives (VSDs), soft starters, power quality meters (PQMs), protection relays, remote I/O modules, energy meters, and industrial instrumentation such as flow, level, and pressure transmitters. The standard is relevant to control environments utilising Kingfisher RTUs, Rockwell PLCs, and Emerson DeltaV controllers, ensuring consistent and reliable integration of Modbus-enabled devices.

1.1.4 Out of scope

This document does not cover Modbus implementations outside of control systems environments. It excludes guidance for proprietary industrial protocols or fieldbus systems not based on Modbus (e.g. Profibus, CANbus). The standard also does not apply to wireless Modbus implementations or cloud-based data aggregation platforms interfacing via protocol converters.

1.2 Compliance requirements

Compliance with this standard is required for all Watercare sites using the Modbus communication protocol.

Exceptions to this standard are not permitted.

1.3 Relevant Watercare Standards

This Standard shall be read in conjunction with the following Watercare standards:

- ESF-500-STD-404: *Operational Technology Network Switch Procurement Standard* - For guidance about the procurement of network equipment for connectivity between PLCs, RTUs and DCS controller to Modbus slave devices.
- ESF-500-STD-410: *Operational Technology Environment Data Cabling Standard* **-** For data cabling and standards including the implementation of structured cabling, network patching and recommendation of the appropriate equipment to achieve this standard.
- ESF-500-STD-601: *Material Supply Standard* **-** For a list of equipment that can be utilised in Watercare installations.

1.4 Abbreviations

Table 1*: Glossary*

Term	Description
PLC	Programmable Logic Controller
IO	Input / Output
OT	Operational Technology
DI	Digital Input
DO	Digital Output
AI	Analog Input
AO	Analog Output
VAC	Alternate Current Voltage
VDC	Direct Current Voltage
SLA	Service Level Agreement
EOL	End of Life

2. Overarching principles

The following principles shall be applied when designing Modbus networks, selecting Modbus-compatible devices, and configuring Modbus equipment for operational use.

2.1 Interoperability

2.1.1 Reliability of communications

Reliable communication in a Modbus network depends on correct configuration, protocol compatibility, and effective traffic management. The following key practices support consistent and stable interoperability:

- Protocol compliance: Ensure all devices support standard Modbus function codes and have well-documented register maps.
- Appropriate polling rates: Set polling intervals based on device performance, data criticality, and network load to avoid congestion.
- Timeouts and retries: Configure conservative timeout values and limited retries to maintain communication stability during faults.
- Avoiding broadcast overuse: Use broadcast messages cautiously (if at all), as not all devices support or respond predictably to them.

2.1.2 Equipment selection

Ensuring interoperability in a Modbus network requires adherence to established protocol standards and alignment between device capabilities and controller expectations. The following practices support reliable integration:

- Standards compliance: Select devices that conform to Modbus RTU or TCP specifications as defined by the Modbus Organisation.
- Supported addressing: Confirm that slave devices support the full address range and data types expected by the controller.
- Function code compatibility: Ensure devices support the Modbus function codes used by the controller (e.g. 03 for reading holding registers, 06 or 16 for writing).
- Data formatting alignment: Validate data types (e.g. 16-bit, 32-bit, floating point) and byte ordering to ensure correct interpretation.
- Avoiding low-quality devices: Be cautious with low-cost or generic Modbus devices, which may omit essential features, have undocumented registers, or handle edge cases inconsistently.
- Documentation availability: Choose devices with clear, vendor-provided Modbus documentation to support reliable configuration and troubleshooting.

2.2 Scalability

2.2.1 Accommodating future growth

For large-scale installations such as Water and Wastewater Treatment Plants utilising DCS architectures, scalable Modbus networks are very important. These systems necessitate the ability to seamlessly integrate new devices, I/O points, or communication loads without fundamental redesign, ensuring long-term operational efficiency and expansion capabilities.

Designing Modbus networks for scalability ensures they can grow with operational demands without requiring major redesign. The following practices support future expansion:

- Modular topologies: Use star or segmented designs that allow additional devices to be added with minimal disruption.
- Headroom in addressing: Reserve unused slave addresses or IP allocations to accommodate future devices.
- Performance capacity: Select devices that support more simultaneous connections and higher data throughput than currently needed.
- Flexible cabling infrastructure: Install spare network ports and conduits to simplify future wiring extensions.
- Configuration scalability: Use controllers that can manage expanded register maps and support additional polling without performance degradation.
- Documentation and labelling: Maintain accurate network diagrams and naming conventions to streamline integration of new components.

2.2.2 Applying modular topologies

Using modular topologies and structured address allocation simplifies network expansion and future modifications. The following practices enable scalable and organised growth:

- Segmented network design: Divide networks into logical zones or segments based on function or location to support isolated expansion. This approach is especially critical for large WTP/WWTP environments with DCS, as it limits the impact of a failure or security breach to a specific segment, enhancing overall system resilience and manageability
- Star topology preference: Adopt a star topology where each device connects to a central switch, allowing easy addition of new nodes.
- Reserved address ranges: Allocate address blocks (slave IDs or IP ranges) with spare capacity to accommodate future devices in each segment.
- Consistent naming and addressing conventions: Use structured naming and addressing to simplify integration, documentation, and troubleshooting.
- Expandable switch capacity: Choose Ethernet switches with spare ports or stackable options to support additional devices without replacement. Always allow for a minimum of 20% spare capacity.
- Labelled connection points: Clearly label spare network points and address slots in cabinets to facilitate controlled growth. Refer to Watercare standard mentioned earlier for labelling standards

