Mission Resilience

Helping Water Utilities Stay Safe, Secure & Connected

Helping water and wastewater utilities maintain visibility, continuity, and confidence through secure monitoring, alarming, and control solutions.

RECENT WATER SECTOR CYBERSECURITY EVENTS

WHAT HAPPENED?
Cyberattacks on water infrastructure in communities nationwide

DEFAULT PASSWORDS LEFT IN PLACE
- PLCs deployed with factory-default credentials
- Weak authentication enabled unauthorized access

CONTROLLERS EXPOSED TO THE INTERNET
- Critical operational devices accessible from public networks
- Lack of segmentation increased risk

PLC SECURITY RISKS
- Not vendor-specific
- Root cause was insecure deployment and configuration

OPERATIONAL IMPACTS
- Service disruptions
- Process interruptions
- Operational downtime
- Increased cyber risk exposure

MISSION ENHANCED SECURITY FEATURES

Designed to Help Water Utilities Stay Safe, Secure & Connected

NO DEFAULT HARDWARE CREDENTIALS
Devices are not deployed with common factory passwords.

2FA PROTECTED LOGIN
Additional authentication layer helps prevent unauthorized access.

CONFIGURABLE PASSWORD REQUIREMENTS
Support utility-specific password policies and standards.

ROLE-BASED ACCESS CONTROL
Limit user access based on responsibilities and job functions.

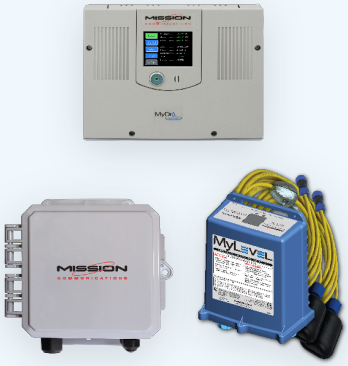
SECURE ISOLATED CELLULAR COMMUNICATIONS
Reduce exposure to public networks through dedicated communications architecture.

Mission combines **secure hardware**, **protected communications**, and **cloud-based monitoring** to help utilities **reduce risk** while maintaining **visibility** and **control**.

THE MISSION DIFFERENCE: BUILT FOR WATER UTILITIES

INDEPENDENT MONITORING
- Continuously monitor critical infrastructure independent of PLC operation
- Increase visibility across remote assets

BACKUP CONTROL CAPABILITY
- Maintain operations during equipment, communications, or cyber disruptions
- Provide an additional layer of visibility and control when it matters most.



INTELLIGENT ALARMING
- Detect abnormal operating conditions
- Deliver actionable alerts when attention is needed

SECURE BY DESIGN
- Purpose-built for water infrastructure
- Leverages Private Cellular Networks, VPNs, Firewalls, and Other Industry Security Best Practices

5 CYBERSECURITY BEST PRACTICES FOR WATER UTILITIES

1 ENCRYPT ALL COMMUNICATIONS
Ensure that data transmitted between field devices and central servers is encrypted using secure protocols. This protects against interception and tampering.

2 USE MULTI-FACTOR AUTHENTICATION (MFA)
Require MFA for all users accessing the SCADA dashboard or water utility monitoring system.

3 HOST IN A SECURE CLOUD ENVIRONMENT
If your SCADA system is cloud-based, verify that it's hosted in a secure, compliant environment with firewalls, intrusion detection, and redundancy.

4 MAINTAIN AUDIT TRAILS
Keep detailed logs of system access, configuration changes, and alarm activity. These records are essential for compliance and incident response.

5 APPLY REGULAR UPDATES & PATCHES
Outdated software is a common vulnerability. Make sure your SCADA platform receives timely updates and security patches—ideally managed by your vendor.

Mission solutions help utilities implement and maintain many of these cybersecurity best practices while improving system visibility and control.

NEED ASSISTANCE?

LOCAL SUPPORT
Local support is available through our Distributor network which can be identified at:
www.123mc.com/en/contact/

24/7 U.S.-BASED TECHNICAL SUPPORT
1-877-923-1454 (Option 2)
Our technical support team is available 24 hours a day, 7 days a week to assist Mission customers.

MISSION 123SCADA

Secure cloud monitoring platform

Mission helps utilities reduce risk, improve visibility, and continue delivering essential services when challenges arise.