BETTER PROTECTION AND MAINTENANCE OF WATER AND WASTEWATER SYSTEMS

Honeywell

CONTENTS PAGE

INTRODUCTION

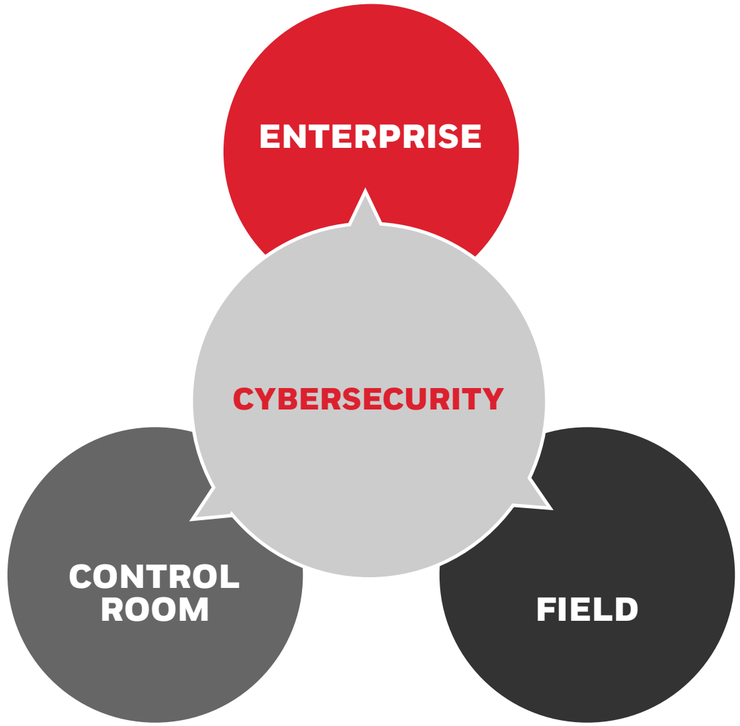
Improvements to water and wastewater facilities continue to grow in importance as infrastructure ages. In a recent study conducted by Water & Wastes Digest, more than a quarter of those polled indicated they planned new water and wastewater facility construction over the course of 2020 and 2021, and 44 percent said they planned to upgrade existing facilities. The largest investment in water and wastewater solutions is expected to be in system monitoring as technology becomes more robust and demand for services increases.

As the world's population grows, the need for fresh water will grow with it, putting pressure on legacy systems. Those who maintain these water and waste utilities must find effective ways to upgrade them to keep pace. This e-book will discuss leading-edge technology solutions that are being used with great success across the industry to upgrade and grow water solution infrastructure while providing innovative and cost effective improvements. When demand requires a system upgrade, it's time to look at implementing smart solutions that will enable future growth in addition to immediate need.

Because water and wastewater infrastructure systems are fundamental to the health and well-being of the entire world's population, their security, integrity and resilience are crucial. However, maintaining and protecting them involves attention to a wide variety of significant challenges: quality standards, compliance issues, efficiency, costs and reliability, among others. In addition, there is the critical need for protecting them against cybersecurity threats.

The complexity of these issues extends throughout each layer of the water and wastewater system:

The enterprise level, which relies on secure data and system analytics reporting for budgeting, benchmarking purposes and process improvement. This information may include supervisory control and data acquisition (SCADA) system information on water flow, dissolved oxygen, energy usage, daily and weekly trends, inefficiencies and so on. It also reveals cost and performance issues associated with less-than-optimal system components, allowing for cost analysis, financial reporting and replacement budgeting by decision-makers. In addition, detailed data must be collected by the system for the purposes of regulatory compliance.



The control room level, in which operators must monitor and maintain the operational environment in real-time for optimal system performance. This data is used to schedule predictive maintenance, identify potential points of failure and existing leaks, address flow issues and proactively replace failing system assets—all with information derived from multiple information-gathering components of varying ages, made by different original equipment manufacturers (OEMs) and using a variety of protocols. Without a communication standard and a centralized, integrated display with alarms, operators may not have ready access to the information needed to keep the water flowing.

