Water Utilities

Cisco Reference Design

Introduction

Water utilities operate some of the most dispersed and consequential infrastructure in the public sector.

Treatment works, pumping stations, boreholes, reservoirs, and distribution networks must stay available through storms, droughts, and cyber incidents—often with aging SCADA, incomplete asset records, and field sites that still have no practical way to trench fiber.

At the same time, regulators and frameworks such as NIS2 expect demonstrable visibility, segmentation, and secure remote access across operational technology (OT), not only in the corporate office.

This Water Solution Design is Cisco's reference architecture for that reality.

It gives utility architects, partners, and system integrators a single, end-to-end blueprint: how to connect plants and remote assets, how to modernize from serial and TDM to IP, and how to embed security and automation into the network rather than bolting them on afterward.

The goal is not connectivity for its own sake, but a foundation for safe water delivery, efficient operations, and defensible compliance.

Who should use this document

- Water and wastewater utilities planning a network refresh, SCADA IP migration, or smart-water initiatives
- Systems integrators and OT partners standardizing Cisco designs across treatment, distribution, and remote sites
- IT/OT and cybersecurity teams aligning IEC 62443 zone thinking with NIS2-style governance

What the design addresses

One coherent model for every site type

From water and wastewater treatment works to pumping stations, boreholes, wells, storage tanks, and dam instrumentation.

The architecture scales from high-density plant rings to single-cabinet remote outstations backhauled over fiber, SD-WAN, cellular, or Ultra-Reliable Wireless Backhaul (URWB).

Industrial automation as it exists today

The design embraces multi-vendor SCADA and field protocols (DNP3, Modbus/TCP, Ethernet/IP, and others) and resilient L2 rings (Cisco REP, IEC MRP).

It also supports legacy serial devices, backhauling serial data to operations centers while utilities migrate from serial and TDM to IP at a controlled pace.

WAN and operations at scale: Software-defined WAN (SD-WAN) provides flexible underlays, centralized policy, and integrated security. It delivers the operational consistency needed to manage hundreds of geographically scattered sites without per-site custom firewall sprawl.

Security built into the architecture—aligned with NIS2 and critical-infrastructure expectations, the design delivers:

- Visibility into plant and remote OT devices and their communications (Cisco Cyber Vision)
- Segmentation and electronic security perimeters (VLANs, TrustSec with SGTs and dACLs where adopted)

- Detection and response support through integration with the broader Cisco Secure portfolio and SIEM
- Data protection and disciplined remote access (for example, Cisco Secure Equipment Access) instead of always-on VPNs into OT.
- Proactive network assurance using centralized management and analytics (Catalyst Center, SD-WAN observability).

Edge intelligence where the asset lives

Catalyst industrial routers and IOx application hosting aggregate Ethernet and serial field data, run local analytics, and reduce dependence on extra gateways and PCs in harsh, space-constrained cabinets.

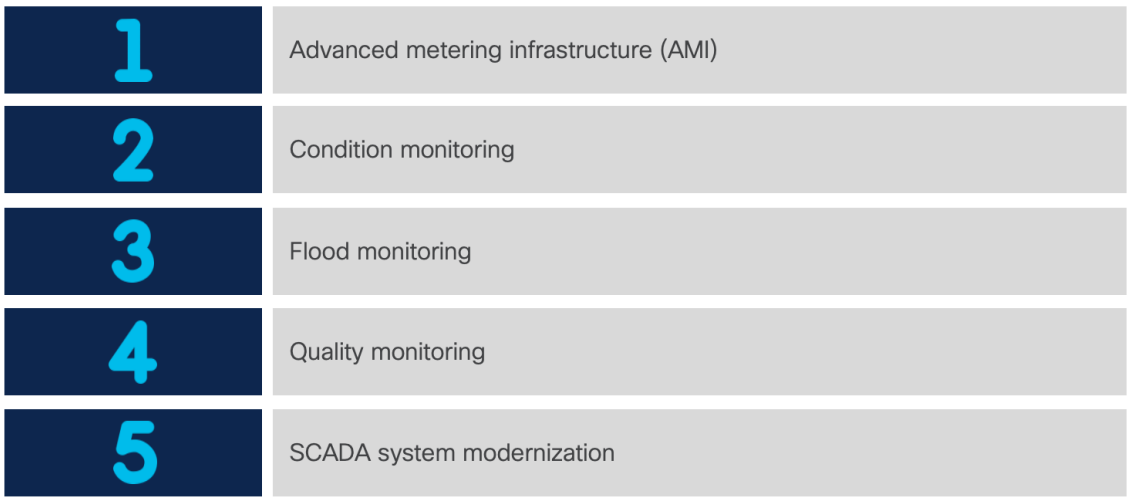
A path off legacy networking

Follow practical guidance to refresh obsolete switches and routers while preserving uptime for SCADA and brownfield interoperability.

The sections that follow move from utility use cases (metering, quality, flood response, condition monitoring, SCADA modernization) through network engineering patterns, remote asset connectivity, cybersecurity, and edge services.

Teams can adopt the whole reference design or implement phased capabilities matched to budget and risk.

Figure 1. Use Cases



Use Cases

Advanced Metering Infrastructure (AMI)

Advanced Metering Infrastructure (AMI) enables two-way communication between utilities and customers' meters.

It provides real-time or near-real-time data collection and remote-control capabilities.

Core Components

- **Smart Meters**: Digital meters with communication capabilities installed at customer premises to measure consumption (water, electricity, gas).
- **Communication Network**: Wireless mesh networks, cellular, or RF systems that transmit data between meters and the utility.
- **Head-End System:** Central data collection and management platform that processes meter data and manages the network.
- **Meter Data Management System (MDMS):** Software that validates, stores, and analyzes the massive volumes of consumption data.

Primary Use Cases

- **Automated Meter Reading**: Eliminates manual meter reading, reducing labor costs and human error. Meters transmit readings automatically at scheduled intervals (hourly, daily).
- **Demand Response and Load Management**: Utilities can monitor consumption patterns in real-time and implement time-of-use pricing or send signals during peak demand to encourage conservation or activate load control devices.
- **Leak Detection (Water)**: Continuous monitoring identifies abnormal consumption patterns indicating leaks. For water utilities, this can detect both customer-side leaks and distribution system losses quickly, preventing water waste and infrastructure damage.
- **Outage Management**: Smart meters send "last gasp" signals when power is lost, enabling utilities to pinpoint outage locations immediately. They also confirm restoration without dispatching crews.
- **Theft Detection**: Identifies tampering or unauthorized usage through consumption anomalies and meter health diagnostics.
- **Improved Billing Accuracy**: Eliminates estimated bills based on actual consumption data. Supports flexible billing cycles and prepaid models.
- **Customer Engagement**: Provides customers with detailed consumption data through web portals or mobile apps, enabling them to understand usage patterns, set budgets, and receive alerts for unusual consumption.
- **Asset Management:** Meter health monitoring provides data on battery levels, communication quality, and device failures, enabling proactive maintenance.
- **Distribution System Optimization**: Aggregated consumption data helps utilities optimize infrastructure investments, identify capacity constraints, and plan system improvements.
- **Regulatory Compliance**: Automated data collection supports compliance with conservation mandates, environmental reporting, and rate case requirements.

Benefits

- Operational efficiency: 30–50% reduction in meter reading costs.

- Revenue protection: Detection of non-technical losses and billing errors.
- Customer satisfaction: Accurate billing and self-service tools.
- Conservation: Visibility drives 5-15% reduction in consumption.
- System reliability: Faster outage response and reduced service interruptions.

Condition Based Monitoring (CBM)

Condition-Based Maintenance is a predictive maintenance strategy that monitors the actual condition of assets in real-time to determine when maintenance should be performed. For water utilities, this represents a shift from reactive (fix when broken) or time-based (scheduled regardless of condition) approaches to data-driven maintenance optimization.

Core Components

- **Sensors and Instrumentation**: Vibration sensors, temperature monitors, pressure transducers, flow meters, acoustic sensors, motor current analyzers, and oil quality sensors installed on critical assets.
- **Data Acquisition Systems:** SCADA systems, IoT gateways, and edge devices that collect continuous or periodic data from field instrumentation.
- **Analytics Platform**: Software that processes sensor data, applies machine learning algorithms, identifies anomalies, and predicts failure patterns.
- **CMMS Integration**: Connection to Computerized Maintenance Management Systems to automatically generate work orders based on condition triggers.

Primary Use Cases

- **Pump Condition Monitoring**: Vibration analysis, bearing temperature, and motor current signature analysis detect bearing wear, impeller damage, cavitation, and alignment issues before catastrophic failure. This is critical since pumps are among the most failure-prone and energy-intensive assets.
- **Valve Health Assessment**: Acoustic monitoring and actuator torque measurement identify internal corrosion, seat wear, stem binding, and actuator degradation. Prevents unexpected valve failures that can cause water hammer or loss of system control.
- **Pipe Leak Detection and Burst Prevention**: Acoustic sensors, pressure transducers, and flow monitoring detect developing leaks before they become main breaks. Identifies anomalous flow patterns indicating pipe deterioration, reducing non-revenue water and emergency repairs.
- **Motor and VFD Monitoring:** Current and voltage monitoring, thermal imaging, and vibration analysis on motors and variable frequency drives predict winding failures, bearing issues, and power quality problems. Prevents unplanned outages of critical equipment.
- **Tank and Reservoir Integrity**: Level sensors, structural monitoring, and cathodic protection monitoring detect corrosion, structural degradation, and coating failures before catastrophic loss of storage capacity.
- **Treatment Process Optimization:** Monitoring membrane differential pressure, filter turbidity breakthrough, chemical feed pump performance, and UV lamp intensity ensures treatment efficacy while maximizing asset life.
- **Chlorine Residual Monitoring**: Continuous monitoring throughout the distribution system ensures water quality compliance and identifies areas where re-chlorination or system flushing is needed.
- **SCADA System Health**: Monitoring communication quality, RTU battery health, and PLC processor utilization prevents telemetry failures and loss of remote control.

Implementation Approach

- **Asset Criticality Assessment**: Prioritize CBM deployment on high-consequence assets where failure would cause service disruption, regulatory violations, safety hazards, or significant economic loss.
- **Baseline Establishment**: Collect data under normal operating conditions to establish performance baselines and define alarm thresholds.
- **Predictive Models**: Develop algorithms that correlate sensor data with failure modes, often using historical failure data to train machine learning models.
- **Alert Management**: Configure tiered alerts (advisory, warning, critical) to avoid alarm fatigue while ensuring actionable notifications reach appropriate personnel.

Benefits

- **Reduced Downtime**: 30-50% reduction in unplanned outages by addressing issues before failure occurs. Critical for maintaining continuous water service.
- **Extended Asset Life**: Optimized maintenance timing prevents both premature replacement and operation-to-failure, extending equipment lifespan by 20-30%.
- **Lower Maintenance Costs**: 25-35% reduction in maintenance expenses by eliminating unnecessary preventive maintenance and reducing emergency repair premiums.
- **Energy Efficiency**: Early detection of pump inefficiency, motor issues, and system losses reduces energy consumption by 10-20%.
- **Regulatory Compliance**: Proactive monitoring ensures treatment processes and distribution system meet water quality standards, avoiding violations and public health risks.
- **Labor Optimization**: Maintenance crews focus on actual needs rather than routine inspections, improving workforce productivity.
- **Non-Revenue Water Reduction:** Early leak detection recovers 5-15% of water losses, directly impacting revenue and conservation goals.

Technology Enablers

- **Wireless Sensor Networks**: Low-power, long-range wireless (LoRaWAN, cellular IoT) enables cost-effective monitoring of remote assets without extensive cabling.
- **Edge Computing**: On-site processing reduces data transmission costs and enables real-time decisions even with intermittent connectivity.
- **Cloud Analytics**: Scalable platforms process data from thousands of assets, apply machine learning, and provide dashboards accessible to distributed teams.
- **Digital Twins**: Virtual models of physical assets enable simulation of failure scenarios and optimization of maintenance strategies.

Challenges

- **Initial Investment**: Sensor deployment, software platforms, and integration require significant capital outlay, though ROI typically achieved within 2-3 years.
- **Data Quality**: Sensor calibration, communication reliability, and data validation are critical to avoid false alarms and maintain trust in the system.
- **Skills Gap**: Maintenance staff need training in data interpretation and predictive analytics alongside traditional mechanical/electrical skills.

- **Cybersecurity**: Connected sensors and remote monitoring expand the attack surface, requiring robust security protocols.
- **Legacy Infrastructure**: Older equipment may lack monitoring points or require retrofitting to enable condition monitoring.

Practical Example

Booster pump bearing degradation detected early.

A water utility installs vibration sensors on critical booster pump stations. The system detects increasing vibration amplitude and changing frequency patterns indicating bearing degradation. An alert is generated three weeks before predicted failure.

Maintenance is scheduled during a planned low-demand period, replacement bearings are ordered, and the repair is completed without service disruption. This avoids a midnight emergency callout, prevents secondary damage to the motor and coupling, and maintains system reliability.

Industry Trends

Water utilities are increasingly adopting CBM as aging infrastructure, workforce retirements, and budget constraints make reactive maintenance unsustainable.

Integration with asset management systems enables data-driven capital planning, while regulatory pressure for water quality and conservation makes predictive capabilities essential.

The shift to CBM represents a cultural change from " maintaining what's scheduled" to " maintaining what's needed," requiring organizational commitment alongside technology deployment.

Flood Monitoring

Flood monitoring systems provide real-time surveillance of water levels, rainfall, and environmental conditions to predict, detect, and respond to flooding events.

For water utilities, this is critical for protecting infrastructure, ensuring operational continuity, preventing contamination, and fulfilling public safety responsibilities.

