Indegy
Activate All Your Senses

Case Study

# Indegy Helps City of Raleigh Ensure Safety and Sustainability of Public Utilities

Raleigh

## At a Glance

**Customer:** City of Raleigh, NC
Municipal Government

### Challenges:

**Difficult and time-consuming** to manually track asset inventory

**Inability to confirm maintenance** work performed by third-party contractors

**Lack of visibility** into all our operations assets

**Need for compliance** with new regulatory requirements

### Results:

**Stronger Security & Control -** Dynamic threat hunting, vulnerability management and incident response

**Greater Visibility & Simplicity -** Comprehensive situational awareness in a single pane of glass

**Enhanced Productivity and Efficiency -** Detailed asset inventory management through automated discovery

**Compliance Readiness -** Audit trail enables demonstrative and proactive compliance to regulatory agencies

## Background

The City of Raleigh Public Utilities department is responsible for providing water and sanitary sewer services to a population of 570,000 people in Raleigh, NC and adjacent areas. These services are managed and maintained by the Technical Applications group, which is responsible for the SCADA network operations and security.

Aware of the growing cyber threat to critical infrastructure facilities and the need to comply with new regulations concerning risk assessment and emergency response, Raleigh's Public Utilities department decided to upgrade its SCADA security solution.

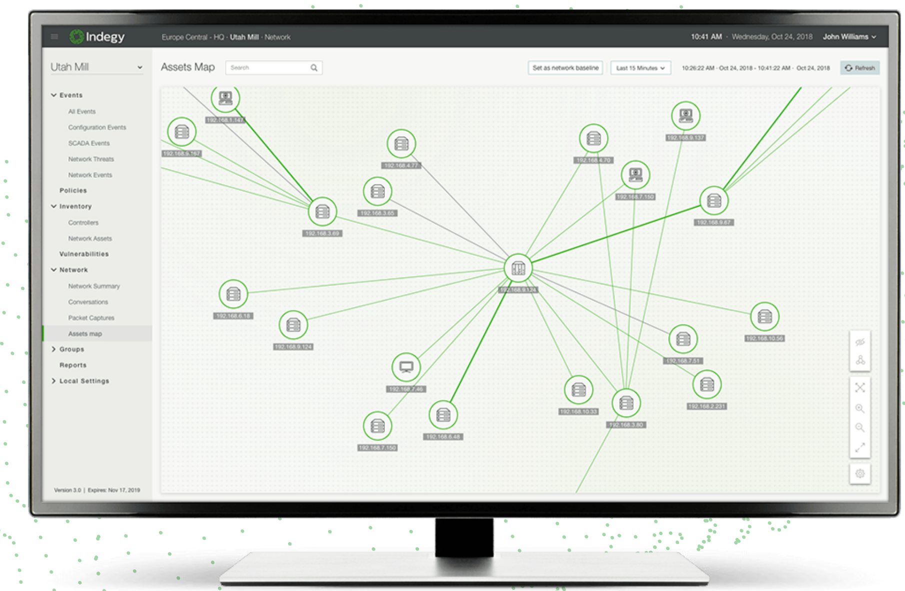
## Passive Network Monitoring Is Not Enough

To ensure a safe and more resilient water infrastructure and to detect potential security threats that could potentially harm the water supply and disrupt critical services, the Public Utilities department required full visibility and control of changes made to PLCs and other key devices in its industrial environment.

They realized that network traffic monitoring only provides half of what's needed to secure ICS environments. Accordingly, they were interested in adding an active detection component that could work alongside passive network monitoring to provide critical information about the ICS environment that cannot be gathered solely by listening to network traffic.

Another key security requirement for the City of Raleigh was automated asset discovery and management. The manual processes previously used for inventory management were both time-consuming and error-prone, making it difficult to maintain an up-to-date and accurate inventory of ICS assets, which is crucial for risk assessment and regulatory compliance.

Automated asset management was also important for operational reliability and safety, as it enables OT managers to plan maintenance schedules, track changes made to devices and restore misconfigured devices.



## Why City of Raleigh Chose Indegy

The City of Raleigh chose Indegy after a thorough RFP process during which they evaluated several vendors. "We chose the Indegy platform for its unique ability to monitor, proactively detect and alert our staff to any changes made to our industrial control systems that could impact their integrity and proper operation," stated Steve Worley, SCADA Security Manager for City of Raleigh.

### Automated Asset Discovery

Given the size and complexity of the SCADA environment, automated asset discovery was a "must have" requirement. Within a matter of minutes of installing the Indegy solution, Worley's team was able to automatically gather and display "huge amounts of data on our network that would have taken weeks to gather manually". The automation provided asset names and IP addresses, MAC addresses and the like, which are useful from a network management standpoint. These details, as well as access to the asset map, were available to all users on a single pane of glass on the Indegy console.

### Real-time Threat Detection

While other vendors offered a more passive monitoring solution, the fact that Indegy offered both passive and active components provided real value for the City of Raleigh. Specifically, the ability to actively query PLCs and learn what programming changes had been made, including versioning history, was a major advantage. "Prior to Indegy, we didn't really have a way to get that version information as changes were made. Now we have a timestamp on when the changes are made and we can determine who made those changes and hold them accountable," explained Worley. This was particularly relevant for monitoring the activities of any third-party contractor or systems integrator, who make changes to PLCs on a regular basis.

### Reliable, Expert Service & Support

With the support of Indegy's engineers, the City of Raleigh smoothly deployed the Industrial Cybersecurity suite within its Public Utilities' ICS/SCADA network. The initial system was up and running on the first day, providing local engineers with complete visibility and control over all industrial operations.

> "Thanks to Indegy's automated asset management, I can **spend less time** on inventory management and **more time on investigating and remediating** actual threats and vulnerabilities," said Worley.

Play Video

Solution: Indegy Industrial Cybersecurity Suite

### Device Integrity

Because the visibility detail was so valuable to Raleigh's SCADA engineers, the Indegy solution's use of patented active detection technology enabled them to experience a more complete security coverage. This was apparent to them in the way the solution discovers, classifies and queries all ICS assets and devices - even those that are not communicating in the network. Native device querying ensures zero impact on network operations. The asset inventory details and enriched context for alerts helped improve alert accuracy and ultimately boost efficiency and productivity for their security team.

### Asset Tracking

Indegy's automated asset discovery provides City of Raleigh with comprehensive visibility, security and control of the ICS environment. It gathers and tracks all device-related activities, creating an up-to-date inventory of all ICS assets, including dormant devices. Indegy automatically maps all controllers and devices on the network, documents their configuration, and provides in-depth visibility into their state. The inventory contains unparalleled asset information depth – tracking Firmware and OS versions, internal configuration, running software and users, as well as serial numbers and backplane configuration for both PCs and Industrial controllers.

## Real-Time Alerts

In addition to the ability to log into a dashboard, Indegy provides real-time alerts for Raleigh with detailed contextual information gathered from devices. The data about suspicious activities and unauthorized changes enables engineering and security to work together, quickly identifying the source of potential problems and instantly mitigating potential risks.

## Comprehensive Audit Trail

The Indegy Industrial Cybersecurity Suite provides a comprehensive audit log detailing all engineering activities related to the devices. By capturing the 'who', 'what', 'when', 'where' and 'how,' the audit trail enables the Raleigh security team to quickly pinpoint the problem, identify the responsible party and facilitate recovery.

Like this case study?

Visit us at Indegy.com for more content like this.

Follow us:

Indegy