CHALLENGES TO EFFICIENT AND SECURE WATER MANAGEMENT

RISING MAINTENANCE COSTS

EXPANDABILITY

REDUCED ENERGY COSTS

UTILITY TRANSFORMATION

INTEGRATED CONTROLS

IMPROVED PERFORMANCE

WATER QUALITY STANDARDS

COST AND SCHEDULE CONTROLS

PLANT UPTIME

REGULATORY COMPLIANCE

CYBERSECURITY RISKS

LIFECYCLE COST MANAGEMENT

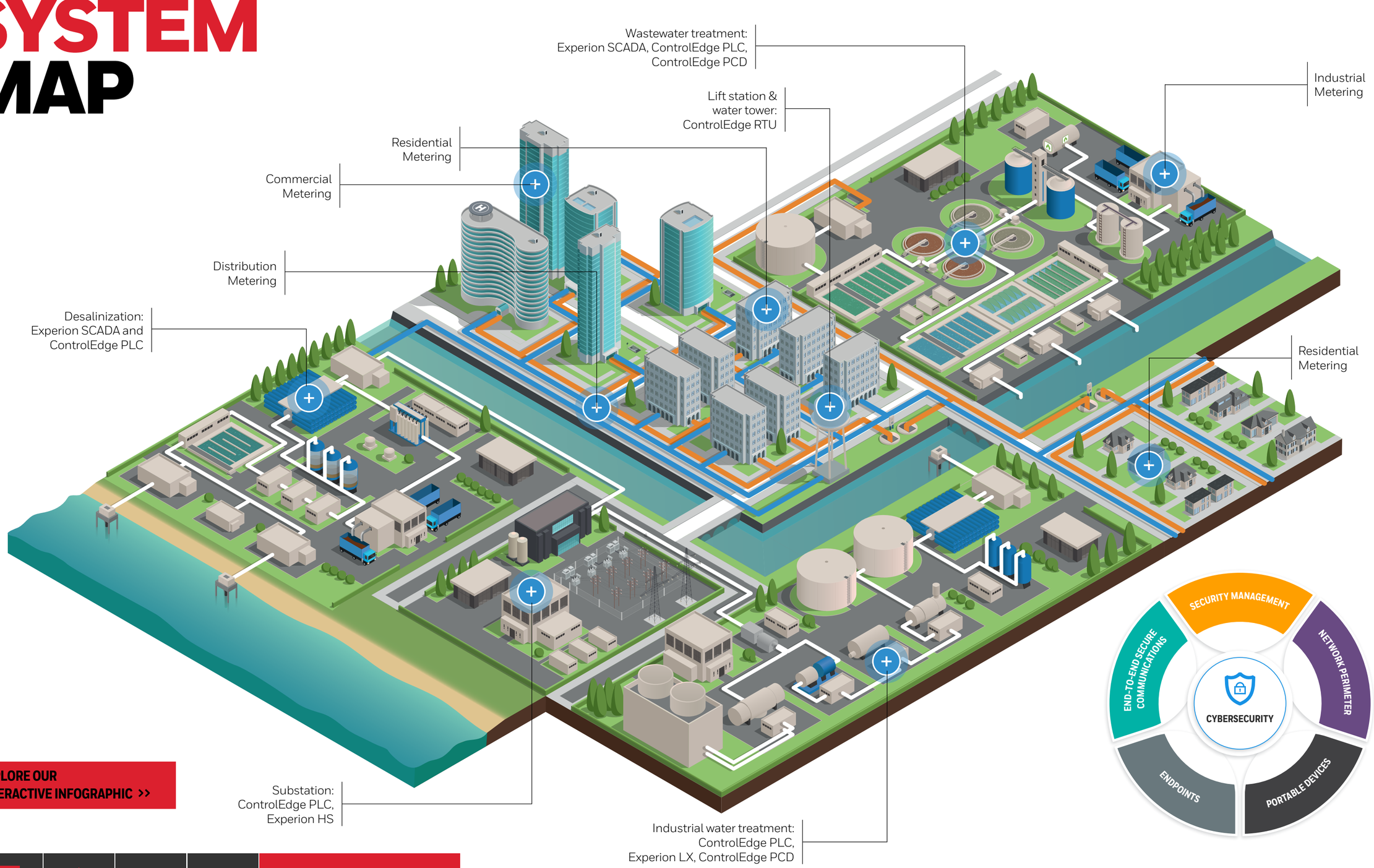
Remote field locations and assets, including pump and lift stations, storage tanks and meters, all of which must be kept secure and optimized for performance. This requires real-time data collection technology, which must be transmitted to and interpreted by the master SCADA system, regardless of the devices' technology. Field data is typically transmitted over the internet, which can save the cost of on-site visits, but operations technology (OT) assets in the field must be secured and their data protected from cyberattack.

Cybersecurity is of concern at each of these levels, whether the operations technology (OT) employed is modern or a legacy system. The challenge here is that any such solution must be technology-agnostic while protecting operations and maintaining coordinated control within a variety of systems in numerous physical locations. Security must be end-to-end along its entire pathway—whether it resides internally, within removable media or is delivered across the web.

This e-book will explore the inherent challenges to water and wastewater utilities—of managing a multitude of components of different technology generations, dispersed across extended geography, performing a variety of tasks and using different operating protocols. It will discuss effective ways in which each operating layer can leverage that unified data, present the unique concerns of cybersecurity as it impacts each, and discuss how Honeywell has successfully addressed these issues through advanced technology.

LEARN MORE >

SYSTEM MAP



EXPLORE OUR INTERACTIVE INFOGRAPHIC >>

LEARN MORE >

ENTERPRISE LEVEL CHALLENGES AND SOLUTIONS

High-performing water utilities need accurate analytics reporting and data visualization to optimize performance and effectively benchmark their operations' efficiency. To be comprehensive, the data must provide a complete history, regardless of the control systems employed, and offer a reliable and robust archive of customizable reports.

This is essential for cost analysis and budgeting purposes, as well as for asset planning and management. The enterprise level is also responsible for ensuring compliance with national and regional water quality standards and regulatory requirements.

Data and visualization

To provide real-time digital intelligence, a solution must be compliant with Industry 4.0 protocols. This is a recent technology approach that requires a blending of physical systems, sensors, wired and wireless communication that, when taken together, allows all components within the system to interact with one another and with human operators—an "internet of things" (IoT) for industry.