Core Components

- **Level Sensors**: Ultrasonic, radar, pressure transducers, and float switches installed in rivers, streams, stormwater systems, treatment basins, and wet wells to monitor water levels continuously.
- **Rain Gauges**: Tipping bucket or weighing rain gauges positioned throughout the service area to measure precipitation intensity and accumulation.
- **Weather Stations**: Monitor temperature, humidity, barometric pressure, and wind to support predictive models and correlate with rainfall events.
- **Flow Meters:** Measure discharge rates in channels, culverts, and pipes to detect abnormal flows indicating flooding or system overload.
- **CCTV and Visual Monitoring**: Cameras at critical locations provide visual confirmation of flood conditions and infrastructure status.
- **Communication Infrastructure**: Telemetry systems (cellular, satellite, radio) transmit data from remote monitoring sites to central control systems, often in areas without reliable power or connectivity.
- **Analytics and Alerting Platform**: Software that processes sensor data, applies hydrological models, generates flood forecasts, and triggers automated alerts and response protocols.

Primary Use Cases

Infrastructure Protection

- **Treatment Plant Flood Defense**: Monitor water levels around treatment facilities to activate flood barriers, pumps, or shutdown procedures before floodwaters can damage electrical systems, disrupt treatment processes, or cause contamination.
- **Pump Station Security**: Real-time monitoring of wet well levels and surrounding water bodies prevents flooding of pump stations, which are often located in low-lying areas near water sources. Enables remote shutdown or activation of emergency pumps.
- **Wellfield Protection:** Monitor groundwater levels and surface water near wellfields to prevent contamination from floodwaters carrying pollutants, sewage, or agricultural runoff into drinking water sources.
- **Dam and Reservoir Management**: Track reservoir levels, inflow rates, and weather forecasts to optimize controlled releases, prevent overtopping, and maintain safe operating levels during storm events.

Operational Response

- **Combined Sewer Overflow (CSO) Management**: Monitor stormwater inflows to combined sewer systems and predict when capacity will be exceeded. Activates CSO diversion, alerts operators, and documents overflow events for regulatory reporting.
- **Wastewater Treatment Bypass Prevention**: Track influent flows during wet weather to prevent treatment plant overload. Enables equalization basin management and process adjustments to maintain treatment efficiency.
- **Distribution System Integrity**: Monitor manholes, valve vaults, and low-lying infrastructure for flooding that could allow contamination to enter the water distribution system, triggering water quality alerts.
- **Emergency Water Supply**: Identify when flooding threatens primary water sources or treatment capacity, enabling activation of alternate supplies, interconnections, or emergency treatment protocols.

Public Safety and Communication

- **Early Warning Systems**: Integrate utility flood data with municipal emergency management to provide early warnings to residents in flood-prone areas, supporting evacuation decisions and emergency response.
- **Road Closure Coordination**: Share real-time flood data with transportation departments to inform road closure decisions, especially where utility infrastructure (manholes, hydrants) may be submerged or compromised.
- **Water Quality Alerts**: Detect conditions where flooding may compromise water quality (surface water intrusion, cross-connections, treatment disruption) and issue boil water advisories or other public notices.

Asset Management and Planning

- **Floodplain Risk Assessment**: Historical flood data informs infrastructure siting decisions, identifies vulnerable assets requiring hardening or relocation, and supports climate adaptation planning.
- **Insurance and Resilience**: Documented flood monitoring data supports insurance claims, FEMA coordination, and funding applications for flood mitigation projects.

- **Stormwater System Capacity**: Monitor performance of drainage infrastructure during storm events to identify undersized systems, blockages, or areas requiring expansion to handle increasing precipitation intensity.

Technology Implementation

- **Sensor Networks**: Deploy distributed networks of low-cost, battery-powered sensors across watersheds, particularly in areas upstream of critical infrastructure to provide maximum lead time for flood warnings.
- **Predictive Modeling**: Integrate real-time rainfall and level data with hydrological models (HEC-HMS, SWMM) to forecast flood arrival times, peak levels, and duration hours or days in advance.
- **GIS Integration**: Map flood sensor data with infrastructure locations, elevation data, and flood zones to visualize risk and prioritize response actions spatially.
- **Mobile Accessibility**: Field crews access real-time flood data via mobile apps to assess conditions safely and coordinate response activities without returning to operations centers.
- **Automated Controls**: Trigger automated responses such as closing flood gates, starting emergency pumps, shutting down vulnerable equipment, or diverting flows based on pre-programmed thresholds.

Benefits

- **Infrastructure Resilience**: Prevent millions of dollars in flood damage to treatment plants, pump stations, and other critical assets through early detection and proactive protective measures.
- **Service Continuity**: Maintain water and wastewater services during and after flood events by protecting key infrastructure and implementing contingency plans before systems are compromised.
- **Regulatory Compliance**: Document CSO events, treatment bypasses, and water quality impacts as required by EPA and state regulations. Demonstrate due diligence in flood response.
- **Public Health Protection**: Prevent waterborne disease outbreaks by detecting contamination risks early and implementing appropriate water quality safeguards.
- **Emergency Response Coordination**: Provide situational awareness to utility operators and municipal emergency managers, enabling coordinated response and resource allocation.
- **Climate Adaptation**: Historical flood data and trend analysis inform long-term infrastructure investments and adaptation strategies as precipitation patterns change.
- **Operational Efficiency**: Reduce emergency response costs by transitioning from reactive flood fighting to planned, measured responses with adequate lead time.

Practical Example

A water utility operates a treatment plant adjacent to a river. Upstream rainfall sensors detect intense precipitation, and river level gauges show rapidly rising water. The flood monitoring system predicts the river will exceed flood stage at the plant in 6 hours.

Operators receive automated alerts and implement their flood response plan: deploy temporary flood barriers around electrical equipment, transfer operations to a backup control room, stage additional pumps, and notify mutual aid partners.

The flood arrives as predicted, but treatment continues uninterrupted because protective measures were in place.

Without monitoring, the flood would have arrived undetected during night hours, potentially causing catastrophic damage and service disruption.

Integration with Broader Systems

- **Weather Services**: Integrate with National Weather Service forecasts, NOAA precipitation data, and commercial weather services for enhanced predictive capability.
- **SCADA Systems**: Flood monitoring data feeds into existing SCADA platforms, providing operators with comprehensive situational awareness alongside normal operational parameters.
- **Emergency Management:** Share flood data with county/municipal emergency operations centers, supporting community-wide disaster response coordination.
- **Smart City Platforms**: Contribute flood data to broader urban monitoring systems that integrate transportation, utilities, and public safety information.

Water Quality Monitoring

Water quality monitoring is a critical operational function for water utilities. It involves continuous surveillance, measurement, and analysis of physical, chemical, and biological parameters throughout the water distribution system to ensure safe drinking water delivery to consumers and regulatory compliance.

Business Context

Water utilities are responsible for providing potable water that meets stringent health and safety standards defined by regulatory bodies such as the EPA (Environmental Protection Agency) or equivalent national authorities. Real-time and periodic monitoring enables utilities to detect contamination events, optimize treatment processes, maintain system integrity, and respond proactively to quality degradation before it affects public health.

Key Monitoring Points

The monitoring process spans multiple stages of the water lifecycle: raw water sources (rivers, lakes, groundwater), treatment plant intake and output, distribution networks including storage reservoirs and pumping stations, and customer endpoints. Each point requires different monitoring strategies and parameters based on risk assessment and regulatory requirements.

Technical Parameters

Utilities monitor a comprehensive range of water quality parameters:

- pH levels
- turbidity
- chlorine residuals (free and total)
- dissolved oxygen
- temperature
- conductivity
- total dissolved solids (TDS)
- specific contaminants including heavy metals, organic compounds, pathogens, and emerging contaminants such as pharmaceuticals or microplastics

Advanced monitoring may include microbiological testing for E. coli, total coliforms, and other indicator organisms.

Monitoring Technologies

Modern water utilities employ a combination of manual sampling with laboratory analysis and automated sensor networks connected through SCADA (Supervisory Control and Data Acquisition) systems.

Online analyzers provide continuous real-time data, while grab samples support detailed laboratory testing for parameters that cannot be measured in-situ.

Recent innovations include:

- IoT-enabled smart sensors
- wireless sensor networks
- mobile monitoring units

Data Management and Analytics

Monitoring generates substantial data volumes requiring robust data management infrastructure.

Utilities use specialized software platforms to:

- aggregate monitoring data
- validate data
- analyze data
- generate alerts when parameters exceed threshold values

Advanced analytics, including machine learning models, help to:

- predict quality trends
- identify anomalies
- optimize treatment processes

Regulatory Compliance and Reporting

Water quality monitoring programs must satisfy regulatory reporting requirements, including:

- periodic compliance reports to environmental agencies
- public notification of violations
- consumer confidence reports

Documentation and audit trails are essential for demonstrating due diligence and regulatory adherence.

Operational Benefits

Effective monitoring enables utilities to:

- optimize chemical dosing
- reduce treatment costs
- extend infrastructure lifespan
- minimize water loss through early leak detection
- rapidly respond to contamination incidents

This proactive approach protects public health while improving operational efficiency and customer trust.

SCADA System Modernisation

SCADA (Supervisory Control and Data Acquisition) system modernisation upgrades legacy control and monitoring infrastructure to contemporary platforms that leverage:

- modern computing architectures
- enhanced cybersecurity frameworks
- advanced analytics capabilities
- improved human-machine interfaces

For water utilities, this transformation is essential to maintain operational reliability, meet evolving security requirements, and enable data-driven decision-making across treatment plants, pumping stations, and distribution networks.

Current State Challenges

Many water utilities operate aging SCADA systems that were implemented decades ago, often running on obsolete hardware with proprietary protocols, unsupported operating systems, and limited integration capabilities.

These legacy systems present significant challenges:

- difficulty sourcing replacement parts
- vulnerability to cyber threats due to outdated security architectures
- inability to scale with growing infrastructure demands
- limited remote access functionality
- poor interoperability with modern business systems such as asset management, GIS (Geographic Information Systems), and customer information platforms

Modernisation Architecture

Contemporary SCADA architectures adopt:

- standardized protocols like OPC UA (Open Platform Communications Unified Architecture)
- web-based visualization interfaces
- virtualized server infrastructure
- cloud-hybrid deployment models

The modernised system typically comprises:

- field instrumentation and RTUs (Remote Terminal Units) or PLCs (Programmable Logic Controllers)
- secure communication networks utilizing VPNs and encrypted protocols
- redundant SCADA master stations with high availability configurations
- historian databases for long-term data retention
- integrated analytics platforms supporting real-time and predictive insights

Cybersecurity Enhancements

Modernisation prioritizes cybersecurity through implementation of defense-in-depth strategies, including:

- network segmentation separating operational technology (OT) from information technology (IT) networks

- multi-factor authentication
- intrusion detection and prevention systems
- continuous vulnerability monitoring
- security information and event management (SIEM) platforms
- compliance with frameworks such as NIST Cybersecurity Framework or IEC 62443 standards

These measures protect critical water infrastructure from increasingly sophisticated cyber threats targeting industrial control systems.

Integration and Interoperability

Modern SCADA platforms enable seamless integration with enterprise systems including:

- computerized maintenance management systems (CMMS)
- hydraulic modeling software
- laboratory information management systems (LIMS)
- customer billing platforms
- advanced metering infrastructure (AMI)

This integration eliminates data silos, automates workflows, and provides comprehensive visibility across operational and business domains, enabling utilities to optimize performance holistically rather than managing isolated systems.

Advanced Operational Capabilities

Modernised SCADA systems incorporate advanced features such as:

- mobile access for field operators enabling remote monitoring and control
- predictive maintenance algorithms that analyze equipment performance trends to anticipate failures
- automated alarm rationalization reducing operator alert fatigue
- energy optimization modules that minimize pumping costs through intelligent scheduling
- digital twin capabilities allowing operators to simulate scenarios and optimize operational strategies without impacting live systems

Migration Strategy and Risk Management

Successful modernisation requires careful planning to minimize operational disruption. Utilities typically adopt:

- phased migration approaches with parallel operation of legacy and new systems during transition periods
- comprehensive factory acceptance testing (FAT) and site acceptance testing (SAT) protocols
- extensive operator training programs
- detailed rollback procedures
- thorough documentation of system configurations

Risk mitigation includes:

- maintaining redundancy throughout the migration

- scheduling critical transitions during low-demand periods
- establishing clear escalation procedures for addressing unexpected issues

Compliance and Standards

Modern SCADA implementations must comply with regulatory requirements:

- EPA water security guidelines.
- State-specific operational reporting mandates.
- Industry standards such as AWWA (American Water Works Association) recommendations for control system design.

The modernised system should facilitate automated compliance reporting, provide audit trails for regulatory reviews, and support documentation requirements for safety and environmental permits.

Business Benefits

SCADA system modernisation delivers substantial business value across operational, financial, and strategic dimensions.

Operationally, utilities achieve:

- Improved system reliability through reduced downtime.
- Enhanced situational awareness enabling faster response to anomalies.
- Optimized resource utilization resulting in lower energy consumption and chemical usage.

Financially, modernisation delivers:

- Reduced maintenance costs associated with obsolete equipment.
- Extended asset lifecycles through better condition monitoring.
- Improved operational efficiency translating to measurable cost savings typically ranging from 15-30% of operational expenses.

Strategically, modern SCADA platforms enable:

- Scalable infrastructure supporting IoT sensor integration, artificial intelligence applications, and advanced analytics capabilities.
- Enhanced cybersecurity posture that protects critical infrastructure while reducing risk exposure and potential regulatory penalties.
- Improved data quality and accessibility for better capital planning decisions, regulatory compliance demonstration, and customer service delivery.
- Transformation of SCADA from purely an operational control system into a strategic enterprise asset that drives continuous improvement, supports workforce development through intuitive interfaces, and ensures long-term sustainability of essential water services for communities.