2.3 Reliability and resilience

2.3.1 Network topologies and hardware redundancy

For DCS-based installations in large WTP/WWTP, where availability and redundancy are paramount and single points of failure are intolerable, implementing resilient network topologies and hardware with redundancy features is essential to minimise risk and enhance system reliability

Implementing resilient network topologies and hardware with redundancy features reduces the risk of single points of failure and enhances system reliability. The following practices support robust network design:

- Use of star or ring topologies: Design networks using star or ring configurations to isolate faults and maintain communication paths during failures.
- Redundant network paths: Deploy redundant ring protocols to ensure continued operation if one connection is lost where appropriate. This is particularly relevant for large plants where DeltaV is implemented, necessitating robust and independent communication channels to maintain operational continuity.
- Avoid daisy-chaining critical devices: Reserve daisy-chain connections for low-priority devices; isolate high-priority nodes with dedicated links.
- Segregation of critical assets: Group critical control devices separately from non-essential nodes to reduce risk exposure.
- Fault isolation planning: Ensure the design allows for quick identification and isolation of failed components without impacting the entire network.

2.3.2 Wiring protection and power conditioning

Ensuring robust physical infrastructure is essential to maintaining reliable Modbus communication in industrial environments. The following practices help minimise disruption due to physical or electrical issues:

- Use industrial-grade cabling: Select shielded, high-quality Ethernet (RS-485 cables if this is still being used) suitable for the environmental conditions and communication type.
- Protect against interference: Route communication cables away from high-voltage wiring and use proper grounding and shielding to prevent electromagnetic interference.
- Environmental sealing: Install connectors, junction boxes, and devices with appropriate IP ratings in areas exposed to dust, moisture, or chemicals.
- Physical cable protection: Use conduits, trays, or armoured cables to prevent mechanical damage in high-traffic or harsh areas.
- Power conditioning: Supply devices and switches with stable, filtered power through surge protectors, isolation transformers, or UPS systems.
- Strain relief and secure terminations: Ensure cables are properly anchored, with no stress on connectors or terminals, to avoid loose or intermittent connections.
- Use appropriate structured cabling as described by the ‘Operational Technology Environment Data Cabling Standard’ listed earlier in this document.

2.4 Standards compliance

Adhering to recognised control systems and industrial communication standards ensures compatibility, reliability, and long-term supportability of Modbus networks. The following practices promote consistent and standards-based implementation:

- Follow Modbus protocol specifications: Design and configure systems in accordance with Modbus.org guidelines for Modbus RTU and Modbus TCP.
    - Modbus Application Protocol Specification V1.1b
    - Modbus Messaging on TCP/IP Implementation Guide V1.0b.
- Apply cabling standards: Use structured cabling practices aligned with TIA/EIA-568 and TIA-1005-A for industrial environments.
- Reference IEC standards: Where applicable, align implementations with IEC 61158 and IEC 61784 for industrial communication protocols.
- Comply with industry-specific standards: Observe relevant national or sector-specific requirements, such as AS/NZS or water sector guidance, for control system design.
- Promote interoperability through conformance: Select devices and tools that demonstrate adherence to relevant communication and physical layer standards.
- Incorporate updates over time: Monitor changes to applicable standards and update internal practices accordingly to maintain compliance and best practice alignment.

3. Implementation guideline

This section provides practical guidance for the implementation of Modbus TCP in both new installations and upgrade systems where legacy Modbus RTU (typically operating over RS-485) is being replaced. It outlines recommended approaches for network design, hardware selection, wiring practices, and integration strategies to ensure reliable and future-ready communication infrastructure.

3.1 The Modbus TCP protocol

Modbus TCP is an Ethernet-based communication protocol used widely and is intended to be a replacement of the Modbus RTU protocol running over more modern network infrastructures.
It is an extension of the traditional Modbus protocol, originally designed for serial communication, adapted to run over standard TCP/IP networks.
Modbus TCP encapsulates Modbus messages within a TCP frame and transmits them over Ethernet, allowing for high-speed, high-reliability communication using standard networking infrastructure. Unlike Modbus RTU, which supports only a single master per network segment, Modbus TCP enables multiple clients (masters) to communicate with one or more servers (slaves) simultaneously, enhancing scalability and flexibility. Multi-master implementations are not common across Watercare.

Key characteristics of Modbus TCP include:

- Transport Layer: Utilises TCP/IP over Ethernet (typically port 502), enabling integration into existing LAN and WAN infrastructure.
- Message Structure: Modbus TCP retains the standard Modbus function codes but replaces the RTU frame’s CRC and address fields with a Modbus Application Protocol (MBAP) header.
- Connection Management: Supports persistent or on-demand TCP connections between clients and servers, with connection-oriented error handling and flow control.
- Multi-Master Capability: Allows several client devices—such as SCADA systems, HMIs, and data loggers—to simultaneously access the same server device.
- Standardisation: Fully defined by the Modbus Organisation’s specifications, specifically the Modbus Application Protocol Specification V1.1b (or later, such as V1.1b3) and the Modbus Messaging on TCP/IP Implementation Guide V1.0b, ensuring interoperability across vendors.

Modbus TCP is ideal for new systems requiring high-speed communications, remote diagnostics, and integration with modern supervisory platforms. It also serves as the preferred upgrade path from Modbus RTU where performance, scalability, or integration constraints exist.

