

Audit of Department of Utilities Supervisory Control and Data Acquisition (SCADA) System

Report# 2023/24-08 | February 2024

Audit standards allow for the exclusion of information from a publicly available or widely distributed report in circumstances associated with public safety, privacy, or security concerns. Due to the critical and sensitive nature of SCADA, this report omits details that could put SCADA at risk. We have provided a detailed oral report to the Department of Utilities for further consideration.



City of SACRAMENTO

Office of the City Auditor

Performance Audit Division

Farishta Ahrary, Interim City Auditor
Jordan Sweeney, Principal Fiscal Policy Analyst
Parinaz Nejatie, Fiscal Policy Analyst



Our Mission

To provide a catalyst for improvements of municipal operations and promote a credible, efficient, effective, equitable, fair, focused, transparent, and fully accountable City government.

Our Vision

To improve City services by providing independent, objective, and reliable information regarding the City's ability to meet its goals and objectives and establish an adequate system of internal controls, root out improper governmental activities (i.e., fraud, waste, or abuse), and address racial, gender, and ethnic inequities.

Suggest an Audit

The Office of the City Auditor conducts performance audits of the City of Sacramento's operations to determine whether these operations and programs are operating efficiently and effectively. If you would like to offer ideas for audits to save the City money, increase revenues, or improve the efficiency and effectiveness of City operations and programs, please fill out our online form:

https://forms.cityofsacramento.org/f/Suggest_an_Audit_Form

Whistleblower Hotline

In the interest of public accountability and being responsible stewards of public funds, the City has established a whistleblower hotline. The hotline protects the anonymity of those leaving tips to the extent permitted by law. The service is available 24 hours a day, 7 days week, 365 days per year. Through this service, all phone calls and emails will be received anonymously by third party staff.

Report online at <http://www.cityofsacramento.ethicspoint.com> or call toll-free: 888-245-8859.

The City of Sacramento's Office of the City Auditor can be contacted by phone at 916-808-1166 or at the address below:

915 I Street
MC09100
Historic City Hall, Floor 2
Sacramento, CA 95814

Table of Contents

Audit Fact Sheet	3
Introduction	4
Background	4
Funding	5
Proposition 218	5
Organization and Staffing	5
Cybersecurity	6
Standard Frameworks	6
Previous Assessments of SCADA	6
Objective, Scope, and Methodology	7
Findings and Recommendations	8
Department Response	9

Audit of the Department of Utilities Supervisory Control and Data Acquisition (SCADA) System

February 2024

Report # 2023/24-08

What is SCADA?

SCADA is a computer-based industrial control system that allows staff to remotely control operations, monitor equipment status, and analyze historical and real-time data. SCADA is a critical component of the Department of Utilities' operations as it allows the department to operate over 200 facilities throughout the City, including two water treatment plants, a wastewater treatment plant, and numerous wells, sewer pumps (sumps), and reservoirs.

Findings and Recommendations

Audit standards allow for the exclusion of information from a publicly available or widely distributed report in circumstances associated with public safety, privacy, or security concerns. In such circumstances, auditors may issue a separate report only to those parties responsible for acting on the auditor's recommendations. Due to the critical and sensitive nature of SCADA, this report omits details that could put SCADA at risk. We have provided a detailed report to the Department of Utilities for further consideration.

Cybersecurity Risk Assessment Framework

Cybersecurity can be defined as "technologies, processes, and practices designed to protect an organization's information assets - computers, networks, programs, and data - from unauthorized access."

The Institute of Internal Auditor's Global Technology Audit Guide *Assessing Cybersecurity Risk* describes a cybersecurity risk assessment framework that identifies six components and details how vulnerabilities in any one of these areas can cause an organization to be at risk. The six components include: 1) Cybersecurity Governance; 2) Inventory of Information Assets; 3) Standard Security Configurations; 4) Information Access Management; 5) Prompt Response and Remediation; and 6) Ongoing Monitoring.



Institute of Internal Auditor's Global Technology Audit Guide
Assessing Cybersecurity Risk

Introduction

In accordance with the City Auditor’s 2022/23 Audit Plan, we have completed the Audit of the Department of Utilities Supervisory Control and Data Acquisition System (SCADA). We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit standards allow for the exclusion of information from a publicly available or widely distributed report in circumstances associated with public safety, privacy, or security concerns. Due to the critical and sensitive nature of SCADA, this report omits details that could put SCADA at risk. We have provided a detailed oral report to the Department of Utilities for further consideration.