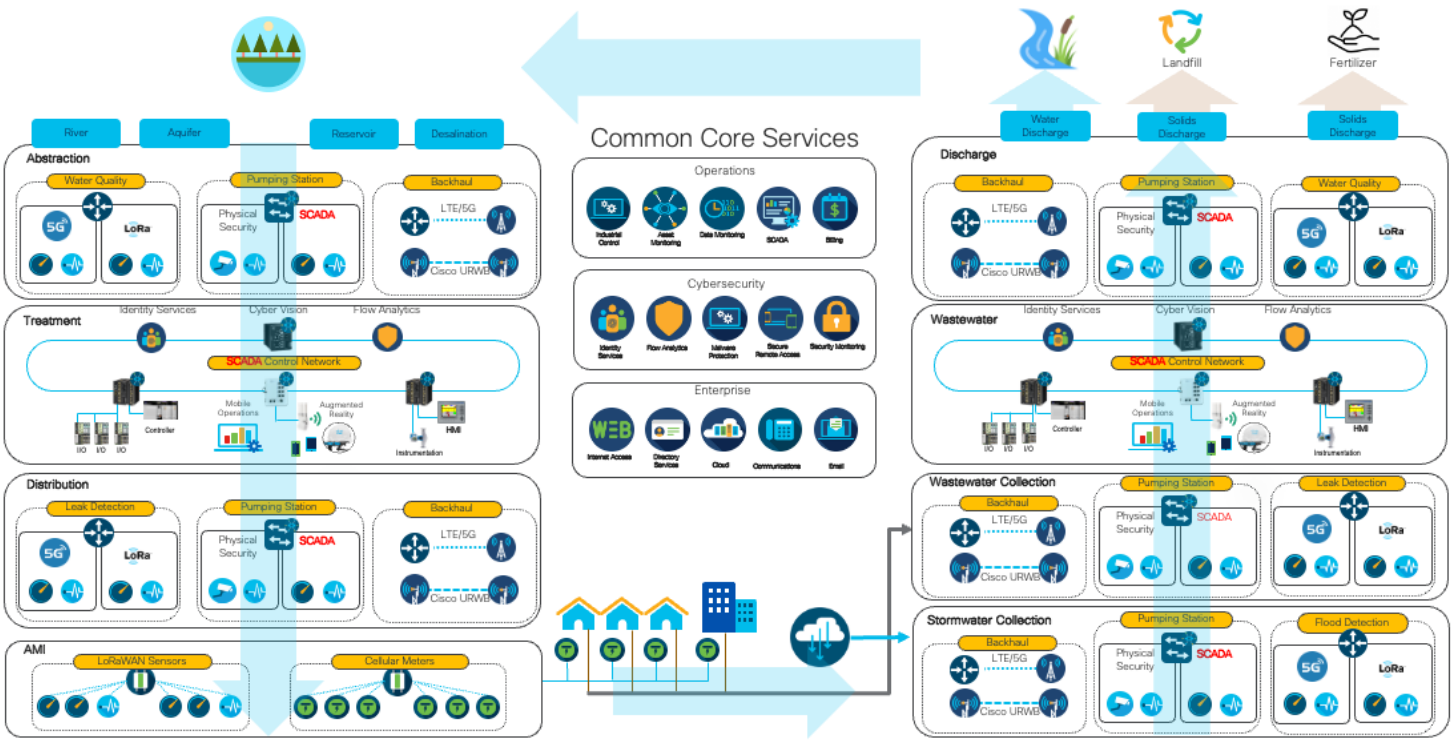
Architecture

This technical architecture document defines the enterprise-wide network and technology infrastructure design for water utilities leveraging Cisco's portfolio of networking, security, and IoT solutions.

The architecture provides a comprehensive blueprint for modernizing water utility operations by establishing secure, resilient, and scalable connectivity across geographically dispersed assets including treatment plants, pumping stations, reservoirs, distribution networks, and administrative facilities.

Architecture Framework

Figure 2. Architecture Framework



The document establishes a multi-layered architecture encompassing:

- The core data center hosting enterprise applications and SCADA master stations.
- Campus networks serving administrative buildings and treatment facilities.
- Wide area network (WAN) connectivity linking remote sites through MPLS, SD-WAN, or cellular technologies.
- Industrial networking at operational sites utilizing ruggedized switches and routers designed for harsh environments.

The architecture embraces Cisco's intent-based networking principles and zero-trust security model to ensure operational technology (OT) and information technology (IT) convergence while maintaining appropriate segmentation and access controls.

Key Technology Components

Cisco technology solutions specified:

- Industrial Ethernet switches (IE series) for field deployment in SCADA networks.
- Catalyst Enterprise and Industrial router platforms for branch connectivity.
- Catalyst switches for enterprise campus networks.
- Cisco Catalyst Center for network automation and assurance.
- SD-WAN infrastructure using Cisco SD-WAN technology for intelligent WAN optimization.
- Wireless solutions including outdoor access points for mobile workforce connectivity.
- Cisco Secure Firewall (formerly Firepower) for unified threat management.
- Industrial IoT-specific components include Cisco Industrial routers for cellular connectivity and for enabling edge computing at remote sites.

Security Architecture

Security framework:

- Network segmentation through VLANs and VRFs to isolate SCADA, business, and guest networks.
- identity services engine (ISE) for network access control and device profiling.
- Encrypted communications using MACsec for wired networks and WPA3 for wireless.
- Threat intelligence integration through Cisco Talos.
- Security monitoring via Splunk platform providing unified visibility across the security ecosystem.

The architecture addresses regulatory compliance requirements including NIST cybersecurity standards and critical infrastructure protection mandates.

Operational Benefits

High-level architecture outcomes:

- Unified network management that reduces operational complexity.
- Improved visibility across both IT and OT environments.
- Enhanced security posture protecting critical water infrastructure from cyber threats.
- Scalable infrastructure supporting future IoT sensor deployments and smart water initiatives.
- Standardized design patterns that accelerate deployment of new sites.
- Reduced total cost of ownership through automation and simplified troubleshooting.

The architecture positions utilities to leverage emerging technologies including artificial intelligence for network optimization, edge computing for local data processing, and cloud integration for advanced analytics while maintaining the reliability and security essential for critical infrastructure operations.

Network Engineering

The reference design splits the overall design into two main types (based on the architecture framework in the previous section):

- Plant-based networks consist primarily of switching-based networks with routers to connect to the WAN.
- Remote site or assets consist of small compact routers that provide routing and some switching capability in one platform. Additional compact switching products can be used to increase the port count or area coverage as needed.

On top of these architectures, we can overlay other capabilities as required. Technologies such as WIFI can be added as necessary to the underlaying network.

Wide Area Network

The WAN provides the connectivity between sites and the enterprise locations.

The WAN needs to be flexible and be able to cope with multiple underlay technologies, such as:

- Cellular
- Fiber
- Leased line
- MPLS
- Satellite networks

It also must provide a security capability to enable the Utility to engineer suitable security policies for each site centrally and deploy them to the routers at the network edge.

Software-Defined Wide Area Networking (SD-WAN) represents a transformative approach to enterprise connectivity that addresses the limitations of traditional WAN architectures.

By abstracting network control from the underlying hardware and centralizing management through software-based policies, SD-WAN enables organizations to achieve greater agility, improved application performance, and reduced operational complexity.

This technology leverages multiple transport services—including MPLS, broadband internet, LTE, and 5G—to create resilient, cost-effective connections between distributed sites while providing real-time visibility and granular control over traffic routing.

As businesses increasingly adopt cloud services and require reliable connectivity for remote locations, SD-WAN has emerged as a critical infrastructure component that delivers enhanced security, optimized bandwidth utilization, and simplified network operations at scale.

Cisco Software-Defined Wide Area Network (SD-WAN) is an advanced, intent-based networking solution that simplifies the management and operation of a WAN by decoupling the networking hardware from its control mechanism.

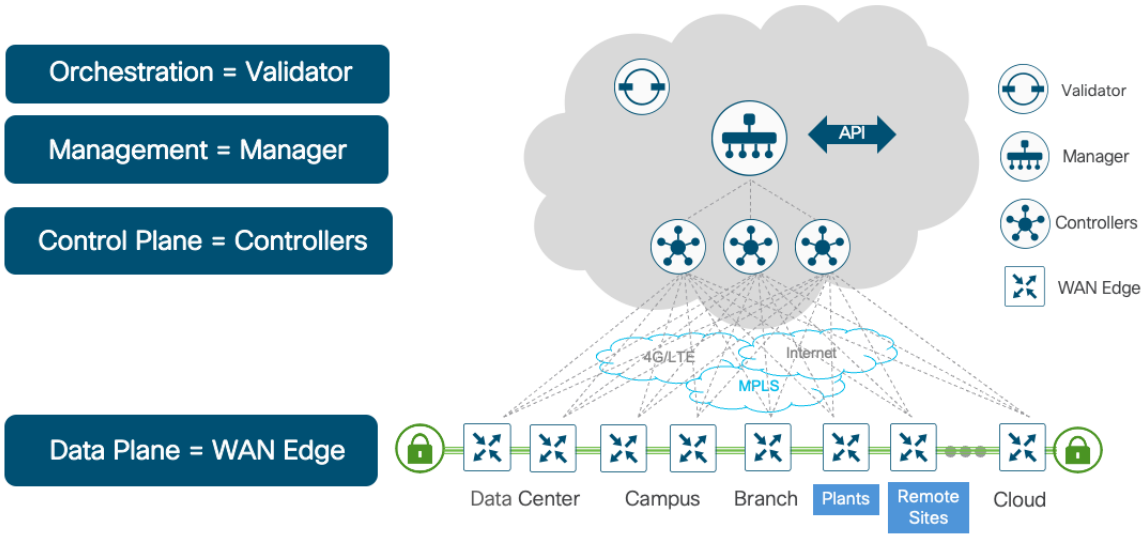
Built on the principles of software-defined networking (SDN), Cisco SD-WAN provides secure connectivity that optimizes application performance and improves user experience across distributed operational environments.

The Cisco SD-WAN solution enables organizations to:

Increase agility by deploying and managing WAN services centrally through a single orchestrator.
Enhance security with end-to-end encryption, segmentation, and integrated threat defence.
Improve performance through intelligent path selection and application-aware routing.
Simplify operations via centralized policy, automation, and analytics.

The SD-WAN architecture consists of four key centralised components:

Figure 3. Wide Area Network



Controllers: The centralized brain of the network, responsible for control-plane policies and routing decisions.
WAN Manager: A web-based interface for configuration, monitoring, and lifecycle management.
Validator: The initial authentication and orchestration gateway that facilitates secure connectivity between components.
WAN Edge Routers (Cisco IOS-XE Routers): The data-plane devices deployed at remote site, branch, data centre, or cloud locations.

SD-WAN Security

Cisco SD-WAN delivers enterprise-grade security through an integrated, multi-layered approach that extends protection across the entire distributed network fabric. The platform embeds advanced security functions directly into the WAN edge, including next-generation firewall capabilities, intrusion prevention systems (IPS), URL filtering, DNS-layer security, and advanced malware protection through integration with Cisco Umbrella and Threat Grid.

It incorporates secure connectivity through encrypted IPsec tunnels and enforces segmentation policies at every node.

Cisco SD-WAN ensures that traffic remains protected whether traversing public internet, private MPLS, or cellular networks. The architecture's unified policy framework enables consistent security posture enforcement across all locations while providing centralized visibility and threat intelligence correlation.

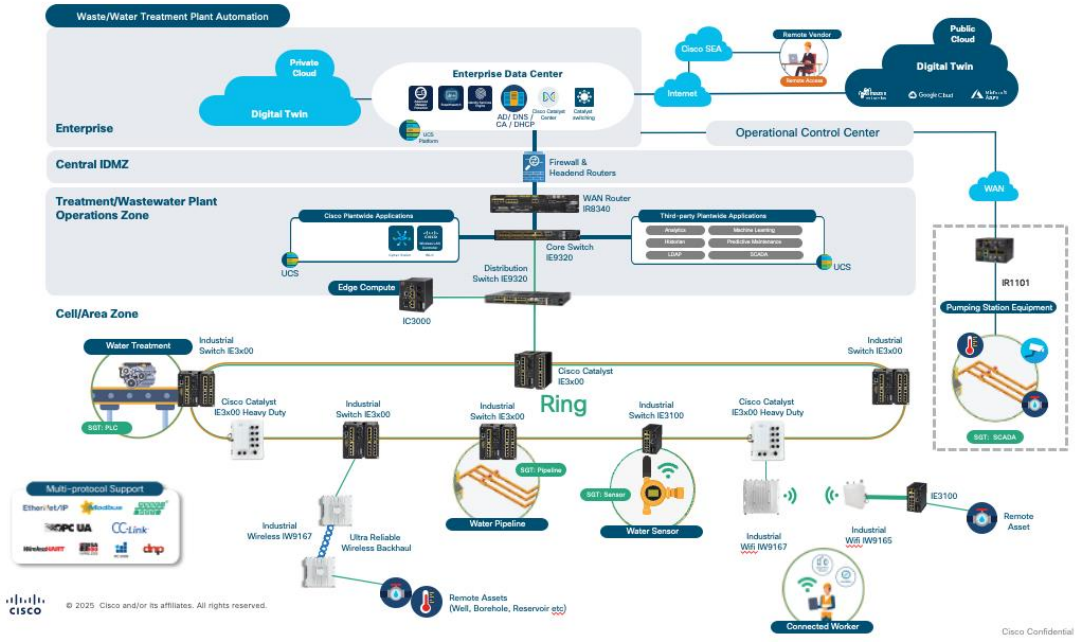
This approach reduces the attack surface and eliminates the need to backhaul branch traffic through centralized security inspection points. It not only strengthens security but also improves application performance and reduces costs by enabling direct internet breakout with full security stack protection at

the remote site or plant level, making it particularly valuable for organizations embracing cloud-first strategies and zero-trust network architectures.