In the context of this standard, Modbus TCP is the recommended protocol for all new implementations and should be adopted in upgrade projects where feasible to ensure alignment with current technology standards and to support future operational requirements.

3.2 Communication topology implementation

The communication topology defines how Modbus TCP devices are physically and logically connected within a control network. A well-planned topology ensures reliable data exchange, ease of maintenance, and flexibility for future expansion. This section outlines recommended approaches for implementing communication topologies for Modbus TCP networks, both in new installations and as part of upgrade projects from Modbus RTU.

3.2.1 Topologies

3.2.1.1 Star topology (preferred)

Each Modbus TCP device connects directly to a central Ethernet switch. This topology offers high reliability—if one device or cable fails, others remain unaffected—and simplifies fault isolation. Star topologies also allow consistent bandwidth per device and are easily scalable.

3.2.1.2 Ring topology

Devices or switches are connected in a closed loop. When used with managed switches that support ring redundancy protocols (e.g. Media Redundancy Protocol or Rapid Spanning Tree Protocol), the network can self-heal by rerouting traffic if a link fails. This topology is suited for high-availability systems but requires more complex configuration.

3.2.1.3 Daisy chain / line topology (limited use)

Devices with dual Ethernet ports and internal switch functionality can be connected in series. While cost-effective and suitable for short linear layouts, a failure in one device or cable can disrupt communication to all downstream devices. This topology is only recommended for low-criticality installations or where ring configurations are not feasible.

3.2.2 Reference architecture implementation guidelines

For large Water and Wastewater Treatment Plants employing multi-node DCS architectures, such as those utilizing Emerson DeltaV controllers, the integration of Modbus TCP devices requires specific considerations to ensure the highest levels of availability, redundancy, and resilience. These environments cannot tolerate single points of failure in communications. The following principles guide the integration of Modbus TCP devices into such complex control systems:

3.2.2.1 Segmented network architecture for distributed control

Implement a segmented network design where Modbus TCP devices are organized into logical zones or segments based on their functional area or physical location. This approach supports isolated expansion and limits the impact of localized communication issues, crucial for maintaining overall plant operation in a multi-node DCS. Each DCS controller node or processing unit should ideally connect to its dedicated segment(s) of Modbus devices, preventing a single network segment failure from impacting the entire DCS.

3.2.2.2 Redundant communication paths to DCS nodes

Deploy dual Ethernet links or redundant ring protocols to ensure continued operation if one connection to a DCS controller node is lost. This is particularly critical for high-availability systems where DeltaV is implemented. For critical infrastructure, communication networks should be designed with independent and physically separate channels to minimize common-mode failures.

Utilize industrial-grade managed switches that support ring redundancy protocols where ring topologies are approved, allowing the network to self-heal upon a link failure. However, star topologies are preferred for their reliability, simplicity, and ease of maintenance, with each Modbus TCP device connecting directly to a central Ethernet switch to isolate faults.

Implement redundant switches for critical communication paths to eliminate single points of failure. Ensure that the DCS controllers and HMIs are configured to support dual-network configurations as required by the system design.

3.2.2.3 Distributed device allocation

Distribute Modbus TCP field devices across multiple DCS controller nodes to ensure that a failure in one controller or its associated communication path does not compromise the entire system. This aligns with the DCS objective of distributing control and minimizing the impact of single component failures.

3.2.2.4 Hardwired I/O for critical functions

While Modbus TCP provides efficient data exchange, direct hardwired I/O remains the preferred implementation method for critical control and monitoring functions. For VSDs, actuated valves, and safety-related interlocks, hardwired connections ensure immediate, deterministic response, independent of network conditions. Modbus may be used in parallel for non-critical data, such as extended diagnostics or performance data, but should not replace hardwired signals where real-time control, fail-safe operation, or regulatory compliance is required in a DCS environment.

3.2.2.5 Controller compatibility and device selection

Select Modbus slave devices that are proven compatible with existing DCS controllers. Ensure devices support the necessary quantity of data points, efficient register layouts for block reading, and can reliably maintain connections under varying network traffic conditions.

3.2.2.6 Scalability and management for multi-node systems

Reserve unused IP allocations and maintain consistent naming and addressing conventions across all Modbus TCP segments to simplify integration, documentation, and troubleshooting within the multi-node DCS environment. Ensure expandable switch capacity (minimum 20% spare) to accommodate future growth.

3.2.2.7 Migration considerations for DCS upgrades

For upgrade projects involving DCS, all protocol migrations must include a review of controller capabilities, existing register maps, and required tag structures. IP addressing schemes, network segmentation, and configuration documentation must be updated as part of the migration. Migrations must be thoroughly tested in a controlled environment or simulation prior to live deployment, with all changes tracked via formal change control.

3.2.3 General implementation guidelines

- Switch Selection: Use industrial-grade, DIN-rail-mountable Ethernet switches for control environments. Refer to the Watercare's 'Operational Technology Network Switch Procurement Standard'.
- Redundancy Planning: For critical communication paths, implement redundant links or switches to eliminate single points of failure. Ensure controllers and HMIs support dual-network configurations if required by the multi-node DCS system design. For critical infrastructure and systems with dual or redundant processes, communication networks should be designed with independent and physically separate channels. This is fundamental in DCS environments to minimize the risk of common-mode failures across distributed controller nodes.
- Topology Documentation: Maintain accurate, up-to-date diagrams showing device locations, cable runs, IP addressing, and switch port assignments to support commissioning and troubleshooting.
- Scalability Considerations: Design topologies to allow easy addition of devices without significant rework. Ensure switch port availability and address space accommodates future growth.