At the enterprise level, this information can be used to:

- Model system upgrades and equipment replacement, and their respective costs
- Ensure regulatory compliance related to water quality and sanitation
- Project and proactively manage changes in water usage due to seasonality, weather events and other trends
- Develop mitigation plans in the event of a service interruption or cyberattack
- Acquire benchmarking data to assess the greatest potential areas for improved efficiency and cost reduction

Huge Desalination Project Looks to Honeywell Automation

GEIDA, a consortium of Spanish companies, was looking to build a facility that would desalinate sea water in order to provide drinking water for 750,000 customers in Algeria. GEIDA stakeholders needed an advanced control and automation solution to operate the plant, and turned to Honeywell's Experion PKS because of its technology, leadership and maintenance expertise. "The company had to demonstrate its ability to execute this size and scope of project and provide the maintenance and onsite staff that we felt were imperative to make this project a success," said Miguel Larrinaga, instrumentation, control and electricity assembly manager for Befesa Agua's International Division.

The company needed centralized, integrated control and data from four remote locations, a cost-effective implementation and a fiber optic network. In spite of the size and scope of the project, Honeywell delivered it two months ahead of schedule. "We were able to take advantage of a state-of-the-art control system and plan to use the plant for years to come," adds Larrinaga. "With their help, we were able to start up this facility ahead of time and on budget, and achieve the reliability, safety and efficiency expected."

Key performance indicator (KPI) dashboards provide the advanced analytics required for this high level of aggregated data collection, enabling management to control costs, develop accurate forecasts, set achievable goals for improvement, as well as protect the system from intrusion and the organization from issues arising from noncompliance.

Honeywell's Uniformance Process History Database (PHD) layers on top of the distributed control system (DCS) to collect and organize system data. The business analytics it provides can increase production uptime, reduce operating costs, control risk and provide information valuable for regulatory compliance and reporting.

Data historization and analytics

Historization adds a fourth dimension to data visualization—that of time. This enables analysis of trends based on environmental, seasonal and societal conditions as they evolve.

Large databases contain a lot of information, but without the enhancement of historization, do not generally provide much insight on how that data changes. The result is that the trending information contained within the dataset is buried in it, inaccessible to those who need it for the purposes of developing projections for system upgrades, maintenance schedules, usage fluctuations, and their associated costs and timelines—all those factors that fluctuate over time.

An advanced historization solution provides a consolidated dataset collected from all components of the water and wastewater system, all the way from individual meters to the control room, and presents it in visually impactful dashboards. Instead of just recording data, this process organizes and displays it in a customizable, easily understandable way to enable enterprise-level stakeholders to project costs, budget for system maintenance and manage compliance requirements.

Honeywell's Experion Historization is a universal system-agnostic solution that reports this enterprise-level data. Because it can interpret data from every part of the system, regardless of its technology, it provides a highly-scalable solution for managing large databases containing millions of tags, providing the customizable reporting and trending data necessary to manage operations at the enterprise level.

Cybersecurity

Executives are charged with managing cybersecurity risks to every aspect of the operations technology (OT). It is their ultimate responsibility—and liability—if the system is breached in any way. Every aspect of the process should undergo offensive security testing (aka penetration testing) to identify risks of exploitation by malware, hackers, and bad actors.

It is no longer sufficient to have a site-specific approach to cybersecurity. Protection must be centralized at the enterprise level, encompassing all components of the system end-to-end, no matter how widely distributed or complex. Water utilities should work with a partner for industrial cybersecurity, with expertise in operational technology (OT), and offering vendor-neutral solutions for enterprise-wide deployments.

For example, Honeywell Forge Cybersecurity Suite provides a scalable, single-platform solution that continuously monitors risk and compliance, automates software updates, prioritizes the assets at greatest risk and automates critical data collection activity. Honeywell Cybersecurity Consulting Services provide strong OT cybersecurity expertise that decision-makers need to keep their facilities safer and operational without themselves needing to become experts on the subject.

CONTROL AND DATA CENTER LEVEL CHALLENGES AND SOLUTIONS

Traditionally, control room operators have had to absorb and process facility information largely on their own. In the past, there was no ready solution for accessing consolidated information from the whole system in a single place. Each subsystem generated its own data that required monitoring, and each alarm required individual investigation and resolution, with no automated or naturally intuitive way to prioritize it. This was a process fraught with opportunity for error and it placed undue stress on the personnel tasked with keeping the operation working.

Fortunately, that has changed with the introduction of advanced process control solutions. Not only do these integrate data coming in from the various systems and subsystems along the process chain, regardless of their underlying technology; these solutions also present the data in an easily-understandable, visual format that makes the human-machine interface (HMI) straightforward, facilitating easier and more intuitive decision-making.

Control and metering

Automatic meter reading (AMR) prevents a human being from having to perform readings in-person and manually record the results. In AMR, meters are fitted with transmitters that provide the output via one-way communication to a device that logs the information and is then used to generate a bill to the customer. However, AMR is a “passive” technology in that the meter does not receive information, it only transmits it.

Advanced metering infrastructure (AMI), on the other hand, permits two-way communication between the control system and the meters.

Honeywell Upgrades Finnish Treatment Plant

Espoon Vesi, a water treatment plant in southern Finland, manages the water supply and wastewater treatment for a region of about 300,000 people. In an effort to ensure clean water production and distribution and successfully treat wastewater, Honeywell was brought in modify the automation network, assist with system upgrades and implement Uniformance PHD reporting functions. Plant automation was also brought into compliance with Honeywell’s rigorous cybersecurity standards.