Figure 4. SD-WAN Security

Plant Based Networks

Figure 5. Plant Based Networks



Shown below is the Plant based network design. Encompassing Industrial ethernet switches in ring topologies for connecting various areas of the Treatment or wastewater plants. Rings provide the most

cost effective and efficient way to connect multiple switches in different locations while providing a resilient capability in the event of a failure on the ring (switch or fiber failure).

Ring-Based Solutions

Industrial plant rings often combine standardized Ethernet redundancy with Cisco-optimized segments. Two complementary technologies are REP (Cisco Resilient Ethernet Protocol) and MRP (Media Redundancy Protocol, IEC 62439-2).

Cisco REP (Resilient Ethernet Protocol)

REP is a Cisco Layer 2 ring protocol designed for Industrial Ethernet deployments where spanning-tree-based loops are undesirable.

It organizes the ring into contiguous segments, each with two edge ports that coordinate blocking on a single logical link so that only one alternate path is blocked at any time. Control messages propagate along the segment so that failures can be isolated and connectivity restored quickly—typically sub-second to a few seconds, depending on ring size, timers, and configuration.

REP fits water and wastewater plants that standardize on Cisco IE switches end-to-end: it integrates with familiar IOS configuration, supports VLAN-aware operation where designed into the deployment, and avoids the indirect root-bridge behavior that can make pure STP harder to predict on large rings.

It is well suited to plant rings carrying SCADA, I/O, and IP camera traffic where operations teams want a Cisco-native tool chain, diagnostics, and consistent behavior across the IE portfolio.

MRP (Media Redundancy Protocol, IEC 62439-2)

MRP is an IEC-standard ring protocol used widely in industrial automation. A Media Redundancy Manager (MRM) blocks one port to break the loop under normal conditions, while Media Redundancy Clients (MRC) forward frames on the ring. When a link or device fails, the MRM recomputes the topology and opens the blocked path so that communication recovers according to IEC 62439-2 timing and semantics.

MRP is the default choice when the ring must include multi-vendor automation equipment (PLCs, RTUs, drives, remote I/O) that ships with IEC-compliant MRP rather than Cisco-proprietary protocols. It supports interoperability in brownfield sites and when substation-style or process-control gear must sit on the same resilient ring model as the network design documentation.

Advantages of using both REP and MRP

Using REP and MRP together (typically on separate rings or at controlled interconnection points, not stacked blindly on the same logical ring) gives water utilities several practical benefits:

- Interoperability where it matters: Run MRP on segments that must attach non-Cisco IEC devices, and REP on homogeneous Cisco IE rings for optimized convergence and operational consistency.
- Clear operational boundaries: Each protocol's failure domain and tuning (timers, roles, monitoring) stay scoped to its ring, which simplifies troubleshooting and change control in large treatment or distribution sites.
- Migration and expansion: New Cisco plant infrastructure can use REP, while legacy or vendor-locked islands remain on MRP, with layer-3 or carefully designed L2 boundaries between them as appropriate to the overall architecture.
- Predictable redundancy models: Operators can standardize "IEC ring vs Cisco REP ring" in design guidelines, training, and as-built documentation instead of mixing STP-only designs with ad hoc loops.

Design note: REP and MRP address the same general problem—resilient ring Ethernet—with different standardization and vendor scope. Follow Cisco and IEC design guides for ring size, dual-homing, and never interconnecting incompatible ring protocols on a single loop without explicit translation or routing between domains.

Wireless Access

URWB Connectivity

Cisco Ultra-Reliable Wireless Backhaul (URWB) provides a licensed-exempt, 802.11-based mesh suited to water utilities that must reach assets where fiber, leased line, or trenched copper is impractical, uneconomic, or delayed by planning constraints. URWB is engineered for mission-critical OT backhaul: sub-second convergence, low and predictable latency, and seamless mobility across mesh hops—characteristics that distinguish it from best-effort Wi-Fi used for laptops or guest access. In this solution, URWB extends the plant or enterprise L2/L3 domain to geographically dispersed pumping stations, boreholes, wells, reservoirs, and dam instrumentation without treating each site as an isolated island of connectivity.

The three primary deployment patterns below share a common goal: deliver deterministic OT backhaul to hard-to-connect locations while preserving the security, segmentation, and visibility models described elsewhere in this document.

Remote site asset connectivity (hard-to-connect assets)

Many water utility assets sit in greenfield, agricultural, floodplain, or conservation land where civil works for ducting are prohibited, seasonal, or cost-prohibitive. Examples include isolated booster sets, chlorination or dosing skids, flow and pressure monitoring cabinets, remote I/O, and small RTU/PLC installations that must report to a treatment works or operations center SCADA but cannot justify a dedicated WAN circuit per site.

URWB addresses these hard-to-connect locations by forming a multi-hop wireless fabric from a known anchor point (typically the treatment plant, a major pumping station with fiber, or a hill-top aggregation site) outward to Mesh Points (MPs) at each remote asset. Each MP presents Ethernet attachment for one or more OT devices, allowing utilities to standardize on IP-based SCADA (DNP3, Modbus/TCP, IEC protocols) without maintaining parallel serial radio networks for every outstation.

Design considerations for this pattern include:

- Line-of-sight and path planning — URWB performance depends on RF survey, antenna height, and clearance from vegetation, structures, and seasonal foliage; utilities should plan redundant mesh paths where a single hop failure would otherwise isolate a critical pump or quality monitor.
- Power and enclosure — Remote MPs are often co-located with existing MCC or kiosk power; battery-backed or solar sites require explicit uptime targets aligned with SCADA polling and alarm latency.
- Operational ownership — OT networking teams should own SSID/mesh policy, VLAN assignment, and change control alongside radio maintenance, so mesh tuning does not become an ad hoc field adjustment.

Pumps, boreholes, wells, and reservoir or dam equipment

Water utilities operate a long tail of distributed hydraulic assets that rarely have carrier-grade connectivity today:

Table 1. Remote site assets and connectivity requirements

Asset type	Typical connectivity need	URWB role
Boreholes and wells	Level, flow, pump run status, power quality, and sometimes source protection instrumentation	Mesh MP at the wellhead cabinet backhauls RTU/PLC traffic to the wellfield or treatment plant network
Pumping stations	SCADA control, VFD and motor data, leak and pressure monitoring, CCTV where deployed	Primary or diverse backhaul when fiber exists only to a parent site; supports lift-station rings of multiple MPs
Reservoirs and dams	Level, gate/actuator status, structural or environmental sensors, flood coordination telemetry	Extends plant network across large water bodies and embankments where trenching around the perimeter is not feasible
Storage tanks and towers	Level, mixer, cathodic protection, and quality sampling at the asset	Short-hop mesh from a nearby wired site or elevated Mesh End with clear line of sight

For these assets, URWB bridges the gap between “no connectivity” and full SD-WAN or fiber deployment. Traffic from pumps and instruments lands on the same OT VLAN or VRF design as the parent treatment or distribution site, so SCADA masters, historians, and Cyber Vision (where enabled on Industrial Ethernet aggregation) see remote outstations as first-class IP endpoints rather than as opaque serial radios. Where regulatory or flood-response programs require faster telemetry during storm events, mesh parameters and polling intervals should be validated under worst-case RF conditions, not only under clear-weather baseline surveys.

Backhaul for remote networking assets (switches and Wi-Fi access points)

URWB is not limited to attaching a single PLC at each remote location. A common pattern is to use the mesh as wireless backhaul for a small remote network stack:

- Industrial Ethernet switches (for example Catalyst IE platforms) at a pumping station or wellfield, forming a local REP or MRP ring or star of I/O, drives, and analyzers, with one MP providing the uplink into the URWB fabric.
- Outdoor Wi-Fi access points for maintenance crew mobility, temporary contractor access, or OT client bridging (see Wi-Fi Connectivity below), with the AP’s upstream Ethernet homed to an MP or to a switch whose uplink is the MP.

In this model, URWB carries aggregated site traffic—SCADA, voice, video, and segmented user Wi-Fi—while policy enforcement remains at the plant edge router or firewall (for example IR1101, Secure Firewall, or SD-WAN edge). Utilities should not flatten trust zones across the mesh: assign OT instrumentation, surveillance, and corporate Wi-Fi to distinct VLANs at the remote switch and enforce north-south inspection when traffic leaves the mesh into the operations center.

Benefits of URWB as network backhaul (versus per-device cellular modems) include consistent IP addressing, simplified firewall rules, centralized monitoring of the wireless path, and lower recurring carrier cost when many endpoints share one mesh attachment point.

Reference architecture and roles

The diagrams in this section illustrate a typical plant-anchored mesh that extends Layer 2 connectivity to remote assets.

Topology principles:

- URWB is used to extend the plant network to remote assets that have no direct fixed connectivity (fiber, copper, or dedicated WAN).
- Boreholes, pumping stations, and reservoir/dam assets that must appear on the same logical network as the treatment or operations site are reached via Mesh Points along one or more hops.
- All URWB radios participating in a given extended site design operate within a single L2 domain (or a controlled extension thereof), so SCADA, engineering workstations, and ISE profiling behave predictably; inter-site routing beyond the mesh should use explicit L3 boundaries and firewall zones where the utility's security model requires it.

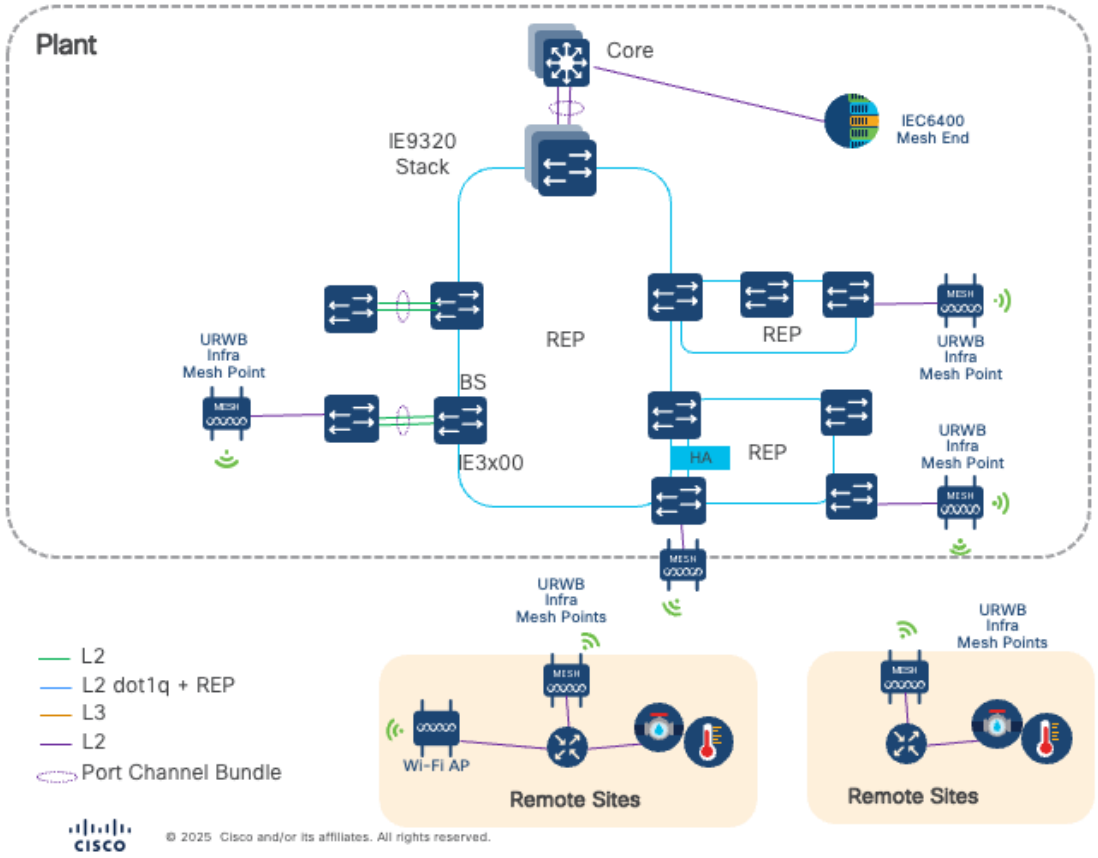
Device roles

Table 2. Roles and functions of devices

Role	Typical platform	Function
Mesh End (ME)	Catalyst IW9167E or IEC6400 (per validated design)	Anchors the mesh to the wired plant core—attached to Industrial Ethernet or aggregation switching at the treatment works or hub site
Mesh Point (MP)	Catalyst IW9167E at remote sites	Provides Infrastructure mode mesh relay and Ethernet downlink for RTU/PLC, IE switch, or outdoor AP
Downstream OT	IE switch, IR1101, RTU, PLC, sensors	Terminates on MP or remote switch; inherits VLAN and zone policy from the wired design

At the anchor site, one or more IW9167E or IEC6400 units are configured as Mesh End (ME) and connected to the plant core (for example IE ring uplink or distribution switch). At each remote asset, IW9167E radios operate as Mesh Points (MPs) in Infrastructure mode, extending connectivity over successive hops until the ME is reached.

Figure 6. Reference architecture and roles



At the anchor site, one or more IW9167E or IEC6400 units are configured as Mesh End (ME) and connected to the plant core (for example IE ring uplink or distribution switch).

At each remote asset, IW9167E radios operate as Mesh Points (MPs) in Infrastructure mode, extending connectivity over successive hops until the ME is reached.