For critical infrastructure and systems with dual or redundant processes, communication networks should be designed with independent and physically separate channels.

3.2.4 Upgrading legacy field networks

This section outlines recommended wiring configurations for migrating from RS-485 serial communication to Ethernet-based Modbus TCP. It presents two common scenarios: one in which the PLC and Modbus slave devices are co-located in the same area, and another where the slave devices are situated in a separate area from the controller. (In the diagram Area 1 is at a considerable distance from Area 2)

Migration from RS485 serial to Ethernet-based communication is mandatory when upgrading existing installations or replacing devices such as VSDs and soft starters.

In the first scenario, a direct star topology connecting all devices to a central switch is preferred. In the second, where distance becomes a factor, deploying a local Ethernet switch near the Modbus devices may be more practical to reduce cabling runs, improve maintainability, and minimise signal degradation.

However, introducing a remote switch adds an additional point of failure and should only be considered when the separation distance justifies the trade-off in cost and complexity.

Scenario 1: PLC and Modbus slaves are in the same area:

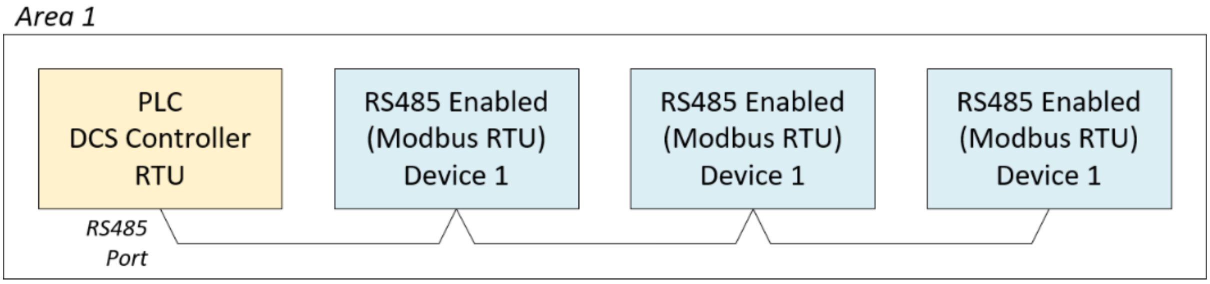

***Figure 1**: Modbus RTU*

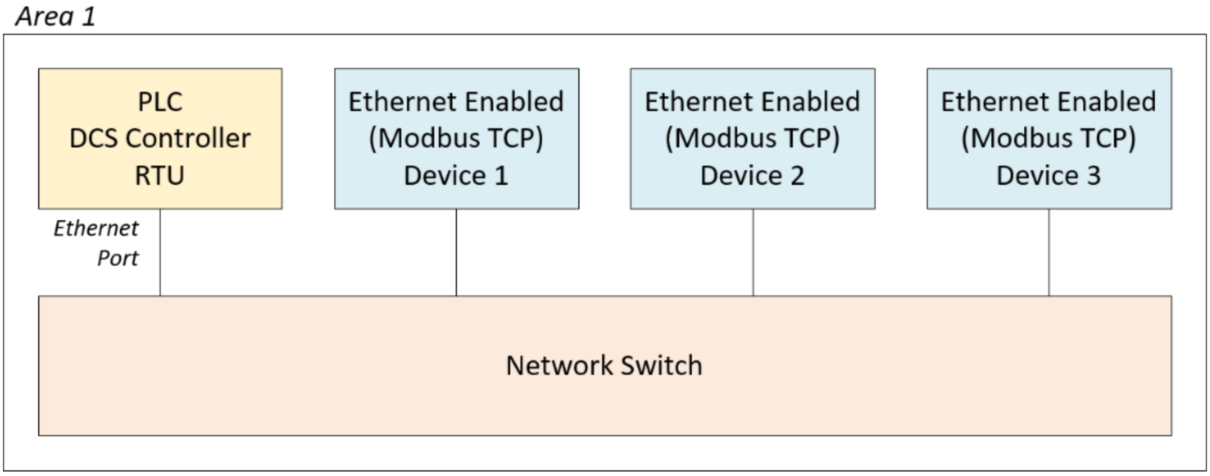

***Figure 2**: Modbus TCP*

Scenario 2: PLC and Modbus slaves are in different same area:

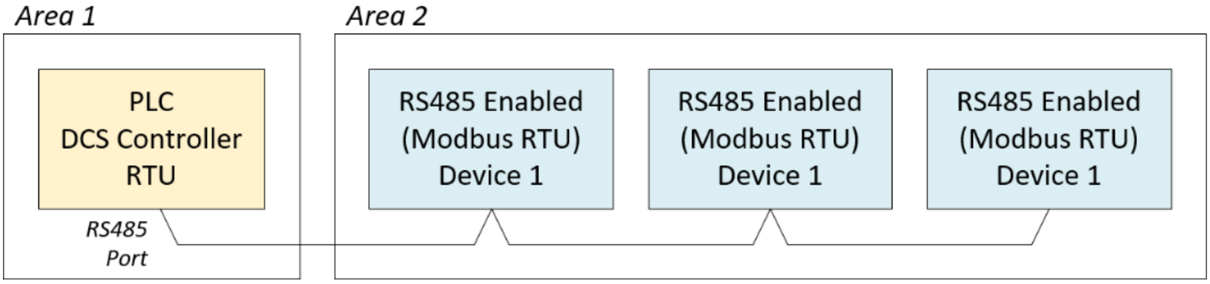
Area 1
Area 2
PLC
DCS Controller
RTU
RS485 Port
RS485 Enabled (Modbus RTU) Device 1
RS485 Enabled (Modbus RTU) Device 1
RS485 Enabled (Modbus RTU) Device 1