Now, the system sends thorough reports on its functionality and potential problem areas to the company’s control room team. It relays plant alarms to the phones to on-duty individuals via a closed VPN tunnel. “We are able to quickly get the information on a damaged device and take immediate action if necessary,” said Jari Alvasto, automation engineer for Espoon Vesi. This warning information can also be sent securely to customers, who are then able to take any necessary action on their equipment.

Alvasto is a satisfied Honeywell customer: “We knew we had a high-quality solution that would help us meet our plant goals. We were able to save both time and money.”

The two-way communication between the meter and the plant enabled by AMI allows integration with SCADA systems to detect and report water usage or tampering. By analyzing flow data combined with water pressure metrics, AMI—or "smart meter"—technology can report a leak in progress before it becomes serious, using a variety of available transmission methods, including Wi-Fi and other wireless options. Operators are able to take immediate action by shutting down a portion of the system remotely and then scheduling a repair.

There is also a customer service benefit to AMI. More accurate bills and reports enable users to better manage their water usage and take action if unusual activity is noted, such as a potential on-premise leak or open tap.

The software that underlies the AMI must implement cybersecurity controls, since data passes back and forth between the meter and the SCADA system. Honeywell Process Solutions (HPS) Secure Product Development Process is ISASecure certified. This represents the standard for security of industrial control systems to ensure product development teams apply cybersecurity best practices in the software development lifecycle. This safeguards the overall water system and its data.

Process control

An optimal control room environment relies upon solid and actionable data, delivered in a visually intuitive manner. A large volume of data must be collected, organized and presented in a user-friendly way that empowers control room personnel to make effective decisions quickly.

In an optimized control room environment, the HMI is seamlessly integrated with the underlying data. Data moves into the touch-enabled display panel PC through the web from a variety of device drivers and protocols. This should be standardized and available throughout the control room environment, whether on console or tablet, allowing operators to move throughout the facility. Ideally, this interface should also be highly intuitive, allowing new operators to get up to speed quickly.

With so much data flowing in from pumping stations, metering subsystems, sludge and wastewater systems, operators need to be able to rapidly absorb it visually and react to it. A real-time graphical display with live trending information and alarm management is essential for efficient—and therefore profitable—operation of water utilities.

The display console should also be ergonomically designed and customizable, so that operators do not become fatigued while using it and are able to configure it to meet their specific needs. The Experion Orion Console was engineered using data gleaned from actual operator behavior. The resulting design reduces strain and facilitates operator movement with the use of a mobile tablet. Its ultra-high definition, pan-and-zoom display is also operator-friendly and easier on the eyes.

One of the challenges in the control room environment is obtaining a display that is optimized for the available space. An application like Honeywell's Panel HMI solution offers a variety of different display sizes and capabilities to ensure the right fit, regardless of the center's particular needs and layout.

While HMI displays are critical to getting a fast and intuitive visual representation of system operation, the technology that powers this intelligence rests upon solid data. The backbone of the control room environment is the SCADA system.

Operators rely on SCADA to gain insight into and control over end-to-end system assets, including wastewater collection and water distribution systems, flow management, pump stations, sewers, sludge monitoring and more. A solution like Experion HS SCADA offers hundreds of pre-built graphs and task-based filters to customize the presentation of data to control room operators. The software's HMI displays real-time and historical process trends such as overflow counts, pumping metrics and dissolved oxygen numbers.

An integrated process control system collects, analyzes and distributes information to operators, who are able to respond more quickly and make better decisions based on it. This not only improves the performance of the assets within the system, it minimizes energy consumption, facilitates regulatory compliance, maximizes plant uptime and increases overall profitability. Honeywell's Experion LX offers an intuitive, uncluttered interface

Experion Orion Console

that makes getting up to speed faster and enables operators to focus on the task at hand rather than the technology behind it.

A cost-efficient alternative to on-premise SCADA systems are cloud-based, like Honeywell's Elevate, a software as a service (SaaS) application. This can eliminate the need for on-site IT staff to update software and maintain it. This is a streamlined approach that ensures the latest version is always available to operators via a web interface connected to Honeywell's own servers. The application's data is maintained securely in the cloud, accessible from any authorized device and protected by robust cybersecurity.