Implementation notes:

- Size the mesh for hop count, throughput, and latency required by the most demanding application on the path (for example teleprotection-style traffic is rarely needed, but sub-second SCADA and IP camera streams may be).
- Coordinate URWB with WAN design: where a remote site later receives fiber or SD-WAN, the MP can remain as diverse backhaul or be redeployed to the next unserved asset.
- Align with cybersecurity architecture: treat the mesh as a conduit into an OT zone; enable embedded Cyber Vision on IE switches at aggregation points where east-west visibility is required, and restrict remote access (for example Secure Equipment Access) to approved assets behind the same segmentation model used for wired sites.

Wi-Fi Connectivity

Wi-Fi is used in two distinct patterns in water utility networks: field and plant worker access to IT and enterprise applications, and wireless attachment of OT assets where running fiber or copper is impractical.

Both require disciplined design, so convenience does not erode the security posture of SCADA and plant zones.

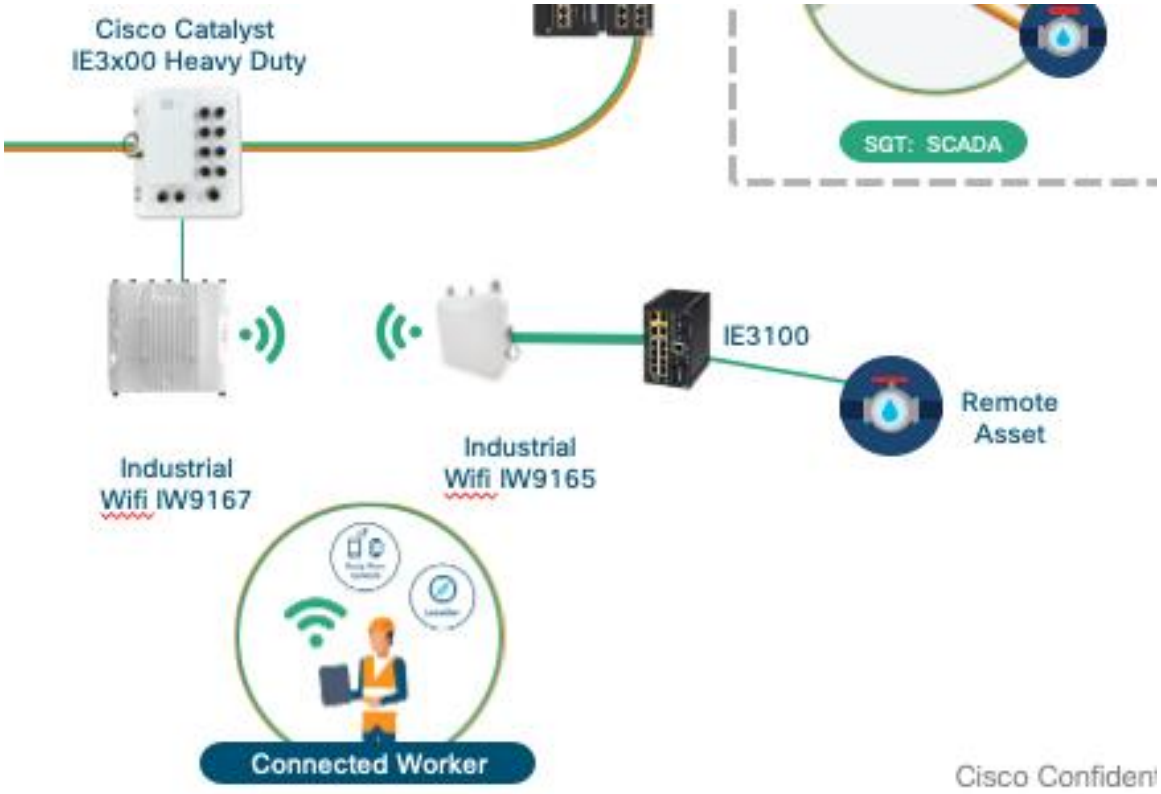
Worker mobility and enterprise access

Maintenance crews, operators, and contractors often need mobility across treatment works, pumping stations, and remote sites while using corporate applications (work orders, CMMS, email, collaboration, asset databases) and voice or video for coordination. Access points on plant or campus infrastructure should treat these clients as user devices on the IT plane: authenticate users and devices (for example via 802.1X and WPA3-Enterprise), assign them to user-oriented VLANs or VNs, and enforce policy through Cisco Identity Services Engine (ISE) with SGTs where the design uses Software-Defined Access or firewall integration. Prefer dedicated SSIDs (for example `CORP-WIFI` or role-based SSIDs) that map to centralized policy rather than a single shared PSK for all staff.

OT asset connectivity

At boreholes, wells, lift stations, and distributed pumps, industrial Wi-Fi or outdoor APs can backhaul sensor, PLC, or RTU traffic where URWB or wired Ethernet is not used end-to-end. These clients are infrastructure devices, not laptops: they should land on OT-scoped VLANs, reach only the SCADA concentrators, historians, or jump hosts required for their function, and avoid direct exposure to the internet or general corporate subnets. Use device identity (802.1X with certificates or MACSec-capable designs where supported, MAC allow lists only as a fallback with compensating monitoring) so rogue or cloned devices cannot easily join the OT SSID.

Figure 7. Wi-Fi Connectivity



Segregating traffic

Separate SSID and VLAN (or policy domain) per trust class—for example distinct SSIDs or at minimum distinct forwarded VLANs for *operations staff*, *contractors/guest*, and *OT instrumentation*. At the plant edge, route between VLANs through a firewall or OT-aware gateway (for example Cisco Secure Firewall, an industrial security appliance, or zone-based rules on the router), not through flat Layer 2 bridging between IT and OT. Use VXLAN/VRF segmentation or macro/micro segmentation with SGTs so that a compromised Wi-Fi client cannot pivot laterally into I/O or PLC subnets. Place Wi-Fi management interfaces on management VLANs isolated from production OT traffic.

Cybersecurity practices

Enforce WPA3 (or WPA2-Enterprise minimum with a migration plan), disable weak legacy Wi-Fi rates where policy allows, and disable unnecessary broadcast features that expand attack surface. Integrate wireless with ISE for posture, profiling, and guest/contractor flows with time-limited access. Log association, authentication, and anomalies (for example Splunk or the same SIEM used for the rest of the utility). For remote sites, centralize SSID and policy definition where possible so local misconfiguration does not open a back door. Align with IEC 62443 zones and conduits: treat wireless as a conduit that terminates in a controlled zone with explicit inspection and monitoring (for example Stealthwatch or Cyber Vision at the aggregation point) rather than blending OT and enterprise traffic in one flat broadcast domain.

Remote Assets

Remote water supply assets—boreholes, wells, booster and transfer pumping stations, reservoir and dam outstations, chlorination skids, and small RTU/PLC cabinets—share the same cybersecurity expectations as treatment plants, but often ship with minimal documentation, no on-site security staff, and heterogeneous vendor equipment installed over many years. The network design patterns in this section (URWB backhaul, IR1101 aggregation, optional Industrial Ethernet at the site) must therefore pair connectivity with visibility (know what is present and how it communicates) and segmentation (limit blast radius when a device or account is compromised).

Two complementary focus areas apply at these sites: visibility for discovery, baseline, and threat detection; and segmentation to enforce zones and conduits consistent with IEC 62443 and utility NIS2-style governance. The subsections below address the visibility-first remote site model; data analytics, edge compute, and remote access via IR1101 and Secure Equipment Access (SEA) are covered in the following subsection.

Visibility focus

Visibility at remote sites answers questions that paper asset registers rarely keep current: which PLCs, RTUs, drives, analyzers, and engineering laptops are on the local subnet, which protocols they use (for example Modbus/TCP, DNP3, Ethernet/IP), and whether observed traffic matches the approved SCADA architecture. For dispersed potable water supply assets, gaps in visibility delay incident response, weaken patch and firmware prioritization, and undermine segmentation projects because firewall rules are written against incomplete inventories.

A practical visibility program for remote sites should target:

- Asset inventory and context — Vendor, product family, firmware indicators, and logical role (for example lift-station PLC, borehole RTU, chlorine analyzer gateway) tied where possible to GIS/CMMS asset IDs.
- Communication graph — Who initiates sessions to whom (master–outstation, HMI–PLC, peer-to-peer I/O) to validate intended conduits and detect rogue masters or scanning.

- North-south and east-west coverage — Understanding both WAN-bound flows (toward operations centers, historians, cloud services) and lateral flows within the remote cabinet or small ring (PLC to I/O, drive to PLC, local HMI).
- Integration with enterprise security — Export of OT context to ISE, Secure Firewall, SIEM (for example Splunk), and Cyber Vision Center so remote-site events are not siloed from plant and IT monitoring.

Remote site water supply asset visibility using Cyber Vision

Cisco Cyber Vision is the recommended OT visibility and threat-detection layer for water utilities extending the architecture described in the Cybersecurity Architecture section of this document. At remote water supply sites, Cyber Vision sensors observe industrial traffic passively and forward metadata to Cyber Vision Center for asset discovery, protocol parsing, baselining, and anomaly indicators—without inserting an inline bump in the SCADA path.

Typical remote site instrumentation visible to Cyber Vision includes:

Table 3. Remote site assets

Asset class	Examples	Visibility value
Control and I/O	Site PLC/RTU, remote I/O, motor VFD	Validates master-outstation relationships and unexpected engineering sessions
Instrumentation	Flow, pressure, level, chlorine residual gateways	Confirms telemetry-only devices are not acting as unexpected clients or servers
Infrastructure	IE switch, IR1101, protocol converters, serial servers	Profiles gateways that bridge legacy serial to IP
Transient endpoints	Vendor laptops, maintenance tablets (when present)	Highlights ad hoc access that should be governed by SEA or approved jump paths

Sensor placement options at remote sites follow the same principles as plants, with constraints imposed by cabinet space, power, and whether switching is consolidated on a router or distributed on Industrial Ethernet:

Table 4. Sensor placements at remote sites

Placement	Platform	Traffic typically observed
Router-hosted sensor	Cyber Vision on Catalyst IR1101 (IOx container)	Flows that traverse the router between WAN/URWB uplink and local Ethernet or serial-aggregated subnets—strong for north-south visibility
Switch-hosted embedded sensor	Cyber Vision embedded on Catalyst Industrial Ethernet	Flows forwarded through the switch between local OT peers—strong for east-west visibility on a small REP/MRP ring or multi-drop Ethernet
Dedicated sensor appliance	Cyber Vision Sensor (where IE/IR models are not used)	Alternative for brownfield or third-party switches when Cisco validated placement applies

Utilities should deploy Cyber Vision Center centrally (virtual or appliance) and enable sensors on every remote site tier that acts as a natural observation choke point, understanding that no single sensor position sees all conversations unless it sits on the forwarding path for those flows.

When the Cyber Vision sensor runs only on the IR1101 at a remote site, visibility is effectively limited to traffic that passes through the router—predominantly north-south flows between the WAN/URWB/SD-WAN uplink and the local site subnet(s). East-west conversations that stay entirely on a downstream Industrial Ethernet switch (for example PLC to I/O, drive to PLC, or peer PLCs on a local ring) may not traverse the IR1101 and therefore will not be observed by the router-hosted sensor alone.

To obtain east-west visibility at remote sites, add a Catalyst Industrial Ethernet switch with the embedded Cyber Vision sensor enabled in the data path between OT peers (or deploy a validated Cyber Vision Sensor at an aggregation point). A common pattern is IR1101 for WAN termination, routing, and north-south inspection, plus IE switching with embedded sensor for local OT mesh or ring traffic—still without TAP cabling, by enabling software on hardware already required for port count and resiliency.

Operational outcomes for water utilities include faster confirmation of compromise scope ("was only the borehole RTU affected or the whole wellfield segment?"), evidence for regulatory and internal audits, and feeds to segmentation policy (which devices truly need to talk to which services).

Segmentation at remote sites

Segmentation prevents a single compromised Wi-Fi client, misconfigured gateway, or vendor laptop from reaching unrelated OT, IT, and management planes. Remote sites should implement default deny between trust classes and explicit allow rules for SCADA, historian, and approved management flows only.

Utilities can implement segmentation at two maturity levels; both are valid depending on staff skills, ISE adoption, and WAN architecture.

VLAN-based segmentation (foundational)

VLANs (and associated VRFs or firewall zones on the IR1101 or upstream SD-WAN edge) provide a simple, widely understood model for remote sites:

- Assign distinct VLANs for OT control (PLC/RTU), instrumentation/analyzers, surveillance (if present), corporate Wi-Fi, and network management.
- Route inter-VLAN traffic through a policy enforcement point—Secure Firewall, zone-based firewall on the industrial router, or centralized head-end rules—not through promiscuous L2 bridging between OT and IT.
- Use private addressing per site with summarized routes toward operations centers to keep WAN ACLs maintainable.
- Pair VLANs with Cyber Vision and logging so new devices appearing in the wrong VLAN are detected quickly.

VLAN segmentation is often the first phase for boreholes and pumping stations where ISE and TrustSec are not yet extended to the OT edge.

TrustSec policy segmentation (advanced)

Where the utility operates Cisco Identity Services Engine (ISE) and Cisco TrustSec across IT and extending into OT, remote sites can adopt a policy-based model that tags traffic with Security Group Tags (SGTs) and enforces downloadable ACLs (dACLs) at capable enforcement points:

Table 5. Segmentation policy component roles

Mechanism	Role at remote sites
SGTs	Classify endpoints by role (for example `OT-PLC`, `OT-IO`, `OT-ENG`, `IT-USER`) independent of IP mobility or subnet redesign
dACLs	Deliver per-session permit/deny lists from ISE to switches, wireless controllers, or router interfaces that support TrustSec enforcement
SGACLs (matrix)	Define which security groups may talk to which (for example RTU → SCADA server allowed; RTU → corporate file share denied) in a central matrix rather than per-device static ACLs

TrustSec is valuable when the same remote site mixes OT devices, contractor access, and Wi-Fi backhauled over URWB, because policy follows identity and group, not only subnet.