***Figure 3**: Modbus RTU*

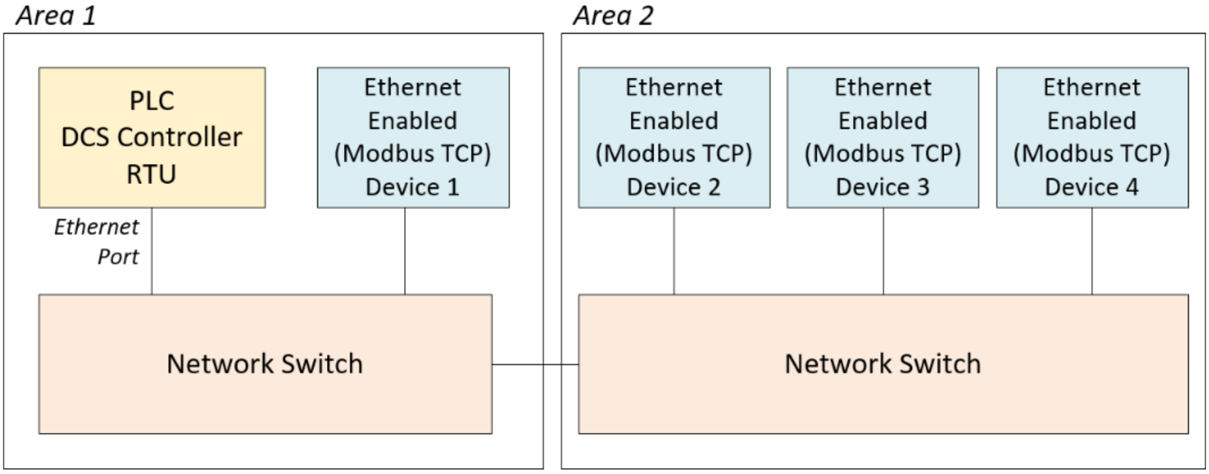
Area 1
Area 2
PLC
DCS Controller
RTU
Ethernet Port
Ethernet Enabled (Modbus TCP) Device 1
Ethernet Enabled (Modbus TCP) Device 2
Ethernet Enabled (Modbus TCP) Device 3
Ethernet Enabled (Modbus TCP) Device 4
Network Switch
Network Switch

***Figure 4**: Modbus TCP*

Ring networks are to be avoided due to their complexity and increased risk of misconfiguration. Star topologies are preferred for reliability, simplicity, and ease of maintenance. Use of ring topologies requires formal approval.

The diagrams provided serve as general guidance for optimal placement of network equipment. Actual layouts may differ significantly depending on site-specific requirements and physical constraints.

3.3 Communication hardware implementation

The installation methodologies listed in the Watercare's 'Operational Technology Environment Data Cabling Standard' must be used when upgrading to Ethernet Based Communications.

3.4 Hardwiring of critical I/Os

While Modbus TCP provides efficient communication for data exchange, direct hardwired I/O is the preferred implementation method for critical control and monitoring functions in Watercare.

Equipment such as variable speed drives (VSDs), actuated valves, and safety-related interlocks must retain hardwired connections for start/stop control, position feedback, fault status, and emergency functions. This ensures immediate, deterministic response, independent of network conditions or communication delays. Modbus may be used in parallel to access extended diagnostics and performance data, but it should not replace hardwired signals where real-time control, fail-safe operation, or regulatory compliance is required.

3.5 Hazardous areas

While Modbus TCP is commonly implemented in Transmission/Network sites (where hazardous areas are typically absent), larger Water Treatment Plants and Wastewater Treatment Plants facilities often contain Hazardous Areas, such as those classified under ATEX or IECEx zones. For installations within these environments, strict adherence to relevant hazardous area standards is mandatory to ensure safety and prevent ignition risks.

Compliance with AS/NZS 60079.14: Explosive atmospheres, electrical installations design, selection and erection is required for all Modbus network components and their associated infrastructure installed within designated hazardous areas.

Key considerations for Modbus TCP implementations in hazardous environments include:

- Network cabling: All network cabling within hazardous areas must be selected and installed in accordance with AS/NZS 60079.14 requirements. This includes consideration for cable type, routing, protection, and termination methods to maintain explosion protection concepts (e.g., intrinsically safe, increased safety, flameproof)
- Enclosure selection: All enclosures housing Modbus devices, switches, and other network components within hazardous areas shall be appropriately certified for the specific zone classification and protection concept. This includes ensuring the correct Ingress Protection (IP) rating and explosion protection marking (e.g., Ex d, Ex e, Ex i).
- Device certification: All Modbus slave hardware, network switches, and any other electrical equipment deployed in hazardous areas must be certified for use in the relevant zone (e.g., Zone 0, 1, or 2) and bear the appropriate hazardous area markings. Preference should be given to devices with recognised certifications like ATEX or IECEx.
- Zoning and intrinsic safety barriers: Where applicable, detailed hazardous area zoning diagrams must be followed, and intrinsic safety barriers (Ex i) shall be implemented for circuits extending into hazardous areas, as required to limit energy levels below ignition thresholds. Design and installation of such barriers must strictly comply with AS/NZS 60079.14 and device-specific requirements.
- Installation and maintenance: All installation, modification, and maintenance activities within hazardous areas must be carried out by certified personnel and adhere to the requirements of AS/NZS 60079.14 to maintain the integrity of the explosion protection.