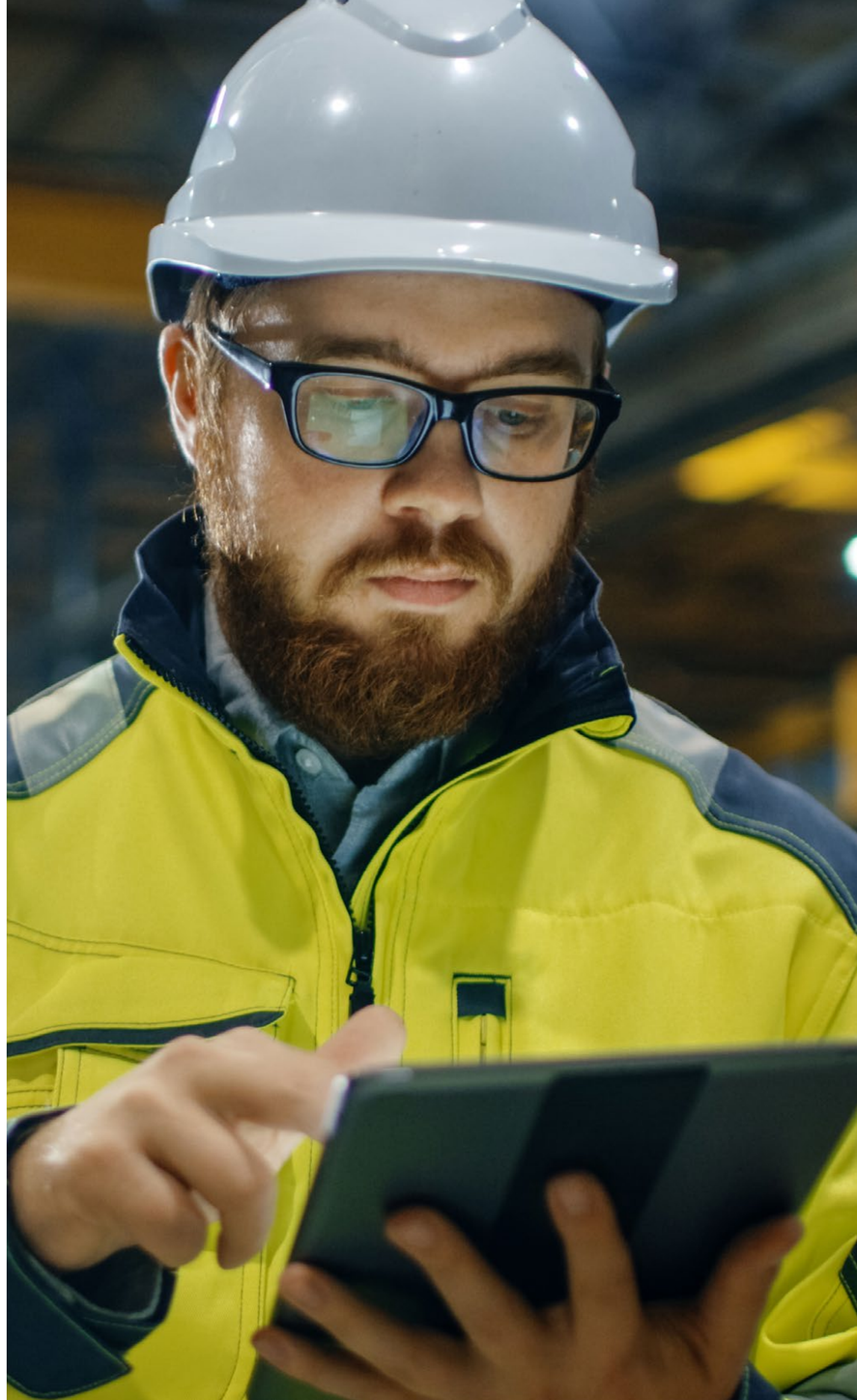
Cybersecurity and Secure Remote Access considerations

One of the significant advantages of the Honeywell Forge Cybersecurity Suite is that it simplifies OT remote access and the complex business of monitoring a variety of assets in many different physical locations. It provides a single platform for multi-site cybersecurity and vendor-neutral solutions, including Industrial Grade Secure Remote Access capabilities, regardless of the control systems used by the various components. This ensures that the entire system is better protected from end to end.

Now more than ever, the health and safety of critical personnel is a top organizational priority, and this may require expanding remote access capabilities for workers. Honeywell Forge Cybersecurity Suite provides mature Industrial Grade Secure Remote Access capabilities designed specifically for OT/control systems. It is safer and more secure than traditional virtual private networking (VPN) and remote desktop (RDP) technologies that could be endangering the integrity of OT due to their history of vulnerabilities[1] [2].

In addition to providing improved/enhanced enterprise-level cybersecurity, Honeywell Forge Cybersecurity Suite helps manage the security of the assets from the field to the control room level, providing an inventory of assets and monitoring them for security issues. The software can prioritize the highest risk components of the system or those that are out of compliance with security standards, based on an intuitive "risk scoring" capability.

Because malware is always changing, with new threats constantly coming online, cyber risks must be monitored and protected against through software updates. Honeywell Forge Cybersecurity Suite simplifies management of antivirus patching while producing fast and simple cybersecurity reporting to stakeholders.



[1] Vulnerabilities in Multiple VPN Applications, Cybersecurity and Infrastructure Security Agency (CISA), published July 2019 and last accessed May 2020.

[2] Wormable vulnerabilities in Remote Desktop, Microsoft Security Response Center, published August 2019 and last accessed May 2020.

FIELD AND REMOTE ASSET LEVEL CHALLENGES AND SOLUTIONS

Field infrastructure in the water and wastewater utility sectors tends to be outdated, which puts additional pressure on the health of the overall network. There is research showing that aging system components and old technology result in the loss of more than a trillion gallons of drinking water each year in the U.S.

Modern industrial IoT technology can go a long way toward improving the quality of water while ensuring compliance with regulatory standards. Sensors are able to detect pressure in the system and adjust flow according to demand, thereby extending the life of the pipes, and can pinpoint problems before they become major incidents. Technology also greatly improves response time in mitigating leaks and reduces the need for on-site emergency personnel.