Industrial Ethernet platforms and wireless integrations must be validated for SGT propagation and enforcement in the specific software train; designs often combine macro-segmentation (VLAN/VRF at the site edge) with micro-segmentation (SGTs within the OT VLAN) for defense in depth.

Choosing an approach:

Table 6. TrustSec approaches

Criterion	Prefer VLAN-centric	Prefer TrustSec (SGTs + dACLs)
Team familiarity	Strong L2/L3 OT networking skills; limited security engineering	Mature ISE operations and OT security architecture
Endpoint mobility	Mostly fixed PLCs and analyzers	Mix of Wi-Fi, laptops, and mobile maintenance devices
Policy change rate	Infrequent site additions	Frequent role changes, contractors, multi-tenant OEM access
Integration target	Firewall zones and SD-WAN VPN segments	ISE, Secure Firewall with SGT, Cyber Vision asset-to-group mapping

Regardless of model, align remote-site segmentation with IEC 62443 zones: the URWB or WAN uplink is a conduit into a defined zone; local switching defines internal conduits; and Cyber Vision validates that observed traffic matches the documented zone diagram.

Data analytics, edge hosting, and remote access

Where the visibility-focused remote site design emphasizes discovery and segmentation, many utilities also need local data processing and governed remote reach into OT assets at boreholes, wells, and pumping stations—without adding a separate industrial PC, protocol gateway appliance, and VPN concentrator in every cabinet. Catalyst IR1101 industrial routers address this by combining WAN/URWB termination, routing and firewalling, and Cisco IOx application hosting on a single IOS-XE platform sized for constrained remote shelters.

The patterns below are complementary: IOx-hosted applications handle aggregation and analytics close to sensors and PLCs; remote access is delivered through a zero-trust service such as Cisco Secure

Equipment Access (SEA)—one Cisco example among several, detailed further in the Remote Access Architecture section of this document.

Edge application hosting on IR1101 (Cisco IOx)

Cisco IOx is the application-hosting framework on supported Catalyst industrial routers and select Industrial Ethernet platforms. On IR1101, IOx runs containerized workloads (Docker-oriented packaging) alongside the router's routing, segmentation, and WAN functions, deployed and life-cycled through Cisco IoT Operations Dashboard, Catalyst SD-WAN Manager, or automation APIs consistent with the rest of the network estate.

For remote water supply sites, IOx is valuable because it collapses functions that would otherwise require extra hardware:

Table 7. Cisco IOx edge application hosting capabilities

Hosted capability	Typical IOx workload	Remote-site benefit
Protocol bridging and polling	Edge Intelligence or partner containers reading Modbus, DNP3, or serial devices	Single northbound stream to SCADA or cloud; fewer parallel modem sessions
Data normalization	Containers mapping vendor tags to a utility data model	Consistent asset IDs and units before data leaves the OT zone
Local analytics	Rules for threshold, rate-of-change, or simple ML on flow/pressure/pump data	Faster local awareness; only exceptions traverse LTE/5G or URWB
Store-and-forward	Buffers during WAN outage or maintenance	Protects permit-linked and safety-related records from backhaul gaps
OT micro-services	Lightweight MQTT/OPC-UA brokers, API gateways to CMMS	Integration without exposing PLCs directly to enterprise APIs
Security services	Cyber Vision sensor or SEA gateway (per platform rules)	One managed Cisco node for connectivity plus a security function

Architectural split: IOS-XE continues to own the dataplane (routing, VPN/SD-WAN, firewall zones, NAT). IOx applications receive bounded CPU, memory, and storage, run in isolated namespaces where the platform supports it, and use northbound encrypted transports aligned with utility policy. This separation keeps control traffic on well-understood network paths while allowing iterative updates to analytics containers without full router image changes—subject to change control appropriate for OT.

Platform note – IOx workload coexistence

Not every IOx application can run together on every SKU. On Catalyst IR1101 / IR1800, Cisco documents that only one of Cyber Vision sensor or 3rd party/edge intelligence application may be active at a time on the same router. Remote-site architects should assign roles per device: for example IR1101 + 3rd party application/ edge intelligence and downstream IE switch + embedded Cyber Vision for east-west visibility—or the inverse priority if visibility on the router matters more than at that hop. Consult current ordering and release notes for memory tiers and supported container combinations.

Further IOx patterns and water-specific edge use cases are documented under Edge Application Hosting later in this solution design.

IR1101 as a field data collection and aggregation point

At remote sites, the IR1101 often acts as the primary IP aggregation point for assets that still use legacy serial or multi-drop Ethernet in addition to modern TCP/IP field devices.

Physical and logical attachment:

- Ethernet — PLCs, RTUs, analyzers, IE switches (local ring or star), and Wi-Fi/URWB backhaul homed to router LAN ports on OT-scoped VLANs.
- Serial — Built-in or module RS-232/RS-485 interfaces for legacy Modbus RTU, proprietary RTU protocols, or serial radios being retired in favor of IP—terminated in the router or passed to an IOx protocol container rather than a standalone protocol converter where possible.

Cisco Edge Intelligence (deployed as an IOx container where licensed) extends the router into an intelligent field gateway: it can poll serial and Ethernet fieldbuses, apply edge filtering (deadband, aggregation, unit conversion), and publish normalized telemetry toward SCADA, historians, or cloud analytics over the WAN/SD-WAN path. That reduces chatty northbound polling from the operations center and keeps timestamping and site context consistent at the source.

Table 8. Typical water utility data flows through IR1101 at a remote site

Source	Example data	Edge handling	Northbound consumer
Borehole RTU	Level, pump status, power alarms	Poll + exception reporting	District SCADA
Booster PLC	Flow, pressure, VFD diagnostics	Local anomaly flags	SCADA + condition monitoring platform
Analyzer gateway	Chlorine residual, turbidity	Validate range; drop invalid samples	Water quality compliance store
IP camera (if present)	Event clips	Thumbnail/event-only uplink on constrained links	Security or operations review

The diagrams below illustrate IR1101 as the convergence point between field instrumentation and wide-area backhaul (cellular, fiber, or URWB extension from a parent site).

Figure 8. IR1101 as a field data collection and aggregation point

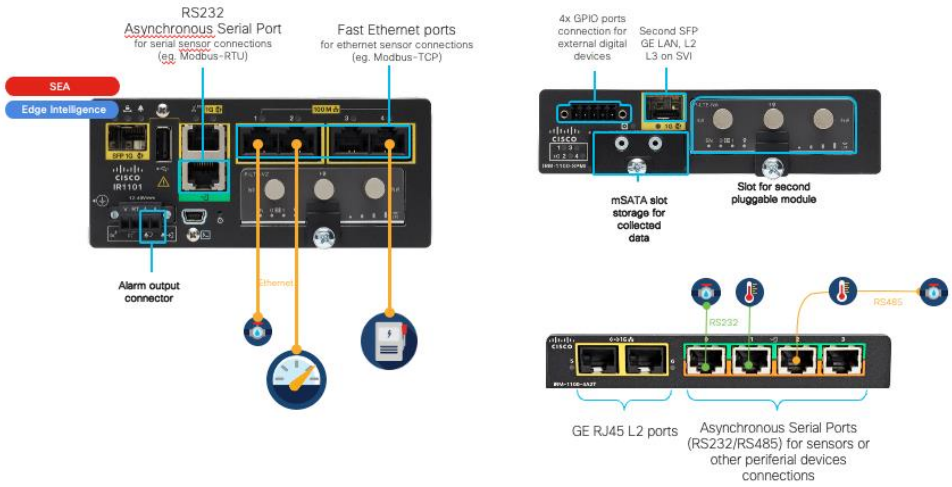
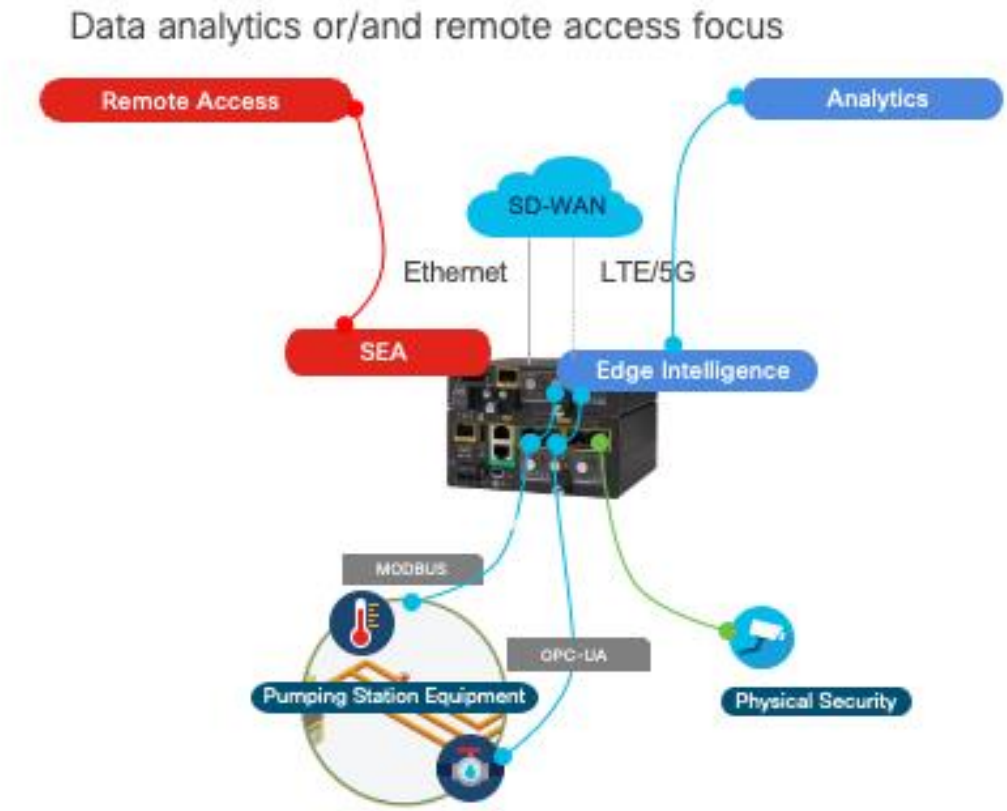


Figure 9. IR1101 as a field data collection and aggregation point



IR1101 aggregating Ethernet-attached OT, serial legacy devices, and IOx containers before secured uplink to operations.

Data collection and store-and-forward at the edge when WAN connectivity is impaired.
Design practices for aggregation sites:

- Keep closed-loop control on the PLC/RTU unless a formal safety and change process moves logic to the edge; use IR1101 for supervisory data services, not unapproved control substitution.
- Segment serial and Ethernet landing zones with the same VLAN/TrustSec model as the visibility section; containers should not bridge OT and IT trust domains without explicit policy.
- Size WAN/URWB for peak publish rates after edge reduction (storms, leak events, and camera surges are common spike drivers).
- Require signed or allow-listed container images and centralized logging so edge compute does not become an unmonitored shadow IT tier in the pump house.

Local data analytics at remote water supply sites

Data analytics at the edge means processing near the asset before—or instead of—shipping raw samples to a central lake. For dispersed water supply assets, motivations include uplink cost, latency for operational alarms, privacy or minimization of raw data, and continuity when backhaul fails.

Table 9. Local data analytics

Analytics pattern	What runs on IR1101 (IOx)	Operational outcome
Threshold and rate-of-change	Rules on level, pressure, flow	Immediate local alarm to SCADA even if cloud path is slow
Pump health indicators	Current, run-hours, starts/stops aggregation	Feeds CBM programs without continuous high-rate upload
NRW / leak hints	Nightflow or DMA imbalance rollups from local meters	Prioritizes crew dispatch; sends summaries not raw tick data
Quality guard bands	Reject or flag out-of-range analyzer readings	Reduces false regulatory events from comms glitches
Storm/flood mode	Temporary higher cadence publish for level sites	Aligns with flood monitoring use cases without permanent over-provisioning

Analytics containers should fail safe: loss of the edge app must not block the PLC/RTU from reporting through traditional SCADA paths where those exist. Prefer read-only integration to field devices for analytics workloads unless engineering workflows explicitly require write access with interlocks and audit.

Governed remote access – SEA as a Cisco example

Utilities and OEMs still need occasional interactive access to PLCs, RTUs, HMIs, and drives at remote sites—for firmware updates, logic downloads, and fault investigation. Traditional site-to-site VPNs or exposed jump hosts broaden attack surface and complicate vendor governance.

Cisco Secure Equipment Access (SEA) is a Cisco-provided example of how to deliver that access from the same IR1101 that already hosts routing and IOx workloads: a SEA agent (IOx application) registers outbound to a cloud ZTNA broker, and policy grants least-privilege sessions to named assets and approved protocols only (for example SSH, RDP, HTTPS to a drive web UI)—not blanket RFC1918 reach into the site.

Table 10. Relevance of SEA at remote water sites

SEA theme	Relevance at remote water sites
Identity and MFA	Workforce and pump/SCADA vendors authenticate via enterprise IdP (SAML) where integrated

SEA theme	Relevance at remote water sites
Time-bound vendor access	Two-hour window on one RTU at a named borehole, with approval workflow
Clientless vs SEA Plus	Browser access for quick checks; native tools (PLC programming) via SEA Plus where licensed
Audit	Session logs support NIS2-style evidence and post-incident review

SEA is not the only remote-access pattern utilities may adopt—some retain operator VPN with strict split tunneling, jump servers in a DMZ, or out-of-band cellular OOB for break-glass—but SEA fits the IR1101 + IOx model because it avoids inbound firewall holes and aligns with zero-trust segmentation described earlier.