3.6 Modbus TCP cybersecurity

3.6.1 Best practices for Modbus TCP security

To help mitigate inherent risks and strengthen the overall security posture of Modbus TCP networks, the following best practices are recommended. These measures are intended to guide system designers, engineers, and operators in implementing practical safeguards that reduce exposure to common vulnerabilities. While not exhaustive or universally mandatory, they represent a baseline for improving resilience against unauthorised access, communication spoofing, and other protocol-level threats.

3.6.1.1 Secure device authentication

Implement mechanisms to verify the identity of Modbus TCP clients and servers to prevent unauthorized devices from communicating on the network. This may involve:

- Strong Credentials: For devices that support user accounts, enforce complex passwords and regular rotation.
- Device Certificates: Utilise devices and network infrastructure that support digital certificates for mutual authentication, ensuring only trusted devices can establish connections.
- Centralised Authentication: Integrate Modbus devices into a centralized authentication system (e.g., RADIUS, Active Directory) where supported by the device and network architecture.

3.6.1.2 Message integrity verification

Ensure that Modbus messages have not been altered or tampered with during transit. Given that standard Modbus TCP does not inherently provide message integrity checks beyond basic TCP/IP mechanisms, this typically relies on network-level controls:

- Secure Communication Channels: Where available and supported by devices, utilize secure tunnels (e.g., IPsec VPNs) or other encrypted overlays to protect Modbus TCP traffic in transit. This is information not directly from the sources.
- Advanced Protocol Features: If MODBUS/TCP Security Protocol Specification v36 is adopted, leverage its defined mechanisms for message integrity, which may include cryptographic hashes. This is information not directly from the sources.

3.6.1.3 Network access controls

Implement strict controls to restrict unauthorized network access to Modbus devices and limit communication paths to only essential connections.

- Network Segmentation: Utilise Virtual Local Area Networks (VLANs) or physically separate subnets to isolate Modbus TCP networks from corporate IT networks and other less secure zones. This limits the attack surface and contains potential breaches.
- Firewall Rules: Implement robust firewall rules at network boundaries and between segments to permit only necessary Modbus TCP traffic (typically TCP Port 502) between authorised Modbus clients and servers.
- IP Whitelisting: Where feasible, select devices that support basic security measures, such as setting IP whitelists. Configure Modbus devices to accept connections only from pre-approved IP addresses of legitimate Modbus clients.
- Port Security: Disable unused ports on network switches and Modbus devices to prevent unauthorized connections. Implement port security features on switches to restrict which MAC addresses can connect to specific ports.

3.6.1.4 Mitigating risks related to cleartext communications in legacy Modbus implementations

Standard Modbus TCP inherently communicates in cleartext, meaning data is not encrypted and can be intercepted and read if network security is compromised. To mitigate this risk:

- Network Hardening: Rely on a robust network design that includes strong perimeter defences, secure tunnels (e.g., VPNs for remote access), and encryption at the network layer to protect the underlying Modbus TCP traffic.
- Physical Security: Ensure that physical access to network infrastructure (switches, cabling) and Modbus devices is strictly controlled to prevent direct tampering or unauthorized connections.
- Avoid Public Exposure: Strictly limit direct exposure of Modbus TCP devices or networks to public internet connections. Remote access should only be established via secure, encrypted VPNs with multi-factor authentication.

3.6.1.5 Secure device configuration and lifecycle management

- Secure Firmware Updates: Devices should support firmware updates via secure channels, and not rely solely on open, unauthenticated access for configuration. This ensures that firmware integrity is maintained and prevents the introduction of malicious code.
- Disable Unused Services: Deactivate any non-essential services or protocols on Modbus devices to reduce the attack surface.
- Regular Security Audits: Conduct periodic security audits and vulnerability assessments of Modbus networks and devices to identify and remediate weaknesses.

4. Modbus slave hardware selection

This section is intended as a guidance for the selection of new Modbus-enabled equipment

Selecting appropriate Modbus slave devices is critical to ensuring reliable communication, interoperability, and long-term maintainability of the control system. Slave devices may include variable speed drives (VSDs), power quality meters (PQMs), energy meters, valve controllers and soft starters.

All new devices intended to communicate with a PLC, RTU or DCS Controller must be Ethernet Enabled with Modbus TCP (EtherNet / IP is also accepted as an alternate protocol for Treatment Plants)

4.1 Protocol compatibility

- All selected devices must support Modbus TCP as required by the intended network design.
- Ensure that the device's Modbus implementation adheres to official Modbus.org specifications, including supported function codes and response timing behaviour.
- Devices should support the Modbus function codes required by the controlling RTUs or PLCs (e.g. read/write of coils and holding/input registers).