The City Auditor’s Office would like to thank the Department of Utilities for their cooperation during the audit process.

Background

The City of Sacramento Department of Utilities is responsible for the City’s water, wastewater, and storm drainage services. In providing these services, the Department of Utilities works in conjunction with other City departments as well as regional, state, and federal agencies towards the operation, maintenance, development, and rehabilitation of the City’s water resources infrastructure. Their mission is “to provide dependable, high-quality water, wastewater, and storm drainage services in a fiscally and environmentally sustainable manner.”

To provide these services, the Department of Utilities uses a computer-based industrial control system called Supervisory Control and Data Acquisition (SCADA). SCADA is a critical component of the department’s operations; it allows staff to remotely control operations, monitor equipment status, and analyze historical and real-time data. The Department of Utilities operates over 200 facilities throughout the City, including two water treatment plants, a wastewater treatment plant, and numerous wells, sewer pumps (sumps), and reservoirs. SCADA has multiple control rooms where they can remotely control operations at their various facilities throughout the City and get the status of each individual facility at any given time. Additionally, SCADA can be used to review historical data to see how equipment performed during storms or other weather events.

Funding

Over the last five fiscal years, the Department of Utilities’ Electrical, Instrumentation, and SCADA (EIS) team has spent an average of \$7.1 million annually for maintenance and operations; this includes¹ employee costs, parts and supplies, computer equipment, and computer software maintenance. EIS supports the City’s water, wastewater, and storm drainage services and is funded by rate payer dollars collected in conjunction with these services.

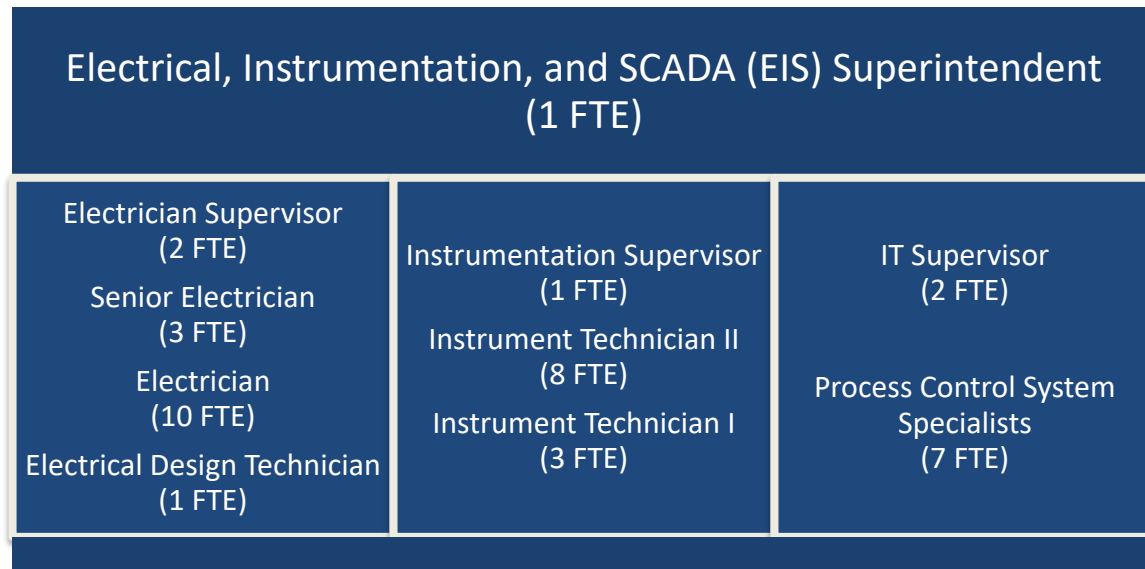
Proposition 218

Proposition 218 is a November 1996 State of California ballot initiative that restricts how much can be charged to ratepayers in California for their utility services. One major aspect of Proposition 218 is that it prohibits the Department of Utilities from charging ratepayers more than the cost to provide the utility service that the rate is charged for. Another major aspect of Proposition 218 is that it prohibits the Department of Utilities from using funds collected for one utility to pay the cost of providing a different utility. For example, funds collected from charging water rates cannot be used to pay for drainage projects that are unrelated to the provision of water service; this includes projects related to SCADA.