Cross-reference: Full SEA architecture (broker roles, capabilities table, deployment with SD-WAN Manager, proxy egress) is in Remote Access Architecture. When Cyber Vision and SEA are both required at the same remote site, you can either plan two enforcement/observation nodes (for example SEA on IR1101, Cyber Vision on IE) or deploy a joint SEA+Cyber Vision sensor to the device.Cyber Vision acting as an onsite proxy for all SEA Remote access traffic.

Combined remote-site stack (example):

1. IR1101 — WAN/URWB, VLAN/zone firewall, Edge Intelligence for serial/Ethernet aggregation.
2. IOx analytics container — Local rules and store-and-forward.
3. SEA (optional on same router) — Governed remote access to approved OT targets.
4. IE switch (recommended where port count or east-west visibility is needed) — Local OT ring and embedded Cyber Vision with SEA included in the same container if needed.

This stack keeps connectivity, data, and access on Cisco industrial platforms the field team already maintains—rather than multiplying gateways, PCs, and VPN appliances at every hard-to-connect asset.

Sensors and Meters

Field instrumentation generates the operational truth for distribution, treatment, and environmental programs. Network design should carry deterministic or near-real-time telemetry where safety or compliance demands it, and batch or event-driven data where latency is acceptable—always with authenticated backhaul and zone-aware placement consistent with the cybersecurity architecture later in this document.

Leak detection

Leak detection spans distribution acoustic monitoring, district metering zone balances, customer premise smart metering anomalies, and fixed or mobile correlators on mains and service lines. Sensors may report flow imbalance, pressure transients, or acoustic signatures indicative of background leakage or catastrophic breaks. Utilities use this data to prioritize non-revenue water (NRW) programs, hydraulic model calibration, and emergency dispatch. On the network, leak platforms often consolidate at a SCADA head-end or analytics service; links should be sized for periodic bursts of high-resolution data where vendors require it, with encrypted transport and restricted east-west paths so analysis systems do not become open aggregation points for the OT domain.

Water quality

Water quality monitoring covers continuous online analyzers (for example turbidity, chlorine residual, pH, ORP, UV intensity, particle counters) and grab-sample / lab-linked workflows at treatment plants, storage tanks, and strategic distribution points. Real-time values typically feed SCADA for alarm and control; regulatory evidence may require historians with tamper-aware retention. Architecturally, separate quality monitoring VLANs or microsegments from general IT where possible, enforce read-mostly access from enterprise tools into OT data stores, and ensure time synchronization (for example PTP or NTP discipline) so correlated incident reconstruction holds up under audit.

Consumer and industrial water consumption meters (AMI)

Advanced metering infrastructure (AMI) delivers interval reads, tamper flags, and diagnostics from residential and C&I endpoints to head-end and MDMS platforms. Beyond billing, utilities use AMI for demand optimization, leak alerts at the meter, and outage awareness. Industrial submetering supports allocation, process water accounting, and trade waste reporting. Networking implications include high endpoint counts, scheduled uplink patterns, and often multi-hop RF or cellular before traffic hits Cisco WAN or industrial backhaul. Treat AMI backhaul as its own trust zone: terminate on dedicated concentrators or services, monitor for anomalous gateways or SIM behavior, and avoid bridging AMI management directly into plant I/O VLANs.

Water levels, tide monitoring, and ground moisture

Level instrumentation protects reservoirs, wet wells, dams, pumping stations, and intake structures; coastal or estuary utilities add tide gauges for saline intrusion or flood coordination. Ground moisture or soil probes support watershed, burst prevention, or irrigation-linked studies in partnership with municipalities or agriculture. These sensors are often battery-powered, low duty-cycle, and geographically dispersed—candidate technologies include LoRaWAN, satellite, or licensed radio feeding through industrial routers or gateways. Network design should provision northbound connectivity that matches update rates (storm events may require faster cadence), annotate asset location in monitoring systems for emergency use, and isolate environmental telemetry from direct control paths unless a formally assessed control loop exists.

Communication technologies

LoRaWAN suits widely scattered, battery-powered sensors when a utility deploys or contracts third-party gateways on plant or city sites. Cisco's role is typically secured IP backhaul from those gateways—across

SD-WAN, cellular, or fiber—into monitored aggregation points, with firewall and zoning so the gateway tier does not flatten OT trust boundaries.

Wi-SUN and RF mesh stacks support dense meter or field-device deployments with mesh self-healing at the radio layer. Plan RF coverage and capacity explicitly; terminate mesh networks at controlled gateways that enforce segmentation toward SCADA or MDMS and limit lateral movement from compromised endpoints.

Wired serial or Ethernet connections remain the default where cable and power already exist—directly into Industrial Ethernet, IR1101, or RTU serial ports. Wired paths reduce over-the-air exposure, ease deterministic latency discussions for control-adjacent signals, and pair naturally with REP/MRP plant rings described earlier.

Visibility and Asset Management

Water utilities operate dispersed OT estates: treatment trains, lift stations, wells, booster pumps, chemical dosing skids, lift-station RTUs, site PLCs, motor drives, analyzers, and gateways—often installed over decades with heterogeneous vendors and incomplete documentation. Visibility answers what is on the wire, what talks to what, and whether behavior matches the intended baseline. Asset management closes the loop by reconciling discovered devices with CMMS/EAM, GIS, cyber inventory, and regulatory evidence (for example NIS2-style duties to identify and harden critical systems). Without both, segmentation projects, incident response, and patching priorities rest on spreadsheets that diverge from reality after the first retrofit.

In practice, utilities should prioritize authoritative identity for OT hosts (vendor, model, firmware, logical role), communication patterns (which controllers poll which I/O, which HMIs initiate sessions), and risk-criticality (potable vs wastewater, permit-linked assets, mission pumps). Visibility feeds least-privilege firewall rules, ISE authorization policies, and patch windows scoped to maintenance outages—while asset records support capital refresh, spares, and audit without duplicating manual surveys each year.

Cisco Cyber Vision

Cisco Cyber Vision is Cisco's OT visibility and threat detection platform purpose-built for industrial networks. Observations from sensors are aggregated in Cyber Vision Center (virtual or appliance deployment) for analysis, retention, and integration with the broader security toolchain.

Embedded sensors on Industrial Ethernet (no TAP or SPAN cabling)

On supported Cisco Catalyst Industrial Ethernet switches, the Cyber Vision sensor runs as embedded software directly on the switch—typically delivered as a containerized sensor image co-resident with the IE platform's application hosting capability. Because the sensor leverages the same device that is already forwarding OT traffic, it can inspect conversations passively at the observation point without inserting a separate inline probe into the control path.

For water utilities this has several practical advantages:

- No dedicated sensor appliance or rack is required at that location—avoiding extra power, space, and cooling constraints common in pump houses, wellheads, and cabinet-sized shelters.
- No additional monitoring cabling such as TAPs, mirror/SPAN ports to external collectors, or extra fiber runs solely for security visibility—the switch already sits in the natural forwarding path for the ring, uplink, or cell-router hand-off.
- Faster rollout in brownfield plants: enable the embedded sensor on existing IE switches that were deployed for SCADA resiliency (including REP/MRP rings), rather than re-engineering physical tap points.
- Operations-friendly model: OT networking teams maintain one industrial switching estate that simultaneously carries process traffic and contributes telemetry metadata upstream to Cyber Vision Center.

Centralized Cyber Vision Center is still required to correlate observations from multiple sites, retain history, drive integrations, and present dashboards—only the distributed observation footprint is simplified to software on IE rather than parallel physical sensor hardware.

Optional Cyber Vision Sensor appliances remain available for non-IE environments or special aggregation needs, but a standard IE-led water plant design can rely primarily on embedded sensors where the switching model is Catalyst Industrial Ethernet end-to-end.

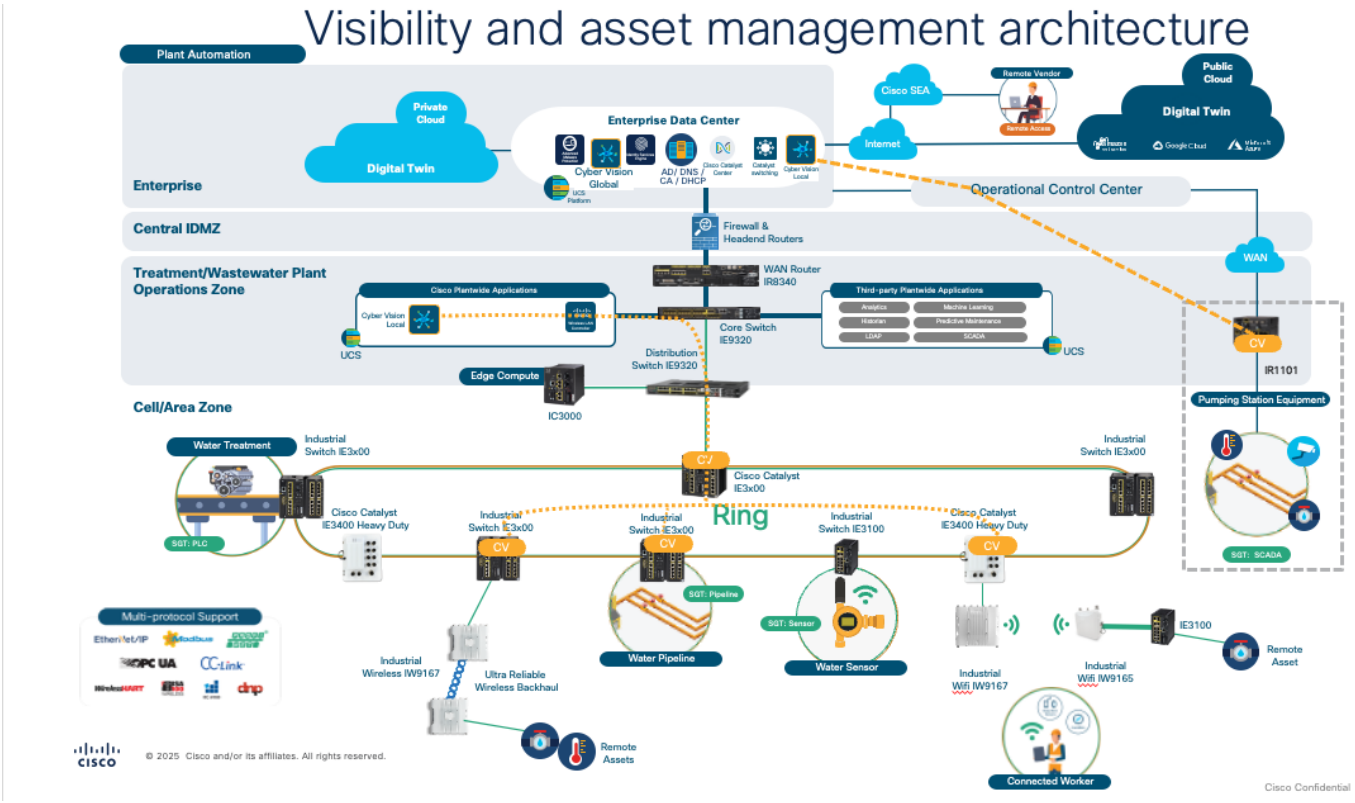
Typical capabilities used in water deployments include:

- Automated OT asset inventory: discovery of industrial endpoints with vendor/model/firmware clues derived from protocol behavior and Ethernet characteristics, reducing reliance on manual OT surveys across plants and remote sites.
- Communication graph and protocol visibility: visibility into east-west conversations between PLCs, RTUs, HMIs, and servers across Modbus, DNP3, Ethernet/IP, IEC 61850, BACnet, and common TCP/UDP services—helping validate intended versus observed conduits under IEC 62443 thinking.
- Baseline behavior and anomaly indicators: deviation from learned who talks to whom patterns to flag possible scanning, rogue masters, or unexpected engineering access paths—complementing perimeter controls rather than replacing them.
- Integration with Cisco Secure portfolio: export of rich context to ISE for profiling and policy, correlation with Secure Firewall and broader Cisco Secure / XDR workflows, and optional forwarding to SIEM (for example Splunk) so OT-relevant incidents appear alongside IT cases with consistent timestamps and asset context.
- Risk prioritization views: grouping assets by criticality or CVE exposure where vulnerability intelligence applies—supporting remediation scheduling aligned with plant maintenance windows.

Deployment note: Visibility follows where embedded sensors are enabled. An IE switch at a north-south choke point (for example plant ring uplink toward operations) emphasizes ingress/egress flows; east-west visibility between peers often improves by enabling embedded sensors on additional IE hops that already carry lateral OT traffic (for example distribution or aggregation IE on the ring)—still without new TAP hardware, only logical enablement on switches already in the path. Designs that terminate OT primarily on IR1101 or non-IE gear may require alternate sensor placement or appliances per validated Cisco guidance for that topology.

Network teams should treat Cyber Vision as passive instrumentation relative to industrial traffic—no deliberate cut-through bump for SCADA frames—while ensuring management paths to Cyber Vision Center and embedded sensor lifecycle (image updates, credentials) are segmented, authenticated, and monitored like any other privileged OT management service.

Figure 10. Embedded sensors on Industrial Ethernet (no TAP or SPAN cabling)



Remote Access Architecture

Water utilities routinely need remote reach into OT for OEM vendors, integrators, internal automation staff, and maintenance partners—without granting an always-on VPN into the plant, exposing flat L2 to partners, or parking jump boxes in a wide industrial DMZ. Cisco Secure Equipment Access (SEA) addresses this use case with a zero-trust remote access model tailored to operational workflows.

Cisco Secure Equipment Access

Cisco Secure Equipment Access is a hybrid-cloud, ZTNA-oriented service that lets authorized people reach specific OT assets for configuration, troubleshooting, or maintenance while maintaining a default-deny posture. It is offered as part of Cisco's industrial security proposition alongside Cyber Vision and integrates with centralized identity and auditing expectations for regulated environments.