4.2 Interoperability and integration

- Choose devices with well-documented register maps, scaling information, and configuration tools.
- Where possible, select equipment that has been tested or proven compatible with existing controllers (e.g. Rockwell PLCs, Kingfisher RTUs, or DeltaV controllers).
- Avoid low-cost, generic devices with incomplete or inconsistent Modbus implementations, as they often lack critical features or diagnostics.

4.3 Performance and capacity

- Assess the device's ability to handle the required polling frequency and number of concurrent client connections for Modbus TCP.
- Confirm the device supports the necessary quantity of data points, and that register layouts are efficient for block reading minimising communication load. Some of the cheaper devices are limited in the amount of data points that can be access with a single poll.
- For TCP devices, ensure they can reliably maintain connections under normal and high network traffic conditions.

4.4 Environmental and mechanical suitability

- Devices must be rated for the environment in which they are installed, considering temperature, humidity, vibration, and ingress protection (IP rating).
- Industrial enclosures and robust connector types (e.g. M12, locking terminals) should be used where required.

4.5 Power and physical interfaces

- Confirm that slave devices support the available power supply voltage (e.g. 24VDC or 230VAC).

- Verify the presence of a reliable Ethernet interface, ideally with link and activity indicators for diagnostics.

4.6 Diagnostics and monitoring features

- Select devices that support basic diagnostics via Modbus, such as status codes, fault registers, or health indicators.
- Preference should be given to devices that provide local indicators (e.g. LEDs for power, communication, and fault) to aid in troubleshooting.

4.7 Vendor support and lifecycle

- Choose vendors with a reputation for reliable industrial equipment and responsive technical support.
- Ensure the product has a clear lifecycle roadmap, with available firmware updates, spares, and long-term availability.
- Documentation, firmware tools, and configuration utilities should be readily accessible and maintained by the vendor.

5. Modbus RTU implementation and exception justification

While this standard mandates the transition from Modbus RTU to Ethernet-based Modbus TCP for new installations and upgrade projects, it is acknowledged that specific operational circumstances or hardware limitations may necessitate the continued use of Modbus RTU or the temporary deployment of protocol gateways. This section provides a structured framework for evaluating and justifying such scenarios, aligning with the document's established "Known Exceptions". This section is particularly focused at the implementation of this standard in Treatment Plants where DeltaV is implemented.

Any decision to retain Modbus RTU beyond a phased migration period, or to employ Modbus gateways as a permanent solution, must be formally justified in writing and approved through the designated exception process by the architecture team.

Evaluation considerations for Modbus RTU implementation decisions

When assessing the feasibility and justification for retaining Modbus RTU or using temporary gateways, consider the following:

Device compatibility and Modbus protocol support

Does the existing Modbus RTU slave device inherently support Modbus TCP, or can it be readily upgraded/replaced with a TCP-compatible version that adheres to Modbus.org specifications? Preference should always be given to replacing legacy serial connections (RS-485/Modbus RTU) with Ethernet-capable devices supporting Modbus TCP.

If the device supports Modbus TCP, does it exhibit reliable communication without address conflicts when integrated into the intended network, especially with the primary controller.

If not, is the inability to modify its unit ID or slave address a limiting factor that makes Modbus TCP communication unworkable for multiple instances of the device? In such cases, Modbus RTU is permitted as an alternative, contingent on all involved Modbus slave devices supporting this mode.

Necessity and impact of Modbus TCP gateway hardware

- Is a new Modbus TCP gateway proposed as a solution to bridge Modbus RTU devices to the TCP network?
- Assess the implications of introducing a gateway: The use of Modbus gateways to overcome address conflicts or protocol limitations is generally not recommended as a permanent solution. Such devices introduce an additional point of failure into the control system architecture, add complexity to the network, and create a dependency on a single device for communication.

If a gateway is considered, can its deployment be strictly temporary as part of a phased migration, with a clear plan for its eventual removal or replacement with native TCP devices? Use of unsupported or unverified protocol converters as a permanent solution is not permitted without explicit sign-off from the architecture team.

Cost-Benefit analysis and lifecycle assessment (for RTU retention/replacement vs. gateway)

- Evaluate the total cost of ownership (TCO): Compare the cost of replacing the existing Modbus RTU device with a native Modbus TCP device versus the cost and long-term implications of implementing a Modbus TCP gateway or retaining Modbus RTU under exception.
- For single, low-cost devices (e.g., small VSDs) where direct TCP replacement might seem disproportionately expensive initially: While the document mandates migration for VSDs,

consider the long-term value of network simplicity, enhanced reliability, and reduced troubleshooting efforts that native TCP provides. Permanent gateways and non-standard solutions can lead to prolonged troubleshooting, increased operational risk, and higher long-term support costs due to added complexity and dependency.

Prioritise solutions that maintain direct, native communication and align with the principles of Scalability and Reliability and Resilience for future-proof networks.

Impact on network complexity, reliability, and supportability

- Complexity: Does the proposed solution (e.g., gateway, retained RTU segment) significantly increase network complexity, making it harder to design, document, commission, and troubleshoot? Star topologies are preferred for reliability, simplicity, and ease of maintenance.
- Reliability: How does the proposed solution affect the overall network reliability and resilience? Gateways introduce a single point of failure that can "disrupt data flow to multiple devices simultaneously" if they fail or are misconfigured. The objective is to design networks to "minimise single points of failure".
- Supportability: Will the solution be easily supportable by Watercare personnel, contractors, and consultants? Non-standard or complex setups often require specialised knowledge and can hinder effective troubleshooting. The standard aims to set out "standardised practices to ensure the correct selection of network topology" to enhance long-term supportability.