Organization and Staffing

The Department of Utilities’ Electrical, Instrumentation, and SCADA (EIS) team is broken up into 4 areas: process control system specialists (PCSS) and security and communications; project support; water plants, wells, and reservoirs; and wastewater and storm drainage. Figure 1 illustrates the organization chart for the Department of Utilities’ EIS team, which consists of 38 full-time equivalent (FTE) positions.

Figure 1: Department of Utilities’ Electrical, Instrumentation, and SCADA (EIS) Team Organizational Chart



Source: Auditor generated based on information provided by the Department of Utilities

¹ Capital improvement costs are not included.

Cybersecurity

The Institute of Internal Auditor’s Global Technology Audit Guide (GTAG) *Assessing Cybersecurity Risk* defines cybersecurity as the “technologies, processes, and practices designed to protect an organization’s information assets— computers, networks, programs, and data – from unauthorized access”. *Assessing Cybersecurity Risk* describes a cybersecurity risk assessment framework that identifies six components, as seen in figure 2 below, and details how vulnerabilities in any one of these areas can cause an organization to be at risk. With the increasing reliance on technology, cyberattacks have become more frequent and have the capability of bringing down critical infrastructure, such as the Department of Utilities’ SCADA system, and disrupting or endangering vital services, including the City’s water, wastewater, and storm drainage services.

Figure 2: Cybersecurity Risk Assessment Framework



Source: Institute of Internal Auditors’ Global Technology Audit Guide, *Assessing Cybersecurity Risk*.

Standard Frameworks

Standard frameworks can be used as guidelines that establish minimum requirements and identify best practices for operating and maintaining SCADA. For example, the State of California uses National Institute of Standards and Technology² (NIST) 800-53 as the minimum information security controls for some state entities. The Department of Utilities follows a combination of frameworks for SCADA.

Previous Assessments of SCADA

There have been three recent assessments of SCADA: (1) an assessment which focused on SCADA system communications, hardware, software, and system operations; (2) a self-assessment focused on

² The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the United States Department of Commerce that promotes innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.

whether appropriate controls are present in the SCADA system; and (3) an assessment which focused on the recent network system upgrade and compared current controls to recommended AWIA criteria.

Objective, Scope, and Methodology

The objective of this audit was to assess the controls over the Department of Utilities' SCADA system, including the controls in place designed to deter and detect fraud. Our scope included SCADA related data and records for fiscal year 2018/19 through fiscal year 2021/22. The primary basis of our methodology came from the Cybersecurity Risk Assessment Framework outlined in the Institute of Internal Auditor's Global Technology Audit Guide *Assessing Cybersecurity Risk*. As such, we reviewed SCADA policies and procedures, financial records, inventory records, logical system access, physical controls, and environmental controls.

Findings and Recommendations

Audit standards allow for the exclusion of information from a publicly available or widely distributed report in circumstances associated with public safety, privacy, or security concerns. Due to the critical and sensitive nature of SCADA, this report omits details that could put SCADA at risk. We have provided a detailed oral report to the Department of Utilities for further consideration.

The detailed oral report provided to the Department of Utilities contained two findings and eight recommendations with opportunities for improvement. While we found that controls over SCADA generally appeared to be working as intended, we found several control gaps that could cause SCADA to be at risk. During the audit, the Department of Utilities addressed several of these control gaps.

Due to the complex nature of SCADA and limited funding, the findings and recommendations contained in the detailed oral report were presented to the Department of Utilities as considerations as they prioritize projects with limited resources.

MEMORANDUM

DATE: January 8, 2024

TO: City Auditor's Office

FROM: Pravani Vandeyar, Director, Department of Utilities

CC: Ryan Moore, Assistant City Manager

SUBJECT: **Audit of the Department of Utilities Supervisory Control and Data Acquisition (SCADA) System**

This memorandum is in response to the City Auditor's Audit of the Department of Utilities Supervisory Control and Data Acquisition (SCADA) System.

The Department of Utilities (DOU) acknowledges receipt and concurs with the recommendations from the City Auditor's oral report. DOU will implement the recommendations in a timely manner.

I would like to take this opportunity to thank the City Auditor and staff for their efforts.