Control

Water treatment processes consist of several stages, each involving specialized equipment that performs specific functions. This process can be managed automatically

ControlEdge PLC

Water Leaks at Complex Airport Site Solved with Smart Metering

The Montpellier-Méditerranée Airport in southern France had experienced significant water leaks throughout its large, complex site, which includes open land, offices and maintenance areas. Merely identifying the problems in order to repair them had become a tedious daily task, requiring constant manual collection of meter data. Failure to control the leaks could result in expensive damage to infrastructure, but without smart metering technology, there was little choice but to send personnel around the site to constantly check them.

The airport chose Honeywell to implement a fixed private network that provided a fast and reliable automated method of meter reading, even for equipment positioned in the most remote locations. Because the meters enabled two-way communication, it was possible to get additional on-demand data from them to better evaluate a problem.

An airport spokesperson said, “The Honeywell smart meters and dashboard replaced the manual readings. It also allows us to limit our leak search to a restricted area, whereas our previous process of random searching was time-consuming and prone to errors.” The airport is expected to grow, and as it does, more data loggers will be installed to ensure that a stable and sustainable water management program grows along with it.

ControlEdge RTU

by programmable logic controllers (PLCs) and software, requiring minimal human interaction. For example, Honeywell's ControlEdge PLC communicates with the system using a variety of available software protocols, and integrates seamlessly with Experion SCADA for optimized performance. Benefits include:

- Reduced integration costs
- Minimized downtime
- Managed cybersecurity
- Lengthened system lifecycle

The data collected by the PLC is regularly published to the SCADA system for historization and reporting.

ControlEdge RTU is a highly-durable PLC designed to operate at low power consumption in extreme outdoor environments. It is ideal for use in remote areas with a limited power supply or in those locations dependent on an alternate energy source, such as wind or solar. The collection intervals for lift stations and water towers can be set by the operator; the data is then automatically gathered and transmitted over wireless networks to the water utility's central SCADA system, even in areas with low bandwidth.

Lift stations in hilly terrain are particularly subject to overloading and malfunctioning. This must be carefully monitored by regular flow metering and diagnostics to keep disruption and the associated maintenance to a minimum. ControlEdge RTU, working with Experion SCADA, has been shown to reduce required engineering time by 90 percent.

Both ControlEdge devices are certified as ISA-Secure Level 2 components. This means they have been rigorously tested and meet strict cybersecurity standards.

Metering

Accurate metering is essential to monitoring water flow and generating customer billings. However, the data from meters is valuable at each level of the system, since it represents the delivery endpoints. This consumption information can be used for a variety of analytics and reporting purposes in addition to invoicing.

For residential metering, a static meter that measures cold, potable water with no moving parts is ideal. It is not affected by the wear and tear caused by particulate matter like sand, resulting

LEARN MORE >

HONEYWELL METERING PRODUCTS

Hybrid Apartment Meter

- Offers secure radio communications so landlords can accurately measure tenant water usage
- A range of different products is available

Hybrid T5000 Turbine Meter

- Widest measuring range of any water meter technology
- Rotor is the only moving part
- Measures flow continuously; nominal battery life of 12 years

Static Q500 Ultrasonic Meter

- Uses no moving parts; no leaded material in contact with water
- Designed for cold potable water in residential applications
- Interface compatible with most AMR/AMI systems

in accurate metering over its lifetime. This type of meter can be integrated into smart systems for automated and accurate readings without human intervention.

The Honeywell Q500 static ultrasonic meter provides data via multiple communication methods and is compatible with most AMR and AMI systems. Its polymer body construction ensures there is no leaded material in contact with the water at any time, and brass thread inserts provide simple and reliable connections by reducing the risk of stripped or crossed threads.

Apartment buildings have unique metering needs. Honeywell offers a range of hybrid water meter products equipped with radio communication devices to permit landlords to accurately measure tenants' usage in multi-family dwellings.

For commercial and industrial applications, bulk flow metering can provide critical data that is useful in environmental analysis geared toward reducing water loss. The Honeywell T5000 hybrid turbine meter is designed for bulk flow metering in commercial and industrial applications, offering a wide dynamic range and excellent high flow capability. Using proven technology, the rotor is the only moving part of the whole meter. The rotation of the rotor is detected using inductive technology. By using contact-free sensing there is no drag on the rotor from gearing, leading to excellent flow performance. This type of meter is well-suited to commercial and industrial uses, and ideally should integrate easily with most Honeywell and third party systems and devices. It has an extended battery lifetime of 12 years, depending on ambient temperature and usage.

Analytics

One of the biggest advantages of connected OEMs is the ability of system components to securely communicate data back to the manufacturers. By sending this information to OEMs about their devices, analytics can be collected to monitor their condition and predict maintenance requirements. This results in improved asset uptime, performance and longevity. This is a win-win for both OEM partners who are able to maintain a connection with their products in the field, enabling them to improve them, and for plant operators who are looking for ways to better manage their field assets.

Cybersecurity

Malware acquired from removable media devices is the number two OT/control system threat, yet USB drives are in common use within water management utility field-level systems. Honeywell's Secure Media Exchange (SMX) technology reduces cybersecurity threats by checking removable media used by personnel and contractors. A check-in system ensures that all USB devices have been scanned for both malicious hardware and software threats before allowing them to access the system. The SMX gateway can provide this protection for legacy devices that cannot, or no longer, support their own malicious software prevention capabilities. This solution enforces USB removable media policies, and manages both malicious hardware and software threats.