How it works

SEA separates three roles:

1. Cloud trust broker (SEA portal / SaaS) — Remote users sign in to a Cisco-hosted ZTNA broker (not directly to plant IP space). The broker authenticates the user (and optionally the device), applies policy, and brokers sessions only when identity, schedule, asset group, and protocol constraints are satisfied.

2. Embedded ZTNA gateway on industrial hardware — A SEA agent runs as a Cisco IOx application on supported Catalyst Industrial Ethernet switches and Catalyst industrial routers (dedicated compute resources on the platform). That agent maintains an outbound relationship to the cloud broker and terminates the controlled path toward on-subnet OT equipment—including assets behind NAT—without requiring a parallel rack of dedicated remote-access appliances at each site.

3. Least-privilege sessions to targeted assets — Administrators define who may access which equipment, when, and with which methods (for example SSH, RDP, VNC, HTTPS, Telnet, or broader TCP/UDP where policy allows). Remote parties never receive carte-blanche network reach; exposure is limited to approved targets and approved protocols.

Connectivity is initiated so that operational networks are not advertised for blanket discovery from the Internet; lateral movement is constrained by microsegmentation that can continue to be enforced on the same industrial router or switch acting as the gateway.

Principal capabilities

Table 11. SEA capabilities and their relevance to water utilities

Theme	Examples relevant to water utilities
Least-privilege policy	Access groups tying identities, asset lists (for example a lift-station PLC cluster), schedules, and allowed methods—so a contractor can work a two-hour window on one RTU, not the entire basin.
Strong authentication	MFA and optional SSO via SAML 2.0 with your enterprise IdP so workforce and partner accounts follow corporate identity lifecycle.
Governed vendor access	Session request / approval flows so a vendor must obtain explicit approval before a session can start—useful for pump OEMs or SCADA suppliers with intermittent access needs.

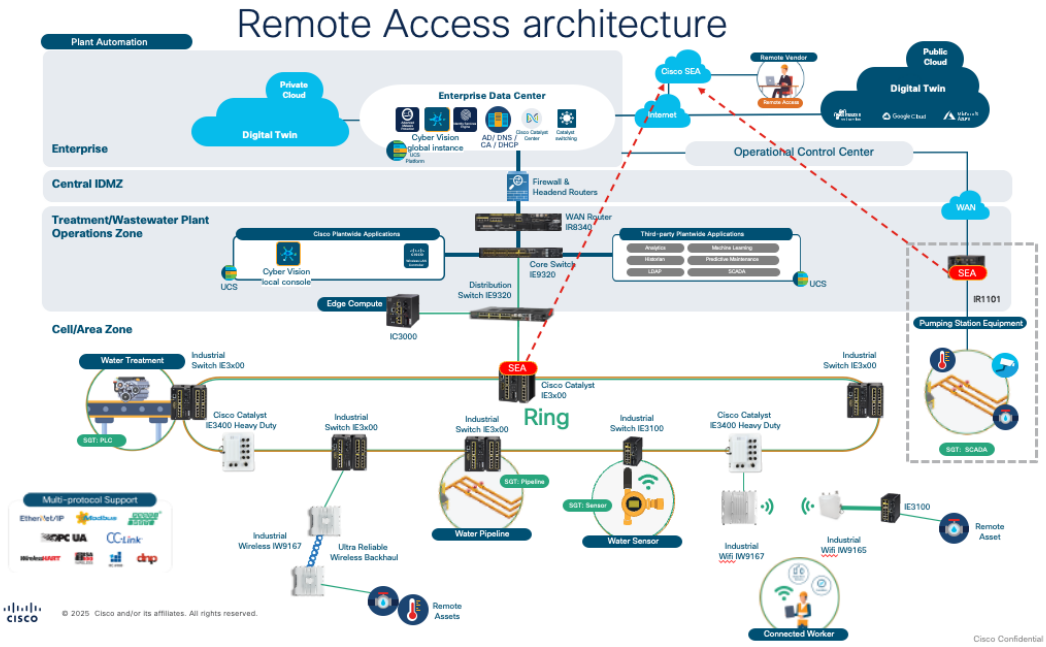
Theme	Examples relevant to water utilities
Device posture (SEA Plus scenarios)	Integration with Cisco Duo to evaluate endpoint posture before granting full IP/application-level access—for example ensuring maintenance laptops meet patch or EDR expectations.
Access modalities	Clientless access through a browser to common interactive protocols (RDP, VNC, HTTP(S), SSH, Telnet). SEA Plus (agent-based ZTNA) establishes a secure IP channel so engineers can run native tools—PLC programming suites, vendor configurators, or secure file transfer—within the same policy envelope.
Operational oversight	Live session monitoring, join-in-progress observation for supervision or coaching, administrator-initiated termination, optional session recording for audit, dashboards for usage and anomalies, and ITDR-style alerts for risky conditions (for example unusual geography or hours).
Audit and compliance support	Exportable logs covering policy changes, authentications, and session activity for regulatory evidence, internal OT governance, or incident reconstruction.

Deployment can be guided from the SEA cloud portal; industrial routers may alternatively align SEA agent rollout with Catalyst SD-WAN Manager where that is the operational model for IR1100 / IR1800 fleets.

Water utility deployment considerations

- Distributed sites: SEA scales across many small facilities (wells, boosters, storm stations) because the gateway function rides on industrial switching or routing already purchased for connectivity—reducing bespoke iDMZ firewall sprawl.
- Outbound-centric model: Gateways initiate outbound connectivity to the broker, which often simplifies firewall posture versus inbound VPN concentrators—subject to your organization's cloud connectivity standards.
- Cyber Vision coexistence: On many IE platforms, Cyber Vision sensor and SEA gateway can run together. On Catalyst IR1101 / IR1800, Cisco documents that only one of Cyber Vision or SEA may be active at a time—water architects should decide per router whether visibility or remote access is the priority on that hop, or distribute roles across devices in the topology.
- Proxy requirements: IE switches can use a customer-controlled HTTP(S) proxy toward the SEA cloud where Internet egress policy requires it—helpful for utilities with strict egress allow lists.

Figure 11. Water utility deployment considerations



Edge Application Hosting

Hosting compute at the network edge lets water utilities process telemetry locally, buffer data during WAN outages, run vendor containers close to PLCs and sensors, and reduce expensive northbound traffic—without installing separate servers in every cabinet. Cisco IOx is Cisco's application-hosting framework on industrial IOS-XE platforms so those workloads run on the same appliances already providing routing, switching, Cyber Vision, or Secure Equipment Access.

Cisco IOx application hosting framework

IOx exposes a controlled runtime on compatible Catalyst industrial routers (for example IR1100 family) and select Industrial Ethernet platforms that include sufficient compute and memory for hosting services. Applications are typically packaged as containers (Docker-oriented workflows) and deployed through Cisco IoT Operations Dashboard, Catalyst SD-WAN Manager, or automation APIs—aligned with how operations teams already stage, upgrade, and rollback network images.

Conceptually, IOx separates network dataplane duties from hosted applications:

- Dataplane continuity: Routing, segmentation, firewall features, and WAN connectivity remain IOS-XE functions with deterministic behavior for OT traffic.
- Edge applications: Supplemental processes receive CPU/RAM/storage quotas, isolated network namespaces where appropriate, and northbound APIs to reach cloud services over encrypted transports aligned with enterprise policy.

Platform specifics vary by hardware—consult Cisco ordering guides for IOx-capable SKUs, memory tiers, and whether multiple hosted services (for example SEA, Cyber Vision sensor, Edge Intelligence) can coexist on the same chassis versus mutually exclusive combinations documented per model.

Cisco Edge Intelligence (where deployed) builds on IOx-style hosting to run partner or utility-developed analytics containers that normalize OT data—for example aggregating serial or Ethernet fieldbus reads before forwarding summaries upstream—without mandating an extra industrial PC at each pumping station.

Operational expectations for IOx workloads mirror OT discipline: life-cycle patch paths, logging that integrates with centralized observability, least-privilege east-west communication between containers and field devices, and cyber hygiene so edge compute does not become an unmanaged shadow IT tier inside the plant VLAN.

Water utility edge use cases

Table 12. Water utility use cases

Use case	Edge role	Utility outcome
Telemetry aggregation and protocol bridging	Combine Modbus, DNP3, MQTT, or vendor-specific polls behind the router into normalized streams toward SCADA or cloud historians.	Fewer parallel cellular sessions, consistent timestamping, and protocol conversion without extra gateways.
Offline / degraded-WAN survivability	Buffer and spool events when SD-WAN, fiber, or cellular is impaired; replay when the path returns.	Continuity of permit-relevant and safety-related records; reduced data loss during storms or backhaul maintenance.

Use case	Edge role	Utility outcome
Local analytics and alarming	Run anomaly rules (for example flow/pressure step changes, pump current signature drift) at the source.	Faster local response; only exceptions or rollups go to the NOC, cutting backhaul and cloud cost.
Image and file triage	On sites with IP cameras or vibration high-sample data, pre-process to thumbnails, events, or FFT summaries at the edge.	Meets uplink budget on LTE/5G-constrained sites.
OT/IT data services	Host lightweight databases, OPC-UA micro-brokers, or API shims for work order or CMMS integration.	Context (asset ID, site) bound to data before it leaves the OT security zone.
Secure service colocation	Co-resident IOx services next to IOx-based SEA or sensors (per platform support) to keep remote support and data prep on a single managed Cisco node.	Simplifies spares, firmware currency, and site access for field teams.

Design practices for these patterns: keep control loops on the PLC/RTU unless a formal safety/change process authorizes moving logic; use the edge for supervisory analytics and data services. Segment container traffic with the same VLAN/zone rigor as the rest of the architecture, and require signed or allow-listed images for production. For ICS regulations and NIS2-style evidence, pair edge applications with auditable session and data-lineage records in the SIEM or data platform of record.

Summary

This Water Solution Design is a Cisco reference design and implementation guide for water and wastewater utilities modernizing operational technology (OT) networks. It is intended for utility architects, system integrators, partners, and operations teams who need a consistent blueprint to deploy secure, resilient, and scalable connectivity from treatment works and data centers through WAN and remote field assets—including pumping stations, boreholes, wells, reservoirs, and distribution instrumentation.

The document ties business and operational use cases to proven Cisco architectures rather than presenting a catalog of products in isolation. It explains why each technology fits typical utility constraints (legacy serial, multi-vendor SCADA, dispersed sites, regulatory pressure) and how components compose into deployable patterns.

What this reference design provides

Operational context and use cases — Foundational coverage of utility programs that depend on reliable connectivity: advanced metering (AMI), condition-based maintenance, flood monitoring, water quality surveillance, and SCADA modernization (IP transition, integration, cybersecurity, and migration discipline). These sections establish the data, latency, and availability expectations that drive network design choices.

Enterprise and plant architecture — A multi-layer framework spanning data center and SCADA master environments, campus and treatment-plant networks, WAN/SD-WAN with multi-transport underlays (fiber, MPLS, cellular, satellite), and industrial edge at operational sites. The design centers on Catalyst Industrial Ethernet (IE) for harsh plant environments, IR industrial routers for remote aggregation, SD-WAN for centralized policy and security, and intent-based operations through platforms such as Catalyst Center.

Network engineering patterns — Actionable guidance for:

- WAN and SD-WAN — Flexible underlays, integrated security, and application-aware routing for distributed utilities.
- Plant networks — Cost-effective ring topologies using Cisco REP and IEC 62439-2 MRP for resilient SCADA and I/O connectivity, including multi-vendor brownfield integration.
- Wireless — Ultra-Reliable Wireless Backhaul (URWB) to reach hard-to-connect assets and backhaul remote switches and Wi-Fi; separate Wi-Fi patterns for OT instrumentation versus corporate mobility, with VLAN and policy segregation.
- Remote assets — Cyber Vision visibility (including north-south vs east-west placement on IR1101 vs IE), segmentation via VLANs or Cisco TrustSec (SGTs and dACLs), IR1101 as a serial/Ethernet aggregator, IOx edge hosting and Edge Intelligence for local analytics, and governed remote access exemplified by Cisco Secure Equipment Access (SEA).

Field instrumentation and backhaul — Considerations for leak detection, quality monitoring, AMI, and level/environmental sensors, plus when to use wired, LoRaWAN, Wi-SUN, or IP backhaul through industrial routers—always with zone-aware placement aligned to security architecture.

Cybersecurity and compliance alignment — A defense-in-depth model supporting NIS2-style duties: OT asset visibility and communication baselines (Cisco Cyber Vision, including embedded sensors on IE without TAP cabling), segmentation and electronic security perimeters, anomaly detection, secure remote access, and integration with ISE, Secure Firewall, and SIEM (for example Splunk). Remote access is addressed explicitly through zero-trust patterns rather than flat VPNs into OT.

Edge compute without extra PCs — Cisco IOx on industrial routers and switches enables protocol bridging, store-and-forward, local analytics, and colocated security or access services—reducing cabinet complexity

at constrained remote sites while keeping control logic on PLCs/RTUs unless formally engineered otherwise.

Design outcomes utilities can expect

Adopting this reference design helps utilities:

- Standardize plant, WAN, and remote-site topologies for faster greenfield and brownfield rollouts.
- Extend IP connectivity to assets that lack fiber or trenching, using URWB, cellular, and IR1101 aggregation.
- Improve security posture with visibility, segmentation, and auditable vendor access—without sacrificing operational availability.
- Reduce cost and complexity by consolidating routing, backhaul, analytics, and remote access on managed industrial platforms.
- Prepare for modernization—smart water, CBM, AMI, and cloud analytics—on a network foundation that supports IEC 62443 zone thinking and regulatory evidence.

This document is guidance, not a substitute for site-specific RF surveys, safety reviews, or vendor FAT/SAT; utilities should validate hop counts, IOx workload coexistence, and TrustSec enforcement against current Cisco ordering guides and release notes for their chosen platforms.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA 06/25