Appendix A: Implementation of ethernet/IP networks

This addendum provides supplementary guidance for the design and implementation of EtherNet/IP networks within Watercare’s Control Systems, where EtherNet/IP is used in place of, or alongside, Modbus TCP. It outlines key principles, design rules, and best practices to support reliable and maintainable communications in systems using the Common Industrial Protocol (CIP) over Ethernet.

This guidance applies to control systems networks where Rockwell or other EtherNet/IP-enabled devices are deployed for plant control and monitoring. It is relevant to both new installations and upgrade projects where EtherNet/IP has been selected as the preferred protocol due to system integration requirements or equipment compatibility.

Protocol overview

- EtherNet/IP operates over standard Ethernet using both TCP (explicit messaging) and UDP (implicit messaging).
- It is based on the CIP object model, enabling detailed data exchange, tag-based addressing, and high-speed, cyclic communications.
- It supports multicast traffic, deterministic communication, and multiple consumers per data source, making it suitable for complex control tasks such as motion, synchronisation, and safety.

Migration methodologies

This section defines the standard methodologies for migrating from legacy communication protocols to modern Ethernet-based alternatives during control systems network upgrades or equipment replacements. The objective is to ensure consistent, supportable, and secure communications across all platforms while aligning with the target architecture of the organisation.

When upgrading communication interfaces, protocol transitions shall follow defined pathways to ensure interoperability, ease of integration, and lifecycle support. Selection of target protocols must consider device type, controller compatibility, and long-term supportability.

Migration pathways

Non-Rockwell devices

Current Protocol	Permitted Migration Target(s)
Modbus RTU	Modbus TCP
Modbus TCP	Modbus TCP (no protocol change required)

- Devices from vendors such as Schneider Electric, Siemens, ABB, and others must be transitioned to Modbus TCP where upgrades are necessary.
- Legacy serial connections (RS-485/Modbus RTU) shall be replaced with Ethernet-capable devices supporting Modbus TCP.
- Protocol converters or serial-to-Ethernet gateways should only be used as a temporary migration measure.

- In cases where controllers (PLCs or RTUs) are not directly compatible with Modbus TCP a protocol converter (such as Ethernet/IP to Modbus TCP converter) can be used. (e.g. a known case where certain models of Rockwell PLCs are only compatible with Ethernet/IP)

Rockwell devices

Current Protocol	Permitted Migration Target(s)
Modbus RTU	Modbus TCP or EtherNet/IP
Modbus TCP	Modbus TCP or EtherNet/IP

- For Rockwell Automation hardware, preference shall be given to migrating to EtherNet/IP, as it offers native compatibility, improved diagnostics, and integration with Rockwell software environments.
- Where Modbus TCP is retained (e.g. due to multi-vendor integration or legacy dependencies), devices must conform to the same Modbus TCP implementation standards outlined in this document.
- The final selection between Modbus TCP and EtherNet/IP shall be based on system architecture, controller compatibility, and performance requirements, and must be documented as part of the design review process.

Implementation considerations

- All protocol migrations must include a review of controller capabilities, existing register maps, and required function codes or tag structures.
- IP addressing schemes, network segmentation, and configuration documentation must be updated as part of the migration.
- Legacy registers or tags shall be mapped consistently in the new protocol to avoid ambiguity or functional mismatch.
- Migrations must be tested in a controlled environment or simulation prior to live deployment, and all changes tracked via formal change control.

Exceptions

- Any deviations from the permitted migration paths must be justified in writing, reviewed by the OT design authority, and approved through the designated exception process.
- Use of unsupported or unverified protocol converters as a permanent solution is not permitted without explicit sign-off from the OT architecture team.

Known exceptions

An exception to the standard implementation approach for Modbus RTU may be justified under specific circumstances where hardware constraints limit the ability to follow preferred communication architecture. This exception applies particularly to Modbus slave devices that are already listed on Watercare's approved hardware register but exhibit configuration limitations that affect their use within a Modbus TCP environment.

A common example involves equipment such as the Kingfisher RTU, which is unable to communicate reliably with multiple Modbus TCP devices that share the same Modbus RTU address. In many cases, the Modbus slave devices in question do not support modification of their unit ID or slave address, either due to fixed firmware settings or restrictions imposed by the vendor. As a result, deploying multiple instances of such equipment on the same Modbus TCP network leads to address conflicts and unreliable communications, making the architecture unworkable.

Where this scenario arises and no suitable workaround is feasible, the use of Modbus RTU is permitted as an alternative. This allowance ensures continued interoperability with existing equipment while maintaining operational continuity. However, this exception is contingent upon all Modbus slave devices involved in the configuration being capable of supporting the Modbus RTU communication mode.

The use of a Modbus gateway to overcome address conflicts or protocol limitations is generally not recommended, as it introduces an additional point of failure into the control system architecture. While gateways can provide functional workarounds, such as address remapping or protocol bridging, they add complexity to the network and create a dependency on a single device for successful communication between the RTU and connected Modbus devices. If the gateway fails, becomes misconfigured, or experiences network issues, it can disrupt data flow to multiple devices simultaneously. For this reason, preference should be given to solutions that maintain direct, native communication between the RTU and end devices, using hardware and configurations that are fully compatible with the required protocol and addressing scheme.