Remote access to field assets must also be better secured to prevent attacks on the system. Honeywell Forge Cybersecurity Core provides Industrial Grade Secure Remote Access for the most critical systems behind multiple network layers and firewalls. As well, Honeywell Industrial Cybersecurity Consulting Services can provide vulnerability scanning and hardening service for the network and its endpoints.

ASSESSING CYBERSECURITY VULNERABILITIES ACROSS THE SYSTEM

Managing cybersecurity in any organization is a challenge, now more than ever. However, managing critical infrastructure cybersecurity within the water and wastewater industry poses additional challenges that require robust solutions that provide the greatest risk mitigation.

Considerations:

- Water and waste utilities are critical infrastructure, vital to the region they serve. There is zero tolerance for a health, safety or environmental incident triggered by a cyber event.
- All spending requires significant justification, particularly for governmental or cooperative-owned entities.
- Cyber incidents are more frequent, and their severity is increasing. Critical infrastructure and corporations are preferred targets for ransomware.
- Effective cybersecurity risk reduction requires planning to mitigate the areas of greatest risk, as well as a lifecycle approach to ensure it is part of every stage—procurement, engineering, commissioning, maintenance.

Honeywell Industrial Cybersecurity understands that each organization and industry is different, the cybersecurity threats they face, and provide end-to-end OT cybersecurity consulting services to help identify and implement the most effective security controls for industrial control system (ICS) and operations technology (OT).

Assessments and audits

Many water and wastewater utility teams wonder where they could be insecure and how they could better manage cybersecurity. The first step is conducting an assessment to understand the current state, gaps and next steps forward. There are many different types of assessments, depending on the needs of the organization.

Honeywell Technology Blocks Security Threats

According to the recent Honeywell Industrial USB Threat Report:

- Of the locations studied, nearly half (44%) detected and blocked at least one malicious or suspicious file that represented a security issue.
- Of those threats blocked by SMX, 1 in 4 (26%) had the potential to cause a major disruption to an industrial control environment, including loss of view or loss of control, and 16% were targeted specifically against Industrial Control System (ICS) or Internet of Things (IoT) systems.
- 15% of the total threats detected and blocked were high-profile, well-known threats, including Stuxnet (2%), Mirai (6%), TRITON (2%), and WannaCry (1%).

Download the complete report here:

https://bit.ly/2Yxd5pK

Cybersecurity vulnerability assessment – A holistic technical review of the OT at a particular point in time to identify vulnerabilities in networks, firewalls, endpoints, applications, etc. Staff can use the report to identify and remediate work prior to corporate audits, help justify cybersecurity spend, and prioritize next steps.

Industrial threat-risk assessment – Explores even deeper into cybersecurity preparedness. This process delivers a detailed security evaluation of the industrial control system's ability to withstand targeted attacks from skilled, motivated and well-sourced bad actors, such as nation-states, terrorist groups, hacktivists and insiders. It identifies the most critical risk scenarios, and uses these attack sequences as basis for further analysis and remediation.

OT penetration testing – Validates the robustness and effectiveness of cybersecurity controls through offensive security testing of the OT system. Honeywell leverages decades of OT experience to provide a safe penetration test of OT/controls systems with very revealing results. Our experience expands beyond just Honeywell control systems, but also any other SCADA, DCS, or operational technology with knowledge of their architectures and common weak points. Our approach and rules of engagement ensures the operability and reliability of the OT/ICS is not negatively impacted.

Cybersecurity assessments or audits are performed at least once every two years by a non-partisan group (i.e., corporate audit or third party) to analyze the current state of OT cybersecurity. Honeywell's OT cybersecurity expertise is one of the strongest and can provided the expert recommendations you need to justify and focus your cybersecurity investment.

LEARN MORE >

USB removable media

It is virtually impossible to maintain OT without the use of portable devices like flash drives and USB memory sticks. In addition to employees, third-party contractors and service providers rely extensively on USB exchanges to move files in and out of the OT system.

Honeywell Secure Media Exchange (SMX) reduces the cybersecurity risk and operational disruption to water OT systems by better protecting the use of removable media, and manages USB ports throughout the facility against cyber risk and unauthorized usage. The easy-to-use interface enables safer, more productive use of removable media and provides operators with unprecedented control and visibility into the use of USB and removable storage.

For water and waste facilities, the SMX Gateway:

- Can be located in a central location like the control center or work permit office
- Is portable and can be carried in a service vehicle to remote locations
- Provides better protection for endpoints and legacy devices that cannot protect themselves from malware
- Delivers vendor-agnostic intelligence updates on the latest threats
- Enforces USB technical controls at the endpoint, ensuring the SMX gateway is not bypassed and rogue USB media is used

For more information on the limitations of existing malware solutions and why SMX is the world's strongest industrial cybersecurity solution for USB protection, please click here.

Staff and skills shortages

Cybersecurity is often added to existing automation and maintenance staff responsibilities. They are expected to be aware of the latest threats, identify vulnerabilities, patch systems, monitor for breaches and respond to attacks if they occur. This assumes a level of expertise that those charged with these responsibilities may not have and detracts from their ability to manage the underlying OT system.

It is challenging to have expert cybersecurity staff in all locations at all times. Rather, an OT security operations center supported by IT-OT staff or a managed security service (MSS) provider is a fast and cost-effective solution to fill skill gaps in the team, so they can focus on what they do best.

Secure Media Exchange

OT security operations center (SOC) – Optimizes resources by centralizing OT cybersecurity management for multiple sites and systems. Honeywell Forge Cybersecurity Platform provides the foundation for an OT SOC and allows entities to simplify, scale and strengthen their cybersecurity investment.

Secure remote access – Increases the productivity of existing staff and enables them to support remote locations securely. Allows staff/contractor remote access and administration for hundreds of sites with multifactor authentication, granular privileges, site-controlled authorization, real-time collaboration, supervision, recording, and detailed auditing. Takes control of remote access and simplifies the experience.

CYBERSECURITY THROUGHOUT THE ASSET LIFECYCLE

Cybersecurity is not a single project—it is a continual program of improvement. Cyberthreats and incidents are becoming more frequent and severe, and cyber threat-actors are becoming more capable and motivated, so continuous reassessment is required to ensure vulnerabilities are mitigated and safeguards remain effective.

In each step along the process of system acquisition, implementation and operation, advanced security technology must be in place and constantly updated to protect against more advanced cyberthreats. This level of attention to security begins with the buying decision, extends through system design, permeates the deployment process and must be applied diligently to daily operations and maintenance. Every potential point of vulnerability must be identified, risk assessed, and managed. These considerations, when taken together, provide an agile and intelligent end-to-end cybersecurity strategy.

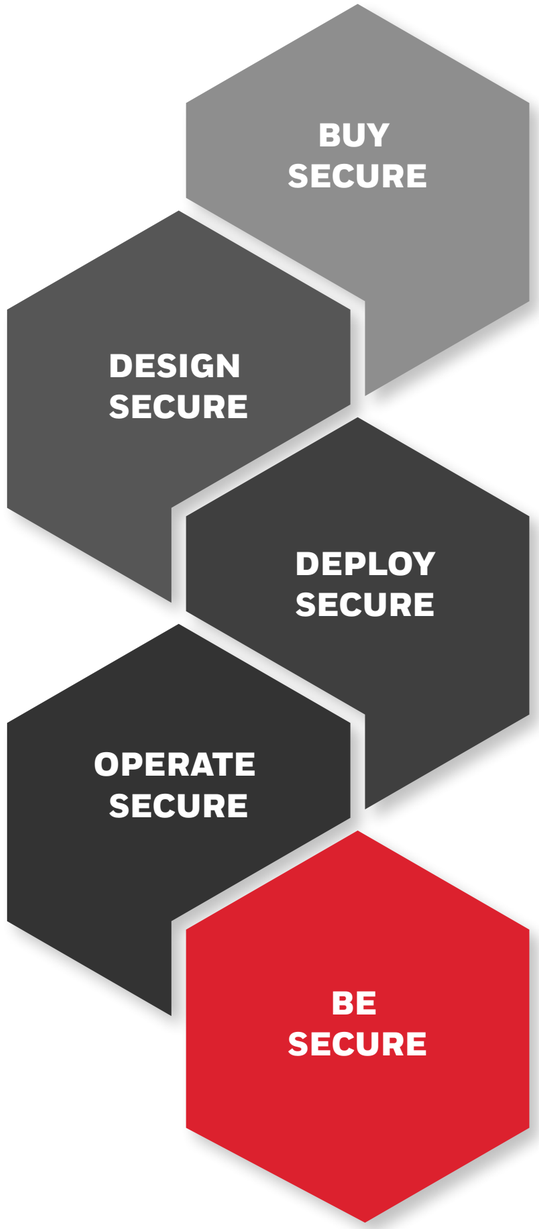
Thorough and well-executed cybersecurity measures include:

Preparation – continuously identifying potential threats and necessary safeguards

Protection – securing remote data access, portable devices and the network perimeter

Detection – monitoring for suspicious behavior, attacks, and addressing compliance issues

Response and recovery – remote incident responses, backup and restore



LEARN MORE >

There is no question that water systems are an attractive target for bad actors. According to Water & Wastes Digest, nearly a quarter of unplanned water outages are the result of cybercrime. The costs for managing a service interruption can be catastrophic, and incidents may violate regulations and cause life-threatening conditions. New malware is constantly being developed, and the security program must be responsive and continuously on guard against both existing and emerging cyberthreats.

While cybercriminals are looking for new ways to penetrate the water and wastewater utility systems, Honeywell's cybersecurity software, products, Managed Security Services (MSS) and Consulting Services, provide trusted expertise in managing the end-to-end security cycle. With three cybersecurity Centers of Excellence located across the globe, research and development efforts are ongoing, and consulting personnel are continuously being trained to meet these evolving challenges.

THE FUTURE IS WHAT WE MAKE IT.

As a global automation leader, Honeywell can help you plan your technology roadmap and stay current with the latest solutions. Furthermore, our turnkey project capabilities deliver the successful outcomes you need.

To learn more about our water and wastewater solutions, visit www.HoneywellProcess.com/Water or contact the Honeywell account manager in your country/region.

Honeywell